Informatica®

10.1

Informatica® PowerCenter Express

10.1

Befehlsreferenz

Informatica PowerCenter Express Befehlsreferenz
10.110.1
Juni 2016

© Copyright Informatica LLC 1998, 2018

Diese Software und die zugehörige Dokumentation enthalten proprietäre Informationen der Informatica LLC, werden unter einem Lizenzvertrag mit Einschränkungen hinsichtlich Verwendung und Veröffentlichung zur Verfügung gestellt und sind urheberrechtlich geschützt. Das Zurückentwickeln (Reverse Engineering) der Software ist untersagt. Ohne ausdrückliche schriftliche Genehmigung der Informatica LLC darf kein Teil dieses Dokuments zu irgendeinem Zweck vervielfältigt oder übertragen werden, unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln (elektronisch, mechanisch, durch Fotokopieren, Aufzeichnen usw.) dies geschieht. Diese Software ist möglicherweise durch US-amerikanische und/oder internationale Patente und weitere angemeldete Patente geschützt.

Die Verwendung, Vervielfältigung oder Veröffentlichung der Software durch die US-Regierung unterliegt den Bestimmungen des jeweiligen Softwarelizenzvertrags sowie ggf. den Bestimmungen in DFARS 227.7202-1(a) und 227.7702-3(a) (1995), DFARS 252.227-7013 © (1)(ii) (OCT. 1988), FAR 12.212(a) (1995), FAR 52.227-19 oder FAR 52.227-14 (ALT III).

Die in diesem Produkt und in dieser Dokumentation enthaltenen Informationen können jederzeit ohne vorherige Ankündigung geändert werden. Sollten Sie mit diesem Produkt oder dieser Dokumentation Probleme haben, teilen Sie uns dies bitte schriftlich mit.

Informatica, Informatica Platform, Informatica Data Services, PowerCenter, PowerCenterRT, PowerCenter Connect, PowerCenter Data Analyzer, PowerExchange, PowerMart, Metadata Manager, Informatica Data Quality, Informatica Data Explorer, Informatica B2B Data Transformation, Informatica B2B Data Exchange Informatica On Demand, Informatica Identity Resolution, Informatica Application Information Lifecycle Management, Informatica Complex Event Processing, Ultra Messaging, Informatica Master Data Management und Live Data Map sind Marken oder eingetragene Marken der Informatica LLC in den USA und anderen Ländern. Alle weiteren Produkt- und Firmennamen sind möglicherweise Markennamen oder Warenzeichen der jeweiligen Eigentümer.

Teile dieser Software und/oder Dokumentation sind durch die Urheberrechte Dritter geschützt, einschließlich und ohne Einschränkung: Copyright DataDirect Technologies. Alle Rechte vorbehalten. Copyright © Sun Microsystems. Alle Rechte vorbehalten. Copyright © RSA Security Inc. Alle Rechte vorbehalten. Copyright © Ordinal Technology Corp. Alle Rechte vorbehalten. Copyright © Aandacht c.v. Alle Rechte vorbehalten. Copyright Genivia, Inc. Alle Rechte vorbehalten. Copyright Isomorphic Software. Alle Rechte vorbehalten. Copyright © Meta Integration Technology, Inc. Alle Rechte vorbehalten. Copyright © Intalio. Alle Rechte vorbehalten. Copyright © Oracle. Alle Rechte vorbehalten. Copyright © Adobe Systems Incorporated. Alle Rechte vorbehalten. Copyright © DataArt, Inc. Alle Rechte vorbehalten. Copyright © ComponentSource. Alle Rechte vorbehalten. Copyright © Microsoft Corporation. Alle Rechte vorbehalten. Copyright © Rouge Wave Software, Inc. Alle Rechte vorbehalten. Copyright © Teradata Corporation. Alle Rechte vorbehalten. Copyright © Yahoo! Inc. Alle Rechte vorbehalten. Copyright © Glyph & Cog, LLC. Alle Rechte vorbehalten. Copyright © Thinkmap, Inc. Alle Rechte vorbehalten. Copyright © Clearpace Software Limited. Alle Rechte vorbehalten. Copyright © Information Builders, Inc. Alle Rechte vorbehalten. Copyright © OSS Nokalva, Inc. Alle Rechte vorbehalten. Copyright Edifecs, Inc. Alle Rechte vorbehalten. Copyright Cleo Communications, Inc. Alle Rechte vorbehalten. Copyright © International Organization for Standardization 1986. Alle Rechte vorbehalten. Copyright © ej-technologies GmbH . Alle Rechte vorbehalten. Copyright © Jaspersoft Corporation. Alle Rechte vorbehalten. Copyright © International Business Machines Corporation. Alle Rechte vorbehalten. Copyright © yWorks GmbH. Alle Rechte vorbehalten. Copyright © Lucent Technologies. Alle Rechte vorbehalten. Copyright © Universität von Toronto. Alle Rechte vorbehalten. Copyright © Daniel Veillard. Alle Rechte vorbehalten. Copyright © Unicode, Inc. Copyright IBM Corp. Alle Rechte vorbehalten. Copyright © MicroQuill Software Publishing, Inc. Alle Rechte vorbehalten. Copyright © PassMark Software Pty Ltd. Alle Rechte vorbehalten. Copyright © LogiXML, Inc. Alle Rechte vorbehalten. Copyright © 2003-2010 Lorenzi Davide. Alle Rechte vorbehalten. Copyright © Red Hat, Inc. Alle Rechte vorbehalten. Copyright © The Board of Trustees of the Leland Stanford Junior University. Alle Rechte vorbehalten. Copyright © EMC Corporation. Alle Rechte vorbehalten. Copyright © Flexera Software. Alle Rechte vorbehalten. Copyright © Jinfonet Software. Alle Rechte vorbehalten. Copyright © Apple Inc. Alle Rechte vorbehalten. Copyright © Telerik Inc. Alle Rechte vorbehalten. Copyright © BEA Systems. Alle Rechte vorbehalten. Copyright © PDFlib GmbH. Alle Rechte vorbehalten. Copyright © Orientation in Objects GmbH. Alle Rechte vorbehalten. Copyright © Tanuki Software, Ltd. Alle Rechte vorbehalten. Copyright © Ricebridge. Alle Rechte vorbehalten. Copyright © Sencha, Inc. Alle Rechte vorbehalten. Copyright © Scalable Systems, Inc. Alle Rechte vorbehalten. Copyright © jQWidgets. Alle Rechte vorbehalten. Copyright © Tableau Software, Inc. Alle Rechte vorbehalten. Copyright© MaxMind, Inc. Alle Rechte vorbehalten. Copyright © TMate Software s.r.o. Alle Rechte vorbehalten. Copyright © MapR Technologies Inc. Alle Rechte vorbehalten. Copyright © Amazon Corporate LLC. Alle Rechte vorbehalten. Copyright © Highsoft. Alle Rechte vorbehalten. Copyright © Python Software Foundation. Alle Rechte vorbehalten. Copyright © BeOpen.com. Alle Rechte vorbehalten. Copyright © CNRI. Alle Rechte vorbehalten.

Dieses Produkt enthält Software, die von der Apache Software Foundation (http://www.apache.org/) entwickelt wurde, und andere Software, die unter den Bedingungen des Apache-Lizenzvertrags lizenziert ist („Lizenz“). Eine Kopie dieser Lizenzen finden Sie unter http://www.apache.org/licenses/. Sofern nicht gesetzlich vorgeschrieben oder schriftlich vereinbart, erfolgt der Vertrieb der Software unter der Lizenz auf der BASIS „WIE BESEHEN” OHNE GARANTIEN ODER KONDITIONEN IRGENDEINER ART, weder ausdrücklich noch impliziert. Berechtigungen und Einschränkungen für bestimmte Sprachen finden Sie in der Lizenz.

Dieses Produkt enthält Software, die von Mozilla (http://www.mozilla.org/) entwickelt wurde, Software Copyright The JBoss Group, LLC. Alle Rechte vorbehalten; Software Copyright © 1999-2006 by Bruno Lowagie und Paulo Soares, und andere Software, die gemäß den verschiedenen Versionen des GNU Lesser General Public License Agreement unter http://www.gnu.org/licenses/lgpl.html lizenziert ist. Die Materialien werden „wie besehen“ kostenlos von Informatica bereitgestellt, ohne ausdrückliche oder stillschweigende Gewährleistung, einschließlich, jedoch nicht beschränkt auf die stillschweigenden Gewährleistungen der Handelsüblichkeit und der Eignung für einen bestimmten Zweck.

Das Produkt enthält ACE(TM) und TAO(TM) Software, Copyright Douglas C. Schmidt und seine Forschungsgruppe an der Washington University, University of California, Irvine und Vanderbilt University, Copyright (©) 1993-2006. Alle Rechte vorbehalten.

Dieses Produkt enthält Software, die von OpenSSL Project zur Verwendung im OpenSSL Toolkit entwickelt wurde (Copyright The OpenSSL Project. Alle Rechte vorbehalten). Die erneute Verteilung dieser Software unterliegt den unter „http://www.openssl.org“ und „http://www.openssl.org/source/license.html“ verfügbaren Bedingungen.

Dieses Produkt enthält urheberrechtlich geschützte Curl-Software (Copyright 1996-2013, Daniel Stenberg, <daniel@haxx.se>). Alle Rechte vorbehalten. Die mit dieser Software verbundenen Berechtigungen und Einschränkungen unterliegen den unter „http://curl.haxx.se/docs/copyright.html“ verfügbaren Bedingungen. Die Erlaubnis, diese Software für jeden beliebigen Zweck gegen Gebühr oder kostenlos zu verwenden, zu kopieren, zu ändern und zu verteilen, wird hiermit erteilt, sofern die oben genannten urheberrechtlichen Hinweise und diese Erlaubnis in allen Exemplaren angegeben werden.

Das Produkt enthält urheberrechtlich geschützte Software, Copyright 2001-2005 (©) MetaStuff, Ltd. Alle Rechte vorbehalten. Die mit dieser Software verbundenen Berechtigungen und Einschränkungen unterliegen den unter „http://www.dom4j.org/ license.html“ verfügbaren Bedingungen.

Das Produkt enthält urheberrechtlich geschützte Software, Copyright © 2004-2007, The Dojo Foundation. Alle Rechte vorbehalten. Die mit dieser Software verbundenen Berechtigungen und Einschränkungen unterliegen den unter „http://dojotoolkit.org/license“ verfügbaren Bedingungen.

Dieses Produkt enthält urheberrechtlich geschützte ICU-Software, Copyright International Business Machines Corporation und andere. Alle Rechte vorbehalten. Die mit dieser Software verbundenen Berechtigungen und Einschränkungen unterliegen den unter „http://source.icu-project.org/repos/icu/icu/trunk/license.html“ verfügbaren Bedingungen.

Dieses Produkt enthält urheberrechtlich geschützte Software, Copyright © 1996-2006 Per Bothner. Alle Rechte vorbehalten. Das Ihnen erteilte Recht, diese Materialien zu verwenden, unterliegt den unter „http:// www.gnu.org/software/ kawa/Software-License.html“ verfügbaren Bedingungen.

Dieses Produkt enthält urheberrechtlich geschützte OSSP UUID-Software (Copyright © 2002 Ralf S. Engelschall, Copyright © 2002 The OSSP Project Copyright © 2002 Cable & Wireless Deutschland). Die mit dieser Software verbundenen Berechtigungen und Einschränkungen unterliegen den unter „http://www.opensource.org/licenses/mit-license.php“ verfügbaren Bedingungen.

Dieses Produkt enthält Software, die von Boost (http://www.boost.org/) oder unter der Softwarelizenz von Boost entwickelt wurde. Die mit dieser Software verbundenen Berechtigungen und Einschränkungen unterliegen den unter „http://www.boost.org/LICENSE_1_0.txt“ verfügbaren Bedingungen.

Dieses Produkt enthält urheberrechtlich geschützte Software, Copyright © 1997-2007 University of Cambridge. Die mit dieser Software verbundenen Berechtigungen und Einschränkungen unterliegen den unter http://www.pcre.org/license.txt einsehbaren Bedingungen.

Dieses Produkt enthält urheberrechtlich geschützte Software, Copyright © 2007 The Eclipse Foundation. Alle Rechte vorbehalten. Die mit dieser Software verbundenen Berechtigungen und Einschränkungen unterliegen den unter „http://www.eclipse.org/org/documents/epl-v10.php“ und „http://www.eclipse.org/org/documents/edl-v10.php“ verfügbaren Bedingungen.

Dieses Produkt enthält Software gemäß den Lizenzbedingungen unter http://www.tcl.tk/software/tcltk/license.html, http://www.bosrup.com/web/overlib/?License, http://www.stlport.org/doc/ license.html, http://asm.ow2.org/license.html, http://www.cryptix.org/LICENSE.TXT, http://hsqldb.org/web/hsqlLicense.html, http://httpunit.sourceforge.net/doc/ license.html, http://jung.sourceforge.net/license.txt, http://www.gzip.org/zlib/zlib_license.html, http://www.openldap.org/software/release/license.html, http://www.libssh2.org, http://slf4j.org/license.html, http://www.sente.ch/software/OpenSourceLicense.html, http://fusesource.com/downloads/license-agreements/fuse-message-broker-v-5-3- license-agreement; http://antlr.org/license.html; http://aopalliance.sourceforge.net/; http://www.bouncycastle.org/licence.html; http://www.jgraph.com/jgraphdownload.html; http://www.jcraft.com/jsch/LICENSE.txt; http://jotm.objectweb.org/bsd_license.html. http://www.w3.org/Consortium/Legal/2002/copyright-software-20021231; http://www.slf4j.org/license.html; http://nanoxml.sourceforge.net/orig/copyright.html; http://www.json.org/license.html; http://forge.ow2.org/projects/javaservice/, http://www.postgresql.org/about/licence.html, http://www.sqlite.org/copyright.html, http://www.tcl.tk/software/tcltk/license.html, http://www.jaxen.org/faq.html, http://www.jdom.org/docs/faq.html, http://www.slf4j.org/license.html; http://www.iodbc.org/dataspace/iodbc/wiki/iODBC/License; http://www.keplerproject.org/md5/license.html; http://www.toedter.com/en/jcalendar/license.html; http://www.edankert.com/bounce/index.html; http://www.net-snmp.org/about/license.html; http://www.openmdx.org/#FAQ; http://www.php.net/license/3_01.txt; http://srp.stanford.edu/license.txt; http://www.schneier.com/blowfish.html; http://www.jmock.org/license.html; http://xsom.java.net; http://benalman.com/about/license/; https://github.com/CreateJS/EaselJS/blob/master/src/easeljs/display/Bitmap.js; http://www.h2database.com/html/license.html#summary; http://jsoncpp.sourceforge.net/LICENSE; http://jdbc.postgresql.org/license.html; http://protobuf.googlecode.com/svn/trunk/src/google/protobuf/descriptor.proto; https://github.com/rantav/hector/blob/master/LICENSE; http://web.mit.edu/Kerberos/krb5-current/doc/mitK5license.html; http://jibx.sourceforge.net/jibx-license.html; https://github.com/lyokato/libgeohash/blob/master/LICENSE; https://github.com/hjiang/jsonxx/blob/master/LICENSE; https://code.google.com/p/lz4/; https://github.com/jedisct1/libsodium/blob/master/LICENSE; http://one-jar.sourceforge.net/index.php?page=documents&file=license; https://github.com/EsotericSoftware/kryo/blob/master/license.txt; http://www.scala-lang.org/license.html; https://github.com/tinkerpop/blueprints/blob/master/LICENSE.txt; http://gee.cs.oswego.edu/dl/classes/EDU/oswego/cs/dl/util/concurrent/intro.html; https://aws.amazon.com/asl/; https://github.com/twbs/bootstrap/blob/master/LICENSE; https://sourceforge.net/p/xmlunit/code/HEAD/tree/trunk/LICENSE.txt.

Dieses Produkt enthält Software, die unter der Academic Free License (http://www.opensource.org/licenses/afl-3.0.php), der Common Development Distribution License (http://www.opensource.org/licenses/cddl1.php), der Common Public License (http://www.opensource.org/licenses/cpl1.0.php), den Sun Binary Code License Agreement Supplemental License Terms, der BSD License (http:// www.opensource.org/licenses/bsd-license.php), der neuen BSD License (http://opensource.org/licenses/BSD-3-Clause), der MIT License (http://www.opensource.org/licenses/mit-license.php), der Artistic License (http://www.opensource.org/licenses/artistic-license-1.0) und der Initial Developer's Public License Version 1.0 (http://www.firebirdsql.org/en/initial-developer-s-public-license-version-1-0/) lizenziert ist.

Dieses Produkt enthält urheberrechtlich geschützte Software, Copyright © 2003-2006 Joe Walnes, 2006-2007 XStream Committers. Alle Rechte vorbehalten. Die mit dieser Software verbundenen Berechtigungen und Einschränkungen unterliegen den unter „http://xstream.codehaus.org/license.html“ verfügbaren Bedingungen. Dieses Produkt enthält Software, die von der Indiana University Extreme! Lab. entwickelt wurde. Weitere Informationen finden Sie unter http://www.extreme.indiana.edu/.

Dieses Produkt enthält Software, Copyright © 2013 Frank Balluffi und Markus Moeller. Alle Rechte vorbehalten. Die mit dieser Software verbundenen Berechtigungen und Einschränkungen unterliegen den Bedingungen der MIT-Lizenz.

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

HAFTUNGSAUSSCHLUSS: Informatica LLC stellt diese Dokumentation „wie besehen“ bereit, ohne ausdrückliche oder stillschweigende Gewährleistung, einschließlich, jedoch nicht beschränkt auf die Gewährleistungen der Nichtverletzung der Rechte von Dritten, der Handelsüblichkeit oder Eignung für einen bestimmten Zweck. Informatica LLC garantiert nicht die Fehlerfreiheit dieser Software oder Dokumentation. Die in dieser Software oder Dokumentation bereitgestellten Informationen können technische Ungenauigkeiten oder Druckfehler enthalten. Die in dieser Software und in dieser Dokumentation enthaltenen Informationen können jederzeit ohne vorherige Ankündigung geändert werden.

HINWEISE

Dieses Informatica-Produkt (die „Software“) umfasst bestimmte Treiber (die „DataDirect-Treiber“) von DataDirect Technologies, einem Betreiber von Progress Software Corporation („DataDirect“), die folgenden Bedingungen und Bestimmungen unterliegen:

1. DIE DATADIRECT-TREIBER WERDEN „WIE GESEHEN“ OHNE JEGLICHE GEWÄHRLEISTUNG, WEDER AUSDRÜCKLICH NOCH STILLSCHWEIGEND, BEREITGESTELLT, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN DER HANDELSÜBLICHKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER NICHTVERLETZUNG VON RECHTEN DRITTER.
2. IN KEINEM FALL SIND DATADIRECT ODER DRITTANBIETER DEM ENDBENUTZER GEGENÜBER HAFTBAR FÜR UNMITTELBARE, MITTELBARE, KONKRETE, NEBEN-, FOLGE- ODER ANDERE SCHÄDEN, DIE SICH AUS DER VERWENDUNG DER ODBC-TREIBER ERGEBEN, UNABHÄNGIG DAVON, OB SIE IM VORAUS ÜBER DIE MÖGLICHKEIT SOLCHER SCHÄDEN INFORMIERT WORDEN SIND ODER NICHT. DIESE BESCHRÄNKUNGEN GELTEN FÜR ALLE KLAGEGEGENSTÄNDE, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF VERTRAGSBRUCH, GEWÄHRLEISTUNGSBRUCH, FAHRLÄSSIGKEIT, KAUSALHAFTUNG, TÄUSCHUNG UND ANDERE UNERLAUBTE HANDLUNGEN.

Publikationsdatum: 2018-09-27

Inhalt

Einleitung 23

Informatica-Ressourcen. 23

Informatica-Netzwerk. 23

Informatica-Wissensdatenbank. 23

Informatica-Dokumentation. 23

Informatica-Produktverfügbarkeitsmatrizen. 24

Informatica Velocity. 24

Informatica Marketplace. 24

Globaler Kundensupport von Informatica. 24

Kapitel 1: Befehlszeilenprogramme und Dienstprogramme. 25

Befehlszeilenprogramme und Dienstprogramme - Übersicht. 25

Kapitel 2: Installieren und Konfigurieren von Befehlszeilendienstprogrammen. 27

Installieren und Konfigurieren von Befehlszeilendienstprogrammen – Übersicht. 27

Installieren der Befehlszeilendienstprogramme. 28

Installationsverzeichnisse. 28

Konfigurieren der Befehlszeilendienstprogramme. 29

Konfigurieren der Informatica-Dienstprogramme. 29

Konfigurieren der PowerCenter-Dienstprogramme. 29

Konfigurieren der Metadata Manager-Dienstprogramme. 30

Erstellen der Datei „domains.infa“. 30

Sicherheitskonfiguration für Informatica-Dienstprogramme 31

Kapitel 3: Verwenden der Befehlszeilenprogramme. 32

Verwenden der Befehlszeilenprogramme - Übersicht. 32

Eingeben von Optionen und Argumenten. 33

Syntax-Notation. 34

Ausführen von Befehlen in einer sicheren Domäne. 35

Ausführen von Befehlen unter UNIX mit Kerberos-Authentifizierung. 36

Ausführen von Befehlen unter UNIX mit Single Sign On. 36

Ausführen von Befehlen unter UNIX ohne Single Sign On. 37

Ausführen von Befehlen unter Windows mit Kerberos-Authentifizierung. 38

Kapitel 4: Umgebungsvariablen für Befehlszeilenprogramme. 39

Umgebungsvariablen für Befehlszeilenprogramme - Übersicht. 40

ICMD_JAVA_OPTS. 41

Konfigurieren von ICMD_JAVA_OPTS unter UNIX. 42

Konfigurieren von ICMD_JAVA_OPTS unter Windows. 42

INFA_CLIENT_RESILIENCE_TIMEOUT. 42
Konfigurieren von INFA_CLIENT_RESILIENCE_TIMEOUT unter UNIX. 42
Konfigurieren von INFA_CLIENT_RESILIENCE_TIMEOUT unter Windows. 43
INFA_CODEPAGENAME. 43
Konfigurieren von INFA_CODEPAGENAME unter UNIX. 43
Konfigurieren von INFA_CODEPAGENAME unter Windows. 43
INFA_DEFAULT_DATABASE_PASSWORD. 43
Konfigurieren von INFA_DEFAULT_DATABASE_PASSWORD unter UNIX. 44
Konfigurieren von INFA_DEFAULT_DATABASE_PASSWORD unter Windows. 44
INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD. 45
Konfigurieren von INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD unter UNIX. 45
Konfigurieren von INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD unter Windows. 45
INFA_DEFAULT_DOMAIN. 46
Konfigurieren von INFA_DEFAULT_DOMAIN unter UNIX. 46
Konfigurieren von INFA_DEFAULT_DOMAIN unter Windows. 46
INFA_DEFAULT_DOMAIN_PASSWORD. 46
Konfigurieren von INFA_DEFAULT_DOMAIN_PASSWORD unter UNIX. 47
Konfigurieren von INFA_DEFAULT_DOMAIN_PASSWORD unter Windows. 47
INFA_DEFAULT_DOMAIN_USER. 47
Konfigurieren von INFA_DEFAULT_DOMAIN_USER unter UNIX. 47
Konfigurieren von INFA_DEFAULT_DOMAIN_USER unter Windows. 48
INFA_DEFAULT_PWX_OSEPASSWORD. 48
Konfigurieren von INFA_DEFAULT_PWX_OSEPASSWORD unter UNIX. 48
Konfigurieren von INFA_DEFAULT_PWX_OSEPASSWORD unter Windows. 49
INFA_DEFAULT_PWX_OSPASSWORD. 49
Konfigurieren von INFA_DEFAULT_PWX_OSPASSWORD unter UNIX. 49
Konfigurieren von INFA_DEFAULT_PWX_OSPASSWORD unter Windows. 49
INFA_DEFAULT_SECURITY_DOMAIN. 49
Konfigurieren von INFA_DEFAULT_SECURITY_DOMAIN unter UNIX. 50
Konfigurieren von INFA_DEFAULT_SECURITY_DOMAIN unter Windows. 50
INFA_JAVA_CMD_OPTS. 50
Konfigurieren von INFA_JAVA_CMD_OPTS unter UNIX. 50
Konfigurieren von INFA_JAVA_CMD_OPTS unter Windows. 51
INFA_PASSWORD. 51
Konfigurieren von INFA_PASSWORD unter UNIX. 51
Konfigurieren von INFA_PASSWORD unter Windows. 52
INFA_NODE_KEYSTORE_PASSWORD. 52
Konfigurieren von INFA_NODE_KEYSTORE_PASSWORD unter UNIX. 52
Konfigurieren von INFA_NODE_KEYSTORE_PASSWORD unter Windows. 53
INFA_NODE_TRUSTSTORE_PASSWORD. 53
Konfigurieren von INFA_NODE_TRUSTSTORE_PASSWORD unter UNIX. 53
Konfigurieren von INFA_NODE_TRUSTSTORE_PASSWORD unter Windows. 54

INFA_REPCNX_INFO. 54
Konfigurieren von INFA_REPCNX_INFO unter UNIX. 54
Konfigurieren von INFA_REPCNX_INFO unter Windows. 54
INFA_REPOSITORY_PASSWORD. 55
Konfigurieren von INFA_REPOSITORY_PASSWORD unter UNIX. 55
Konfigurieren von INFA_REPOSITORY_PASSWORD unter Windows. 55
INFATOOL_DATEFORMAT. 55
Konfigurieren von INFATOOL_DATEFORMAT unter UNIX. 56
Konfigurieren von INFATOOL_DATEFORMAT unter Windows. 56
Verschlüsseln von Passwörtern. 56
Verwenden eines Passworts als eine Umgebungsvariable. 57
Festlegen des Benutzernamens. 58
Konfigurieren eines Benutzernamens als eine Umgebungsvariable unter UNIX. 58
Konfigurieren eines Benutzernamens als eine Umgebungsvariable unter Windows. 58

Kapitel 5: Verwenden von infacmd. 59

Verwenden von infacmd - Übersicht. 59
infacmd-Befehlsprogramme. 60
infacmd ListPlugins. 60
Ausführen von Befehlen. 61
infacmd-Rückgabewerte. 62
infacmd UpdateGatewayInfo. 62

Kapitel 6: infacmd as-Befehlsreferenz. 64

CreateService. 64
ListServiceOptions. 67
ListServiceProcessOptions. 69
UpdateServiceOptions. 71
UpdateServiceProcessOptions. 73

Kapitel 7: infacmd aud-Befehlsreferenz. 76

getDomainObjectPermissions. 76
getPrivilegeAssociation. 78
getUserGroupAssociation. 80
getUserGroupAssociationForRoles. 83
getUsersPersonalInfo. 85

Kapitel 8: Infacmd bg-Befehlsreferenz. 88

upgradeRepository. 88
listGlossary. 90
exportGlossary. 91
importGlossary. 95

Kapitel 9: infacmd cms-Befehlsreferenz 101

CreateAuditTables 101
CreateService 103
DeleteAuditTables 106
ListServiceOptions 108
ListServiceProcessOptions 110
Löschen 112
Aktualisieren des Suchindexes des Modellrepository 114
RemoveService 115
ResyncData 116
UpdateServiceOptions 118
UpdateServiceProcessOptions 120
Upgrade 122

Kapitel 10: infacmd dis-Befehlsreferenz 125

AddParameterSetEntries 126
BackupApplication 128
CancelDataObjectCacheRefresh 130
CreateService 132
DeleteParameterSetEntries 135
DeployApplication 137
ListApplicationObjectPermissions 139
ListApplicationObjects 141
ListApplicationOptions 143
ListApplications 145
ListComputeOptions 146
ListDataObjectOptions 148
ListParameterSetEntries 150
ListParameterSetObjects 152
ListParameterSets 154
ListSequenceObjectProperties 155
ListSequenceObjects 157
ListServiceOptions 159
ListServiceProcessOptions 161
PurgeDataObjectCache 162
PurgeResultSetCache 165
RefreshDataObjectCache 166
RenameApplication 168
RestoreApplication 170
SetApplicationPermissions 172
SetApplicationObjectPermissions 174
SetSequenceState 177

StartApplication. 179
StopApplication. 181
stopBlazeService. 183
UndeployApplication. 185
UpdateApplication. 186
UpdateApplicationOptions. 188
UpdateComputeOptions. 190
UpdateDataObjectOptions. 192
Datenobjektoptionen. 194
UpdateParameterSetEntries. 195
UpdateServiceOptions 197
Optionen des Datenintegrationsdiensts. 199
UpdateServiceProcessOptions 210
Data Integration Service-Prozessoptionen. 212

Kapitel 11: Infacmd es-Befehlsreferenz. 215

ListServiceOptions. 215
UpdateServiceOptions. 217
UpdateSMTPOptions. 218

Kapitel 12: infacmd ihs-Befehlsreferenz. 222

createservice. 222
ListServiceOptions. 226
UpdateServiceOptions. 227
BackupData. 229
Cluster-Dienst aktualisieren. 230
Snapshot entfernen. 232

Kapitel 13: infacmd ipc-Befehlsreferenz. 233

ExportToPC. 233
ImportFromPC. 237
genReuseReportFromPC. 239

Kapitel 14: Infacmd isp-Befehlsreferenz. 242

AddAlertUser. 242
AddConnectionPermissions. 244
AddDomainLink. 246
AddDomainNode. 248
AddGroupPrivilege. 250
AddLicense. 252
AddNamespace. 254
AddNodeResource. 256
AddRolePrivilege. 259

AddServiceLevel. 261
AddUserPrivilege. 263
AddUserToGroup 265
AssignDefaultOSProfile. 267
AssignedToLicense. 270
AssignGroupPermission 271
AssignISToMMService. 274
AssignLicense. 276
AssignRoleToGroup. 277
AssignRoleToUser 279
AssignRSToWSHubService. 281
AssignUserPermission 283
ConvertLogFile. 286
convertUserActivityLogFile. 286
CreateConnection. 287
Adabas-Verbindungsoptionen. 291
DataSift-Verbindungsoptionen. 293
DB2 für i5/OS-Verbindungsoptionen. 294
Facebook-Verbindungsoptionen. 297
Greenplum-Verbindungsoptionen. 299
HBase-Verbindungsoptionen. 300
HDFS-Verbindungsoptionen. 302
Hadoop Connection Options. 304
Hive-Verbindungsoptionen. 311
DB2 für z/OS-Verbindungsoptionen. 316
IBM DB2-Verbindungsoptionen. 318
IMS-Verbindungsoptionen. 322
JDBC Connection Options. 324
LinkedIn-Verbindungsoptionen. 327
Microsoft SQL Server-Verbindungsoptionen. 328
Netezza-Verbindungsoptionen. 332
OData-Verbindungsoptionen. 334
ODBC-Verbindungsoptionen. 335
Oracle-Verbindungsoptionen. 338
Salesforce-Verbindungsoptionen. 341
SAP-Verbindungsoptionen. 343
Sequentielle Verbindungs-Optionen. 344
Verbindungsoptionen des parallelen Teradata-Transporters. 346
Twitter-Verbindungsoptionen. 348
Twitter Streaming-Verbindungsoptionen. 350
VSAM-Verbindungsoptionen. 351
Verbindungsoptionen von Web Content-Kapow Katalyst. 353

CreateFolder. 355
CreateGrid. 357
CreateGroup 358
CreateIntegrationService. 360
Integrationsdienst-Optionen. 364
Integration Service-Prozessoptionen. 369
CreateMMService. 370
Metadata Manager-Dienst-Optionen 372
CreateOSProfile 374
Datenintegrationsdienst-Prozessoptionen für Betriebssystemprofile. 378
PowerCenter-Integrationsdienst-Prozessoptionen für Betriebssystemprofile. 379
CreateRepositoryService. 380
CreateRole. 385
CreateSAPBWService. 387
SAP BW Service-Optionen. 390
SAP BW Service-Prozessoption. 391
CreateUser 391
CreateWSHubService. 394
Web Services Hub-Optionen. 397
DeleteNamespace. 398
DisableNodeResource. 400
DisableService. 402
DisableServiceProcess. 404
DisableUser. 406
EditUser. 408
EnableNodeResource. 411
EnableService. 413
EnableServiceProcess. 414
EnableUser 416
ExportDomainObjects. 418
ExportUsersAndGroups. 421
generateHadoopConnectionFromHiveConnection. 422
GetFolderInfo. 425
GetLastError. 427
GetLog. 429
GetNodeName. 432
GetServiceOption. 433
GetServiceProcessOption. 435
GetServiceProcessStatus. 437
GetServiceStatus. 439
GetSessionLog. 441
GetSystemLogDirectory. 444

getUserActivityLog. 445
GetWorkflowLog. 449
Hilfe. 453
ImportDomainObjects. 453
ImportUsersAndGroups. 457
ListAlertUsers. 459
ListAllGroups. 460
ListAllRoles 462
ListAllUsers 463
ListConnectionPermissions. 465
ListConnectionPermissionsByGroup. 467
ListConnectionPermissionsByUser. 469
ListConnections. 471
ListConnectionOptions. 473
ListDefaultOSProfiles. 475
ListDomainLinks. 477
ListDomainOptions. 479
ListFolders. 480
ListGridNodes. 482
ListGroupPermissions. 483
ListGroupPrivileges. 485
ListGroupsForUser. 487
ListLDAPConnectivity 489
ListLicenses. 491
ListMonitoringOptions. 493
ListNodeOptions. 494
ListNodeResources. 496
ListNodeRoles. 497
ListNodes. 499
ListOSProfiles. 501
ListRepositoryLDAPConfiguration. 503
ListRolePrivileges. 504
ListSecurityDomains. 506
ListServiceLevels. 508
ListServiceNodes. 509
ListServicePrivileges 511
ListServices. 513
ListSMTPOptions. 515
ListUserPermissions. 517
ListUserPrivileges 519
migrateUsers. 521
MoveFolder. 523

MoveObject. 525
Ping. 527
PrintSPNAndKeytabNames. 528
PurgeLog. 530
PurgeMonitoringData. 532
RemoveAlertUser. 534
RemoveConnection. 536
RemoveConnectionPermissions. 538
RemoveDomainLink. 540
RemoveFolder. 542
RemoveGrid. 544
RemoveGroup. 545
RemoveGroupPermission 547
RemoveGroupPrivilege. 549
RemoveLicense. 551
RemoveNode. 553
RemoveNodeResource. 555
RemoveOSProfile. 557
RemoveRole 558
RemoveRolePrivilege 560
RemoveService. 562
RemoveServiceLevel. 564
RemoveUser. 566
RemoveUserFromGroup 568
RemoveUserPermission 569
RemoveUserPrivilege 572
RenameConnection. 574
ResetPassword. 576
RunCPUProfile. 578
SetConnectionPermissions. 580
SetLDAPConnectivity 582
SetRepositoryLDAPConfiguration 585
ShowLicense. 588
ShutdownNode. 590
SwitchToGatewayNode. 591
SwitchToWorkerNode. 593
SyncSecurityDomains. 595
UnassignDefaultOSProfile. 597
UnassignISMMService. 599
UnassignLicense. 601
UnassignRoleFromGroup 602
UnassignRoleFromUser. 605

UnassignRSWSHubService. 607
UnassociateDomainNode. 608
UpdateConnection. 610
UpdateDomainOptions. 614
UpdateFolder. 616
UpdateGatewayInfo 618
UpdateGrid. 619
UpdateIntegrationService. 621
UpdateLicense. 623
UpdateMMService. 625
UpdateMonitoringOptions. 627
UpdateNamespace. 630
UpdateNodeOptions. 633
UpdateNodeRole. 635
UpdateOSProfile. 638
UpdateRepositoryService. 641
UpdateSAPBWService. 646
UpdateServiceLevel. 648
UpdateServiceProcess. 649
UpdateSMTPOptions. 652
UpdateWSHubService. 653
validateFeature. 655
Version. 657

Kapitel 15: infacmd ldm-Befehlsreferenz. 658

BackupData. 658
CreateService. 660
ListServiceOptions. 667
restoreData. 669
removesnapshot. 670
UpdateServiceOptions. 673
upgrade. 674

Kapitel 16: infacmd mrs-Befehlsreferenz. 676

BackupContents. 677
CheckInObject. 679
CreateContents. 680
CreateFolder. 682
CreateProject. 684
CreateService. 686
DeleteContents. 689
DeleteFolder. 691
DeleteProject. 693

ListBackupFiles. 695
ListCheckedOutObjects. 697
listFolders. 699
ListLockedObjects 701
ListProjects. 703
ListServiceOptions. 705
ListServiceProcessOptions. 707
PopulateVCS. 709
ReassignCheckedOutObject. 711
rebuildDependencyGraph. 713
RenameFolder. 715
RestoreContents. 717
UndoCheckout. 719
UnlockObject 721
UpdateServiceOptions. 723
Optionen des Modellrepository-Diensts. 725
UpdateServiceProcessOptions. 729
UpgradeContents. 731

Kapitel 17: infacmd ms-Befehlsreferenz 734

GetRequestLog. 734
ListMappingParams. 736
ListMappingParams-Ausgabe. 738
ListMappings. 739
RunMapping. 741
UpgradeMappingParameterFile. 745

Kapitel 18: Infacmd oie-Befehlsreferenz. 748

DeployApplication. 748
ExportObjects. 749
exportResources. 753
ImportObjects. 755

Kapitel 19: infacmd ps-Befehlsreferenz. 762

cancelProfileExecution. 762
CreateWH. 764
DropWH. 766
Execute. 767
executeProfile. 770
getExecutionStatus. 772
getProfileExecutionStatus. 773
List. 775
migrateProfileResults. 777

migrateScorecards. 779
Purge. 780
synchronizeProfile. 783

Kapitel 20: infacmd pwx-Befehlsreferenz. 785

CloseForceListener. 785
CloseListener. 788
CondenseLogger. 791
createdatamaps. 794
CreateListenerService. 797
CreateLoggerService. 799
DisplayAllLogger. 804
DisplayCPULogger. 807
DisplayEventsLogger. 810
DisplayMemoryLogger. 813
DisplayRecordsLogger. 816
displayStatsListener. 819
DisplayStatusLogger. 822
FileSwitchLogger. 825
ListTaskListener. 828
ShutDownLogger. 831
StopTaskListener. 834
UpgradeModels. 837
UpdateListenerService. 840
UpdateLoggerService. 844

Kapitel 21: infacmd rms-Befehlsreferenz. 849

ListComputeNodeAttributes. 849
ListServiceOptions. 851
SetComputeNodeAttributes. 852
UpdateServiceOptions. 854
Optionen des Ressourcenmanager-Diensts. 856

Kapitel 22: infacmd rtm-Befehlsreferenz. 857

DeployImport. 857
Export. 859
Import. 862

Kapitel 23: infacmd sch-Befehlsreferenz. 865

CreateSchedule. 865
Gültige Zeitzonenparameter. 869
DeleteSchedule. 873
ListSchedule. 875

ListServiceOptions. 877
ListServiceProcessOptions. 879
PauseAll. 881
PauseSchedule. 882
ResumeAll. 884
ResumeSchedule. 885
UpdateSchedule. 887
UpdateServiceOptions. 891
Optionen des Scheduler-Diensts. 892
UpdateServiceProcessOptions. 894
Optionen des Scheduler-Dienstprozesses. 895
Upgrade. 896

Kapitel 24: infacmd search-Befehlsreferenz. 899

CreateService. 899
ListServiceOptions. 902
ListServiceProcessOptions. 904
UpdateServiceOptions. 906
UpdateServiceProcessOptions. 908

Kapitel 25: infacmd sql-Befehlsreferenz. 910

ExecuteSQL. 910
ListColumnOptions. 911
ListColumnPermissions. 913
ListSQLDataServiceOptions. 915
ListSQLDataServicePermissions. 917
ListSQLDataServices. 918
ListStoredProcedurePermissions. 920
ListTableOptions. 922
ListTablePermissions. 924
PurgeTableCache. 925
RefreshTableCache 927
RenameSQLDataService. 929
SetColumnPermissions. 931
SetSQLDataServicePermissions. 933
SetStoredProcedurePermissions. 936
SetTablePermissions. 939
StartSQLDataService. 941
StopSQLDataService. 943
UpdateColumnOptions. 945
Spaltenoptionen. 947
UpdateSQLDataServiceOptions. 948
SQL-Datendienst-Optionen. 949

UpdateTableOptions. 951
Virtuelle Tabellenoptionen. 953

Kapitel 26: infacmd tdm-Befehlsreferenz. 954

CreateService. 954
CreateContents. 960
EnableService. 962
DisableService. 963

Kapitel 27: infacmd wfs-Befehlsreferenz. 966

abortWorkflow. 966
bulkComplete. 968
cancelWorkflow. 970
createTables. 972
dropTables. 974
listActiveWorkflowInstances. 976
listMappingPersistedOutputs. 978
listWorkflowParams. 980
listWorkflowParams-Ausgabe. 982
listWorkflows. 982
recoverWorkflow. 984
setMappingPersistedOutputs. 986
startWorkflow. 989
upgradeWorkflowParameterFile. 992

Kapitel 28: infacmd ws-Befehlsreferenz. 996

ListOperationOptions. 996
ListOperationPermissions. 998
ListWebServiceOptions. 1000
ListWebServicePermissions. 1002
ListWebServices. 1004
RenameWebService. 1006
SetOperationPermissions. 1008
SetWebServicePermissions. 1011
StartWebService. 1014
StopWebService. 1016
UpdateOperationOptions. 1017
Operationsoptionen. 1019
UpdateWebServiceOptions. 1020
Web-Dienst-Optionen. 1022

Kapitel 29: infacmd xrf-Befehlsreferenz. 1024

generateReadableViewXML. 1024

updateExportXML. 1024

Kapitel 30: infacmd-Steuerdateien. 1026

infacmd-Steuerdateien - Übersicht. 1026
Konfiguration von Steuerdateien. 1027
Benennungskonventionen für Steuerdateien. 1027
Exportsteuerdateien. 1028
Export-Steuerdatei-Parameter für Domänenobjekte. 1028
Exportsteuerdateiparameter für Modellrepository-Objekte. 1030
Importsteuerdateien. 1032
Import-Steuerdatei-Parameter für Domänenobjekte. 1033
Importsteuerdateiparameter für Modellrepository-Objekte. 1035
Regeln und Richtlinien für Steuerdateien. 1040
Steuerdatei-Beispiele für Domänenobjekte. 1041
Steuerdatei-Beispiele für Model Repository-Objekte. 1042

Kapitel 31: infasetup-Befehlsreferenz. 1044

Verwenden von infasetup. 1044
Ausführen von Befehlen. 1045
Befehlsoptionen. 1045
infasetup Befehlsreferenz. 1045
Verwenden von Datenbankverbindungsstrings. 1046
BackupDomain. 1046
DefineDomain. 1049
DefineGatewayNode. 1061
DefineWorkerNode. 1068
DeleteDomain. 1072
GenerateEncryptionKey. 1075
Hilfe. 1076
ListDomainCiphers. 1077
MigrateEncryptionKey. 1078
RestoreDomain. 1079
SwitchToKerberosMode. 1082
UpdateGatewayNode. 1083
UpdateKerberosAdminUser. 1088
UpdateKerberosConfig. 1089
UpdateDomainCiphers. 1089
UpdateWorkerNode. 1092
UnlockUser. 1095
ValidateandRegisterFeature. 1096

Kapitel 32: Pmcmd-Befehlsreferenz. 1097

Verwenden von pmcmd. 1098

Ausführen von Befehlen im Befehlszeilenmodus. 1098
Ausführen von Befehlen im interaktiven Modus. 1100
Ausführen im wait-Modus. 1101
Scripting von pmcmd-Befehlen. 1102
Eingeben von Befehlsoptionen. 1102
AbortTask. 1103
abortworkflow. 1105
Connect. 1107
Disconnect. 1108
Exit. 1109
GetRunningSessionsDetails. 1109
GetServiceDetails. 1110
GetServiceProperties. 1112
getsessionstatistics. 1113
GetTaskDetails. 1115
GetWorkflowDetails. 1117
Hilfe. 1121
PingService. 1121
RecoverWorkflow. 1122
ScheduleWorkflow. 1124
SetFolder. 1126
SetNoWait. 1126
SetWait. 1127
ShowSettings. 1127
StartTask. 1127
Verwenden von Parameterdateien mit starttask. 1130
StartWorkflow. 1131
Verwenden von Parameterdateien mit startworkflow. 1134
StopTask. 1135
StopWorkflow. 1137
UnscheduleWorkflow. 1139
UnsetFolder. 1141
Version. 1141
WaitTask. 1141
WaitWorkflow. 1143

Kapitel 33: pmrep-Befehlsreferenz. 1146

Verwenden von pmrep. 1148
Ausführen von Befehlen im Befehlszeilenmodus. 1148
Ausführen von Befehlen im interaktiven Modus. 1148
Ausführen von Befehlen im normalen und exklusiven Modus. 1149
pmrep-Rückgabewerte. 1149
Verwenden von nativen Verbindungsstrings. 1149

pmrep-Sripting-Befehle. 1150
Verbindungsuntertypen. 1151
AddToDeploymentGroup. 1153
ApplyLabel. 1155
AssignIntegrationService. 1157
AssignPermission. 1158
Beispiel. 1159
BackUp. 1160
ChangeOwner. 1161
CheckIn. 1161
CleanUp. 1162
ClearDeploymentGroup. 1162
Connect. 1163
Create. 1164
CreateConnection. 1165
Festlegen der Datenbank-Codepage. 1168
CreateDeploymentGroup. 1168
CreateFolder. 1169
Zuweisen von Berechtigungen. 1170
CreateLabel. 1171
Delete. 1171
DeleteConnection. 1172
DeleteDeploymentGroup. 1173
DeleteFolder. 1173
DeleteLabel. 1173
DeleteObject 1174
DeployDeploymentGroup. 1175
DeployFolder. 1176
ExecuteQuery. 1178
Exit. 1180
FindCheckout. 1180
GetConnectionDetails. 1182
GenerateAbapProgramToFile. 1182
Hilfe. 1184
InstallAbapProgram. 1184
KillUserConnection. 1187
ListConnections. 1187
ListObjectDependencies 1188
ListObjects. 1190
Auflisten von Objekttypen. 1192
Auflisten von Ordnern. 1195
Auflisten von Objekten. 1195

ListTablesBySess. 1196
ListUserConnections. 1197
MassUpdate. 1197
Sitzungseigenschafts-Typen. 1200
Regeln und Richtlinien für MassUpdate. 1203
Beispiel-Protokolldatei. 1203
ModifyFolder. 1204
Benachrichtigen. 1205
ObjectExport. 1205
Beispiele. 1207
ObjectImport 1207
PurgeVersion. 1208
Beispiele. 1210
Register. 1211
RegisterPlugin. 1212
Registrieren eines Sicherheitsmoduls 1213
Beispiel. 1214
Wiederherstellen. 1214
Beispiel. 1215
RollbackDeployment 1216
Beispiel. 1216
Ausführen. 1216
ShowConnectionInfo. 1217
SwitchConnection. 1218
TruncateLog. 1218
UndoCheckout. 1219
Unregister. 1220
UnregisterPlugin. 1221
Aufheben der Registrierung eines externen Sicherheitsmoduls. 1222
Beispiel. 1223
UpdateConnection. 1223
UpdateEmailAddr. 1225
UpdateSeqGenVals. 1225
UpdateSrcPrefix. 1227
UpdateStatistics 1228
UpdateTargPrefix. 1228
Upgrade. 1229
UninstallAbapProgram. 1230
Validieren. 1231
Version. 1234

Kapitel 34: Arbeiten mit pmrep-Dateien. 1235

Arbeiten mit pmrep-Dateien - Übersicht. 1235

Verwenden der persistenten Eingabedatei . . . 1235
Erstellen einer persistenten Eingabedatei mit pmrep. . . . 1236
Manuelles Erstellen einer persistenten Eingabedatei. . . . 1237
Verwenden der Objektimport-Steuerdatei. . . . 1238
Objektimport-Steuerdatei-Parameter. . . . 1239
Objektimport-Steuerdatei – Beispiele. . . . 1242
Importieren von Quellobjekten. . . . 1243
Importieren von mehreren Objekten in einen Ordner. . . . 1244
Einchecken der und Beschriften von importierten Objekten. . . . 1244
Beibehalten von Sequenzgenerator- und Normalisierungsprogramm-Werten. . . . 1244
Importieren von Objekten und lokalen Shortcut-Objekten zum selben Repository. . . . 1245
Importieren von Shortcut-Objekten aus einem anderen Repository. . . . 1245
Importieren von Objekten in mehrere Ordner. . . . 1245
Importieren von spezifischen Objekten. . . . 1246
Wiederverwenden und Ersetzen von abhängigen Objekten. . . . 1246
Ersetzen ungültiger Mappings. . . . 1247
Umbenennen von Objekten. . . . 1247
Kopieren von SAP-Mappings und SAP-Programminformationen. . . . 1248
Anwenden von Standard-Verbindungsattributen. . . . 1248
Auflösen von Objektkonflikten. . . . 1248
Verwenden der Bereitstellungssteuerdatei . . . 1249
Bereitstellungs-Steuerdatei-Parameter. . . . 1251
Bereitstellungs-Steuerdatei – Beispiele. . . . 1254
Bereitstellen der aktuellen Version eines Ordners. . . . 1254
Bereitstellen der aktuellen Version einer Bereitstellungsgruppe. . . . 1255
Auflisten mehrerer Quell- und Target-Ordner . . . 1255
Tipps für die Arbeit mit pmrep-Dateien. . . . 1256

Anhang A: Veraltete Befehle. . . . 1258

Veraltete Befehle - Übersicht. . . . 1258
BackupDARepositoryContents (veraltet). . . . 1259
CreateDARepositoryContents (veraltet). . . . 1260
CreateReportingService (veraltet). . . . 1262
Reporting Service-Optionen. . . . 1264
Reporting-Quelloptionen. . . . 1266
Lineage Service-Optionen. . . . 1266
DeleteDARepositoryContents (veraltet). . . . 1267
RestoreDARepositoryContents (veraltet). . . . 1269
UpdateReportingService (veraltet). . . . 1271
UpgradeDARepositoryContents (veraltet). . . . 1272
UpgradeDARepositoryUsers (veraltet). . . . 1274

Index. . . . 1277

Einleitung

Die *Informatica-Befehlsreferenz* wurde für Informatica-Administratoren und -Entwickler geschrieben, die die Repositories sowie die Domänen und Dienste verwalten. In diesem Handbuch wird davon ausgegangen, dass Sie mit den Betriebssystemen in Ihrer Umgebung vertraut sind. Des Weiteren wird vorausgesetzt, dass Sie sich mit den Schnittstellenanforderungen für die unterstützenden Anwendungen auskennen.

Informatica-Ressourcen

Informatica-Netzwerk

Im Informatica-Netzwerk finden Sie den globalen Kundensupport von Informatica, die Informatica-Wissensdatenbank und andere Produktressourcen. Für den Zugriff auf das Informatica-Netzwerk besuchen Sie https://network.informatica.com.

Als Mitglied können Sie:

- zentral auf alle Ihre Informatica-Ressourcen zugreifen.
- Durchsuchen Sie die Wissensdatenbank nach Produktressourcen, einschließlich Dokumentation, häufig gestellter Fragen und bewährter Methoden.
- Zeigen Sie Informationen zur Produktverfügbarkeit an.
- Ihre Support-Fälle prüfen.
- Ihr lokales Informatica-Netzwerk für Benutzergruppen suchen und mit anderen Benutzern zusammenarbeiten.

Informatica-Wissensdatenbank

Verwenden Sie die Informatica-Wissensdatenbank, um das Informatica-Netzwerk nach Produktressourcen, wie z. B. Dokumentation, Ratgeberartikeln, bewährten Methoden und PAMs, zu durchsuchen.

Für den Zugriff auf die Wissensdatenbank besuchen Sie https://kb.informatica.com. Wenn Sie Fragen, Kommentare oder Ideen zur Wissensdatenbank haben, wenden Sie sich per E-Mail an das Team der Informatica-Wissensdatenbank unter KB_Feedback@informatica.com.

Informatica-Dokumentation

Navigieren Sie zur Informatica-Wissensdatenbank unter https://kb.informatica.com/_layouts/ProductDocumentation/Page/ProductDocumentSearch.aspx, um die aktuelle Dokumentation für Ihr Produkt abzurufen.

Wenn Sie Fragen, Kommentare oder Ideen zu dieser Dokumentation haben, wenden Sie sich per E-Mail an das Informatica-Dokumentationsteam unter infa_documentation@informatica.com.

Informatica-Produktverfügbarkeitsmatrizen

Produktverfügbarkeitsmatrizen (PAMs) geben die Versionen der Betriebssysteme, Datenbanken und anderen Typen von Datenquellen und Zielen an, die in einer Produktversion unterstützt werden. Als Mitglied des Informatica-Netzwerks können Sie unter https://network.informatica.com/community/informatica-network/product-availability-matrices auf PAMs zugreifen.

Informatica Velocity

Bei Informatica Velocity handelt es sich um eine Sammlung von Tipps und bewährten Methoden, die von den professionellen Informatica-Diensten entwickelt wurden. Informatica Velocity basiert auf der Praxiserfahrung aus Hunderten von Datenmanagementprojekten und umfasst das kollektive Wissen unserer Berater, die mit Unternehmen aus der ganzen Welt an der Planung, Entwicklung, Bereitstellung und Wartung erfolgreicher Datenmanagementlösungen gearbeitet haben.

Als Mitglied des Informatica-Netzwerks können Sie unter http://velocity.informatica.com auf Informatica Velocity-Ressourcen zugreifen.

Wenn Sie Fragen, Anregungen oder Ideen zu Informatica Velocity haben, wenden Sie sich an die professionellen Informatica-Dienste unter ips@informatica.com.

Informatica Marketplace

Informatica Marketplace ist ein Forum, das Lösungen zur Erweiterung und Verbesserung Ihrer Informatica-Implementierungen bereitstellt. Indem Sie die zahlreichen Lösungen von Informatica-Entwicklern und -Partnern nutzen, können Sie Ihre Produktivität steigern und die Implementierungsdauer Ihrer Projekte verkürzen. Zugriff auf den Informatica Marketplace erhalten Sie unter https://marketplace.informatica.com.

Globaler Kundensupport von Informatica

Sie können sich telefonisch oder über den Online-Support mit einem globalen Support-Center im Informatica-Netzwerk in Verbindung setzen.

Die Telefonnummer des globalen Kundensupports von Informatica vor Ort finden Sie auf der Informatica-Website unter folgender Verknüpfung: http://www.informatica.com/us/services-and-training/support-services/global-support-centers.

Als Mitglied des Informatica-Netzwerks können Sie den Online-Support unter http://network.informatica.com verwenden.

KAPITEL 1

Befehlszeilenprogramme und Dienstprogramme

- Befehlszeilenprogramme und Dienstprogramme - Übersicht, 25

Befehlszeilenprogramme und Dienstprogramme - Übersicht

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

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

In der folgenden Tabelle werden die Informatica-Dienstprogramme beschrieben:

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

In der folgenden Tabelle werden die PowerCenter-Dienstprogramme beschrieben:

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

In der folgenden Tabelle werden die Metadata Manager-Dienstprogramme beschrieben:

Befehlszeilenprogramm	Beschreibung
mmcmd	Laden und Verwalten von Ressourcen. Importieren und Exportieren von Modellen und benutzerdefinierten Ressourcen.
mmLineageMigrator	Migrieren Sie Verknüpfungsinformationen der Datenverlaufskontrolle nach dem Upgrade von Metadata Manager 9.6.x auf die aktuelle Version. **Hinweis:** Da dieses Programm automatisch ausgeführt wird, führen Sie dieses Programm nicht aus, außer wenn die Migration fehlschlägt und Sie den Fehler beheben, oder wenn Sie durch den globalen Kundensupport von Informatica zum Ausführen dieses Programms angewiesen werden.
mmRepoCmd	Erstellen, Löschen, Sichern und Wiederherstellen von Metadata Manager-Repository-Inhalten. Stellen Sie eine PowerCenter-Repository-Sicherungsdatei, die Metadata Manager-Objekte enthält, in der PowerCenter-Repository-Datenbank wieder her.
mmXConPluginUtil	Generieren Sie die Bild-Mapping-Informationen oder das Plug-In für ein universelles XConnect.
rmu	Migrieren von Ressourcen aus einer früheren Version von Metadata Manager auf die aktuelle Version.
rcfmu	Migrieren einer Ressourcenkonfigurationsdatei aus einer früheren Version von Metadata Manager auf die aktuelle Version.

KAPITEL 2

Installieren und Konfigurieren von Befehlszeilendienstprogrammen

Dieses Kapitel umfasst die folgenden Themen:

- Installieren und Konfigurieren von Befehlszeilendienstprogrammen – Übersicht, 27
- Installieren der Befehlszeilendienstprogramme, 28
- Konfigurieren der Befehlszeilendienstprogramme, 29
- Sicherheitskonfiguration für Informatica-Dienstprogramme , 31

Installieren und Konfigurieren von Befehlszeilendienstprogrammen – Übersicht

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

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

- Installieren Sie die Befehszeilendienstprogramme.
- Konfigurieren Sie die Befehszeilendienstprogramme.

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

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

Installieren der Befehlszeilendienstprogramme

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

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

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

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

Installationsverzeichnisse

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

Installation von Informatica-Diensten

Die Informatica-Dienstprogramme sind im folgenden Verzeichnis installiert:

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

Die PowerCenter-Dienstprogramme sind im folgenden Verzeichnis installiert:

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

Die Metadata Manager-Dienstprogramme sind in folgendem Verzeichnis installiert:

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

Installation des Informatica-Clients

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

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

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

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

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

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

Dienstprogramminstallation über die Befehlszeile

Die Informatica-Dienstprogramme sind im folgenden Verzeichnis installiert:

```
<Dienstprogramm-Installationsverzeichnis>/PowerCenter/isp/bin
```

Die PowerCenter-Dienstprogramme sind im folgenden Verzeichnis installiert:

```
<Dienstprogramm-Installationsverzeichnis>/PowerCenter/server/bin
```

Die Metadata Manager-Dienstprogramme sind in folgendem Verzeichnis installiert:

```
<Dienstprogramm-Installationsverzeichnis>/MetadataManager/utilities
```

Konfigurieren der Befehlszeilendienstprogramme

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

Konfigurieren der Informatica-Dienstprogramme

Konfigurieren der Umgebungsvariablen für die Befehlszeilenprogramme infacmd und infasetup.

Legen Sie zum Ausführen von infacmd die Umgebungsvariable ICMD_JAVA_OPTS fest.

Legen Sie zum Ausführen von infasetup die Umgebungsvariable INFA_JAVA_CMD_OPTS fest.

Konfigurieren der PowerCenter-Dienstprogramme

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

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

Wenn zum Beispiel die Befehlzeilendienstprogramme im Ordner `/data/Informatica_cmd_utilities/` installiert sind, befinden sich die PowerCenter-Dienstprogramme im Ordner `/data/Informatica_cmd_utilities/PowerCenter/server/bin`. Unter Linux können Sie die Umgebungsvariablen an der Eingabeaufforderung wie folgt festlegen:

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

Hinweis: Starten Sie den Computer neu, nachdem Sie die INFA_HOME-Umgebungsvariable oder die Bibliothekspfad-Umgebungsvariable konfiguriert haben.

Konfigurieren der Metadata Manager-Dienstprogramme

Um Metadata Manager-Dienstprogramme zu konfigurieren, konfigurieren Sie Umgebungsvariablen, die den Speicherort der Java Virtual Machine und das Informatica-Root-Verzeichnis angeben. Außerdem müssen Sie den Speicherort für die gemeinsam genutzte Bibliothek für Solaris überprüfen.

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

Konfigurieren Sie die folgenden Umgebungsvariablen:

JAVA_HOME

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

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

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

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

   ```
   set JAVA_HOME=C:\InfaUtilities\PowerCenter\java
   ```

4. Speichern und schließen Sie die Batchdatei bzw. das Shell-Skript.

INFA_HOME

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

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

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

LD_LIBRARY_PATH

Erforderlich für Solaris. Gibt den Speicherort für die gemeinsam genutzte Bibliothek an. Stellen Sie sicher, dass die Umgebungsvariable LD_LIBRARY_PATH die folgenden Verzeichnisse enthält:

```
${JAVA_HOME}/jre/lib/sparcv9/server:${JAVA_HOME}/jre/lib/sparcv9/jli
```

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

Hinweis: Starten Sie den Rechner neu, nachdem Sie INFA_HOME oder die Umgebungsvariable LD_LIBRARY_PATH konfiguriert haben.

Erstellen der Datei „domains.infa“

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

Wenn die Domäne die Kerberos-Authentifizierung verwendet, müssen Sie bei der Ausführung der meisten Befehle von Befehlszeilenprogrammen Informationen zur Domänenkonnektivität eingeben. Geben Sie die Informationen zur Domänenkonnektivität über die Option „--domainName“ oder über die Option „--gateway“

ein. Für die Verwendung der Option „--domainName“ muss die Datei „domains.infa“ die Informationen zur Gateway-Konnektivität für die Domäne enthalten. Wenn die Datei „domains.infa“ nicht vorhanden ist oder die Informationen in der Datei nicht mehr aktuell sind, müssen Sie beim Ausführen von Befehlen, die eine Verbindung zur Domäne herstellen, die Option „--gateway“ verwenden.

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

Führen Sie zum Erstellen der Datei „domains.infa“ den Befehl infacmd isp UpdateGatewayInfo aus. Der Befehl erstellt oder aktualisiert die Datei „domains.infa“ im PowerCenter-Verzeichnis in der Installation des Befehlszeilen-Dienstprogramms, beispielsweise `<Dienstprogramm-Installationsverzeichnis>\PowerCenter`.

Sicherheitskonfiguration für Informatica-Dienstprogramme

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

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

Sichere Kommunikation

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

Kerberos-Authentifizierung

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

Verwandte Themen:

- “ Ausführen von Befehlen in einer sicheren Domäne” auf Seite 35
- “Ausführen von Befehlen unter UNIX mit Kerberos-Authentifizierung” auf Seite 36
- “Ausführen von Befehlen unter Windows mit Kerberos-Authentifizierung” auf Seite 38

KAPITEL 3

Verwenden der Befehlszeilenprogramme

Dieses Kapitel umfasst die folgenden Themen:

- Verwenden der Befehlszeilenprogramme - Übersicht, 32
- Eingeben von Optionen und Argumenten, 33
- Syntax-Notation, 34
- Ausführen von Befehlen in einer sicheren Domäne, 35
- Ausführen von Befehlen unter UNIX mit Kerberos-Authentifizierung, 36
- Ausführen von Befehlen unter Windows mit Kerberos-Authentifizierung, 38

Verwenden der Befehlszeilenprogramme - Übersicht

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

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

Informatica enthält die folgenden Befehlszeilenprogramme:

- **infacmd**. Verwenden Sie infacmd zum Zugreifen auf die Informatica-Anwendungsdienste.
- **infacmd**. Verwenden Sie infacmd zum Abrufen des Knotennamens, zum Aktualisieren der Gateway-Informationen sowie zum Auflisten der unterstützten Plugins.
- **infasetup**. Verwenden Sie infasetup zum Durchführen von Installationsaufgaben, wie z. B. dem Definieren eines Knotens oder einer Domäne.
- **infasetup**. Verwenden Sie infasetup zum Aktualisieren des Gateway-Knotens.
- **pmcmd**. Verwenden Sie pmcmd zum Verwalten von Arbeitsabläufen. Sie können mit pmcmd Arbeitsabläufe starten, stoppen, planen und überwachen.
- **pmrep**. Verwenden Sie pmrep zum Durchführen von Aufgaben zur Repository-Verwaltung, wie z. B. Auflisten von Repository-Objekten, Erstellen und Bearbeiten von Gruppen und Wiederherstellen und Löschen von Repositorys.
- **mmcmd**. Verwenden Sie mmcmd, um Ressourcen zu laden und zu verwalten und Modelle und benutzerdefinierte Ressourcen zu importieren und exportieren.

- **mmLineageMigrator**. Verwenden Sie „mmLineageMigrator“ zum Migrieren von Verknüpfungsinformationen der Datenverlaufskontrolle nach dem Upgrade von Metadata Manager 9.6.x auf die aktuelle Version.

  Hinweis: Da dieses Programm automatisch ausgeführt wird, führen Sie dieses Programm nicht aus, außer wenn die Migration fehlschlägt und Sie den Fehler beheben, oder wenn Sie durch den globalen Kundensupport von Informatica zum Ausführen dieses Programms angewiesen werden.
- **mmRepoCmd**. Verwenden Sie mmRepoCmd, um Metadata Manager-Repository-Inhalte zu erstellen, zu löschen, zu sichern und wiederherzustellen. Sie können auch eine PowerCenter-Repository-Sicherungsdatei, die Metadata Manager-Objekte enthält, in der PowerCenter-Repository-Datenbank wiederherstellen.
- **mmXConPluginUtil**. Verwenden Sie „mmXConPluginUtil“ zum Generieren der Bild-Mapping-Informationen oder des Plug-Ins für ein universelles XConnect.
- **rcfmu**. Migrieren Sie eine Ressourcenkonfigurationsdatei aus einer früheren Version von Metadata Manager auf die aktuelle Version mit „rcfmu“.
- **rmu**. Migrieren Sie Ressourcen aus einer früheren Version von Metadata Manager auf die aktuelle Version mit „rmu“.

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

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

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

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

Eingeben von Optionen und Argumenten

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

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

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

  ```
  Connect -r <repository_name>
  ```
- Geben Sie Optionen in beliebiger Reihenfolge ein.
- Wenn eine von Ihnen über die Befehlszeile angegebene Option Leerzeichen enthält, setzen Sie die Option in doppelte Anführungszeichen.
- Das erste Wort nach der Option ist das Argument.
- Die meisten Optionen erfordern Argumente.
  Bei Verwendung von pmcmd oder infacmd müssen Sie Optionen von Argumenten mit einem einzelnen Leerzeichen trennen. Wenn Sie pmrep verwenden, müssen Sie Optionen nicht von Argumenten trennen.

Bei Verwendung von infacmd müssen Sie Optionen von Argumenten mit einem einzelnen Leerzeichen trennen.

- Wenn ein Argument mehr als ein Wort enthält, setzen Sie das Argument in doppelte Anführungszeichen. Für „pmrep“ und „pmcmd“ können Sie auch einfache Anführungszeichen verwenden.

  Unpaarige Anführungszeichen führen zu einem Fehler.

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

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

- Wenn ein Argument im Format `optionsname=wert` vorliegt und der Wert sowohl ein Leerzeichen als auch ein Gleichheitszeichen (=) enthält, muss dem Gleichheitszeichen ein umgekehrter Schrägstrich vorangestellt werden.
  Beispiel: Ein Argument enthält die Option `DatabaseUser`, und der Name des Datenbankbenutzers lautet `a#v%5^=! !`. Verwenden Sie bei Eingabe des Arguments das folgende Format: `DBUser=a#v%5^\=! !`

- Für „pmcmd“ können Sie Leerzeichen in einem Argument verwenden. Um ein Argument mit Leerzeichen anzugeben, schließen Sie das Argument in einfache oder doppelte Anführungszeichen ein. Wenn Sie einfache oder doppelte Anführungszeichen im Argument verwenden, muss ihnen ein umgekehrter Schrägstrich vorangestellt werden.

Syntax-Notation

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

Konvention	Beschreibung
-x	Eine vor einem Argument platzierte Option. Diese kennzeichnet den Parameter, den Sie eingeben. Um z. B. den Benutzernamen für pmcmd einzugeben, geben Sie -u oder -user gefolgt vom Benutzernamen ein.
< x >	Erforderliche Option. Wenn Sie eine erforderliche Option nicht angeben, gibt das Befehlszeilenprogramm eine Fehlermeldung zurück.

<x | y>
 	
{x | y}
	Wählen Sie zwischen erforderlichen Optionen aus. Um den Befehl auszuführen, müssen Sie aus den aufgeführten Optionen auswählen. Wenn Sie eine erforderliche Option nicht angeben, gibt das Befehlszeilenprogramm eine Fehlermeldung zurück.
	In pmrep kennzeichnen die geschweiften Klammern Gruppen von erforderlichen Optionen, wie im folgenden Beispiel:
	`KillUserConnection`
	`  {-i <connection_id> |`
	`  -n <user_name> |`
	`  -a (kill_all)}`
	Wenn ein Pipesymbol (|) Optionen trennt, müssen Sie genau eine Option angeben. Wenn Optionen nicht durch Pipesymbole getrennt sind, müssen Sie alle Optionen angeben.

Konvention	Beschreibung
[x]	Optionaler Parameter. Der Befehl wird unabhängig von der Eingabe optionaler Parameter ausgeführt. Zum Beispiel hat der Help-Befehl die folgende Syntax: `Help [Command]` Wenn Sie einen Befehl eingeben, gibt das Befehlszeilenprogramm Informationen nur zu diesem Befehl zurück. Wenn Sie den Namen des Befehls nicht angeben, gibt das Befehlszeilenprogramm eine Liste aller Befehle zurück.
[x | y]	Wählen Sie zwischen optionalen Parametern aus. Viele Befehle in pmcmd werden beispielsweise entweder im Warte- oder im Nichtwarte-Modus ausgeführt. `[-wait|-nowait]` Wenn Sie einen Modus angeben, wird der Befehl im angegebenen Modus ausgeführt. Der Befehl wird unabhängig von der Eingabe des optionalen Parameters ausgeführt. Wenn Sie keinen Modus angeben, führt pmcmd den Befehl im standardmäßigen Nichtwarte-Modus aus.
< < x | y> **|** <a | b> **>**	Wenn ein Satz eine Teilmenge enthält, wird die Obermenge mit Klammern in Fettschrift **<** **>** angegeben. Ein Pipesymbol in Fettschrift (**|**) trennt die Teilmengen.
(Text)	In pmrep wird beschreibender Text von Parenthesen umschlossen. Hierzu gehören beispielsweise die Liste möglicher Werte für ein Argument oder eine Erläuterung zu einer Option, die kein Argument annimmt. Beschreibender Text wird in Klammern eingeschlossen, wie z. B. die Liste der möglichen Werte für ein Argument oder eine Erläuterung für eine Option, die kein Argument annimmt.

Ausführen von Befehlen in einer sicheren Domäne

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

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

INFA_TRUSTSTORE

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

INFA_TRUSTSTORE_PASSWORD

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

Hinweis: Das Passwort muss verschlüsselt werden. Verwenden Sie das Befehlszeilenprogramm pmpasswd zum Verschlüsseln des Passworts mit Verschlüsselungstyp CRYPT_SYSTEM. Weitere Informationen hierzu finden Sie unter "Verschlüsseln von Passwörtern" auf Seite 56.

Ausführen von Befehlen unter UNIX mit Kerberos-Authentifizierung

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

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

Ausführen von Befehlen unter UNIX mit Single Sign On

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

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

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

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

Einstellen der Kerberos-Umgebungsvariablen

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

Richten Sie die folgenden Umgebungsvariablen ein:

KRB5CCNAME

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

KRB5_CONFIG

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

Generieren der Cache-Datei für Anmeldedaten

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

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

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

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

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

   Beim Erstellen des Caches für Benutzeranmeldedaten müssen Sie die Option „forwardable“ (-f) oder „proxiable“ (-p) verwenden. Unter Solaris 10 verwenden Sie die proxiable-Option. Auf andere UNIX-Plattformen verwenden Sie die forwardable-Option. Sie können die folgende Befehlssyntax verwenden:
   Solaris 10

   ```
   kinit -p <Prinzipalname>
   ```

   Andere UNIX-Plattformen

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

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

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

3. Geben Sie das Passwort für das Benutzerkonto ein.

Ausführen von Befehlen unter UNIX ohne Single Sign On

Um Befehle unter UNIX ohne Single Sign On auszuführen, setzen Sie die Umgebunsvariable *KRB5_CONFIG* auf den Pfad und den Dateinamen der Kerberos-Konfigurationsdatei. Schließen Sie den Benutzernamen und das Passwort ein, wenn Sie den Befehl ausführen, oder setzen Sie den Benutzernamen und das Passwort in Umgebungsvariablen.

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

1. Befehlsoptionen. Wenn Sie die Benutzernamenoption (-un) und die Passwortoption (-pd) im Befehl einschließen, verwendet der Befehl den Benutzernamen und das Passwort, die für die Optionen angegeben sind.
2. Umgebungsvariablen Wenn Sie die Benutzernamenoption und die Passwortoption im Befehl nicht einschließen, verwendet der Befehl den Benutzernamen und das Passwort, die in den Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER und INFA_DEFAULT_DOMAIN_PASSWORD angegeben sind.

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

Ausführen von Befehlen unter Windows mit Kerberos-Authentifizierung

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

Wenn Sie Single Sign On nicht unter Windows verwenden, setzen Sie die Umgebungsvariable KRB5_CONFIG auf den Pfad und den Dateinamen der Kerberos-Konfigurationsdatei. Der Name der Konfigurationsdatei lautet krb5.conf.
Die Befehle bestimmen die Benutzeranmeldedaten, je nachdem, wie Sie den Benutzernamen und das Passwort angeben. Die Befehle prüfen die Anmeldedaten in folgender Reihenfolge:

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

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

KAPITEL 4

Umgebungsvariablen für Befehlszeilenprogramme

Dieses Kapitel umfasst die folgenden Themen:

- Umgebungsvariablen für Befehlszeilenprogramme - Übersicht, 40
- ICMD_JAVA_OPTS, 41
- INFA_CLIENT_RESILIENCE_TIMEOUT, 42
- INFA_CODEPAGENAME, 43
- INFA_DEFAULT_DATABASE_PASSWORD, 43
- INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD, 45
- INFA_DEFAULT_DOMAIN, 46
- INFA_DEFAULT_DOMAIN_PASSWORD, 46
- INFA_DEFAULT_DOMAIN_USER, 47
- INFA_DEFAULT_PWX_OSEPASSWORD, 48
- INFA_DEFAULT_PWX_OSPASSWORD, 49
- INFA_DEFAULT_SECURITY_DOMAIN, 49
- INFA_JAVA_CMD_OPTS, 50
- INFA_PASSWORD, 51
- INFA_NODE_KEYSTORE_PASSWORD, 52
- INFA_NODE_TRUSTSTORE_PASSWORD, 53
- INFA_REPCNX_INFO, 54
- INFA_REPOSITORY_PASSWORD, 55
- INFATOOL_DATEFORMAT, 55
- Verschlüsseln von Passwörtern, 56
- Festlegen des Benutzernamens, 58

Umgebungsvariablen für Befehlszeilenprogramme - Übersicht

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

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

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

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

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

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

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

Verwandte Themen:

- “Verschlüsseln von Passwörtern” auf Seite 56
- “Festlegen des Benutzernamens” auf Seite 58

ICMD_JAVA_OPTS

Die ICMD_JAVA_OPTS-Umgebungsvariable gilt für das infacmd-Befehlszeilenprogramm.

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

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

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

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

Konfigurieren von ICMD_JAVA_OPTS unter UNIX

So konfigurieren Sie ICMD_JAVA_OPTS unter UNIX:

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

  ```
  setenv ICMD_JAVA_OPTS <Java_Options>
  ```

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

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

Konfigurieren von ICMD_JAVA_OPTS unter Windows

So konfigurieren Sie ICMD_JAVA_OPTS unter Windows:

- Geben Sie die Umgebungsvariable ICMD_JAVA_OPTS ein und legen Sie die Java-Optionen wie die -Xmx-Werte und Systemeigenschaften fest.

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

INFA_CLIENT_RESILIENCE_TIMEOUT

Die INFA_CLIENT_RESILIENCE_TIMEOUT-Umgebungsvariable gilt für das infacmd-, pmcmd- und pmrep-Befehlszeilenprogramm.

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

Konfigurieren von INFA_CLIENT_RESILIENCE_TIMEOUT unter UNIX

So konfigurieren Sie INFA_CLIENT_RESILIENCE_TIMEOUT unter UNIX:

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

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

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

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

Konfigurieren von INFA_CLIENT_RESILIENCE_TIMEOUT unter Windows

So konfigurieren Sie INFA_CLIENT_RESILIENCE_TIMEOUT unter Windows:

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

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

INFA_CODEPAGENAME

Die INFA_CODEPAGENAME-Umgebungsvariable gilt für das pmcmd- und pmrep-Befehlszeilenprogramm.

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

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

Konfigurieren von INFA_CODEPAGENAME unter UNIX

So konfigurieren Sie INFA_CODEPAGENAME unter UNIX:

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

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

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

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

Konfigurieren von INFA_CODEPAGENAME unter Windows

So konfigurieren Sie INFA_CODEPAGENAME unter Windows:

- Geben Sie die Umgebungsvariable INFA_CODEPAGENAME ein und legen Sie den Namen der Codeseite als Wert fest.

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

INFA_DEFAULT_DATABASE_PASSWORD

Die INFA_DEFAULT_DATABASE_PASSWORD-Umgebungsvariable gilt für das infasetup-Befehlszeilenprogramm.

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

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

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

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

Verwandte Themen:

- "Verschlüsseln von Passwörtern" auf Seite 56

Konfigurieren von INFA_DEFAULT_DATABASE_PASSWORD unter UNIX

So konfigurieren Sie INFA_DEFAULT_DATABASE_PASSWORD unter UNIX:

1. Geben Sie an der Befehlszeile Folgendes ein:

   ```
   pmpasswd <database password>
   ```

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

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

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

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

Konfigurieren von INFA_DEFAULT_DATABASE_PASSWORD unter Windows

So konfigurieren Sie INFA_DEFAULT_DATABASE_PASSWORD unter Windows:

1. Geben Sie an der Befehlszeile Folgendes ein:

   ```
   pmpasswd <database password>
   ```

   pmpasswd gibt das verschlüsselte Passwort zurück.
2. Geben Sie die Umgebungsvariable INFA_DEFAULT_DATABASE_PASSWORD ein und legen Sie das *verschlüsselte* Passwort als Wert fest.

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

INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD

Die Umgebungsvariable INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD gilt für das infasetup-Befehlszeilenprogramm.

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

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

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

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

Konfigurieren von INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD unter UNIX

So konfigurieren Sie INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD unter UNIX:

1. Geben Sie an der Befehlszeile Folgendes ein:

   ```
   pmpasswd <database password>
   ```

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

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

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

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

Konfigurieren von INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD unter Windows

So konfigurieren Sie INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD unter Windows:

1. Geben Sie an der Befehlszeile Folgendes ein:

   ```
   pmpasswd <database password>
   ```

   pmpasswd gibt das verschlüsselte Passwort zurück.
2. Geben Sie die Umgebungsvariable INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD ein und legen Sie das *verschlüsselte* Passwort als Wert fest.

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

INFA_DEFAULT_DOMAIN

Die INFA_DEFAULT_DOMAIN-Umgebungsvariable gilt für das infacmd-, pmcmd- und pmrep-Befehlszeilenprogramm.

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

Konfigurieren von INFA_DEFAULT_DOMAIN unter UNIX

So konfigurieren Sie INFA_DEFAULT_DOMAIN unter UNIX:

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

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

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

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

Konfigurieren von INFA_DEFAULT_DOMAIN unter Windows

So konfigurieren Sie INFA_DEFAULT_DOMAIN unter Windows:

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

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

INFA_DEFAULT_DOMAIN_PASSWORD

Die INFA_DEFAULT_DOMAIN_PASSWORD-Umgebungsvariable gilt für das infacmd-Befehlszeilenprogramm.

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

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

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

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

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

Verwandte Themen:

- "Verschlüsseln von Passwörtern" auf Seite 56

Konfigurieren von INFA_DEFAULT_DOMAIN_PASSWORD unter UNIX

So konfigurieren Sie INFA_DEFAULT_DOMAIN_PASSWORD unter UNIX:

1. Geben Sie an der Befehlszeile Folgendes ein:

   ```
   pmpasswd <password>
   ```

   pmpasswd gibt das verschlüsselte Passwort zurück.

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

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

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

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

Konfigurieren von INFA_DEFAULT_DOMAIN_PASSWORD unter Windows

So konfigurieren Sie INFA_DEFAULT_DOMAIN_PASSWORD unter Windows:

1. Geben Sie an der Befehlszeile Folgendes ein:

   ```
   pmpasswd <password>
   ```

   pmpasswd gibt das verschlüsselte Passwort zurück.

2. Geben Sie die Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD ein und legen Sie das *verschlüsselte* Passwort als Wert fest.

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

INFA_DEFAULT_DOMAIN_USER

Die INFA_DEFAULT_DOMAIN_USER-Umgebungsvariable gilt für das infacmd-Befehlszeilenprogramm.

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

Konfigurieren von INFA_DEFAULT_DOMAIN_USER unter UNIX

So konfigurieren Sie INFA_DEFAULT_DOMAIN_USER unter UNIX:

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

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

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

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

Konfigurieren von INFA_DEFAULT_DOMAIN_USER unter Windows

So konfigurieren Sie INFA_DEFAULT_DOMAIN_USER unter Windows:

▶ Geben Sie die Umgebungsvariable INFA_DEFAULT_DOMAIN_USER ein und legen Sie den Standardbenutzernamen als Wert fest.

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

INFA_DEFAULT_PWX_OSEPASSWORD

Die INFA_DEFAULT_PWX_OSEPASSWORD- Umgebungsvariable gilt für das infacmd pwx-Befehlszeilenprogramm.

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

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

1. Verwenden Sie zum Verschlüsseln des Passworts das pmpasswd-Befehlszeilenprogramm.

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

Verwandte Themen:

- "Verschlüsseln von Passwörtern" auf Seite 56

Konfigurieren von INFA_DEFAULT_PWX_OSEPASSWORD unter UNIX

So konfigurieren Sie INFA_DEFAULT_PWX_OSEPASSWORD unter UNIX:

1. Geben Sie an der Befehlszeile Folgendes ein:

   ```
   pmpasswd password
   ```

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

   ```
   setenv INFA_DEFAULT_PWX_OSEPASSWORD encrypted_password
   ```

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

   ```
   INFA_DEFAULT_PWX_OSEPASSWORD = encrypted_password
   export INFA_DEFAULT_PWX_OSEPASSWORD
   ```

Konfigurieren von INFA_DEFAULT_PWX_OSEPASSWORD unter Windows

So konfigurieren Sie INFA_DEFAULT_PWX_OSEPASSWORD unter Windows:

1. Geben Sie an der Befehlszeile Folgendes ein:

   ```
   pmpasswd password
   ```

   Das pmpasswd-Programm gibt das verschlüsselte Passwort zurück.

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

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

INFA_DEFAULT_PWX_OSPASSWORD

Die INFA_DEFAULT_PWX_OSPASSWORD-Umgebungsvariable gilt für das infacmd pwx-Befehlszeilenprogramm.

Für einige infacmd pwx-Befehle ist ein Betriebssystempasswort erforderlich. Sie können ein Nur-Text-Passwort als Option mit infacmd pwx bereitstellen oder als Umgebungsvariable INFA_DEFAULT_PWX_OSPASSWORD speichern.

Konfigurieren von INFA_DEFAULT_PWX_OSPASSWORD unter UNIX

So konfigurieren Sie INFA_DEFAULT_PWX_OSPASSWORD unter UNIX:

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

  ```
  setenv INFA_DEFAULT_PWX_OSPASSWORD password
  ```

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

  ```
  INFA_DEFAULT_PWX_OSPASSWORD = password
  export INFA_DEFAULT_PWX_OSPASSWORD
  ```

Konfigurieren von INFA_DEFAULT_PWX_OSPASSWORD unter Windows

Legen Sie zum Konfigurieren vom INFA_DEFAULT_PWX_OSPASSWORD unter Windows das Nur-Text-Passwort als Wert fest.
Weitere Informationen zum Festlegen von Umgebungsvariablen unter Windows finden Sie in der Windows-Dokumentation.

INFA_DEFAULT_SECURITY_DOMAIN

Die INFA_DEFAULT_SECURITY_DOMAIN-Umgebungsvariable gilt für das infacmd-Befehlszeilenprogramm.

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

INFA_DEFAULT_SECURITY_DOMAIN für die native Sicherheitsdomäne oder für einen LDAP-Sicherheitsdomänennamen festlegen.

Konfigurieren von INFA_DEFAULT_SECURITY_DOMAIN unter UNIX

So konfigurieren Sie INFA_DEFAULT_SECURITY_DOMAIN unter UNIX:

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

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

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

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

Konfigurieren von INFA_DEFAULT_SECURITY_DOMAIN unter Windows

So konfigurieren Sie INFA_DEFAULT_SECURITY_DOMAIN unter Windows:

- Geben Sie die Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN ein und legen Sie den Namen der Sicherheitsdomäne als Wert fest.

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

INFA_JAVA_CMD_OPTS

INFA_JAVA_CMD_OPTS Umgebungsvariable gilt für das infasetup-Befehlszeilenprogramm.

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

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

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

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

Konfigurieren von INFA_JAVA_CMD_OPTS unter UNIX

So konfigurieren Sie INFA_JAVA_CMD_OPTS unter UNIX:

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

  ```
  setenv INFA_JAVA_CMD_OPTS <Java_Options>
  ```

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

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

Konfigurieren von INFA_JAVA_CMD_OPTS unter Windows

So konfigurieren Sie INFA_JAVA_CMD_OPTS unter Windows:

▶ Geben Sie die Umgebungsvariable INFA_JAVA_CMD_OPTS ein und legen Sie die Java-Optionen wie die -Xmx-Werte und Systemeigenschaften fest.

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

INFA_PASSWORD

Die INFA_PASSWORD-Umgebungsvariable gilt für das infacmd- und das infasetup-Befehlszeilenprogramm.

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

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

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

1. Verwenden Sie das Befehlszeilenprogramm pmpasswd zum Verschlüsseln des Benutzerpassworts.

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

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

Verwandte Themen:

- "Verschlüsseln von Passwörtern" auf Seite 56

Konfigurieren von INFA_PASSWORD unter UNIX

So konfigurieren Sie INFA_PASSWORD unter UNIX:

1. Geben Sie an der Befehlszeile Folgendes ein:

   ```
   pmpasswd <password>
   ```

   pmpasswd gibt das verschlüsselte Passwort zurück.

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

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

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

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

Konfigurieren von INFA_PASSWORD unter Windows

So konfigurieren Sie INFA_PASSWORD unter Windows:

1. Geben Sie an der Befehlszeile Folgendes ein:

   ```
   pmpasswd <password>
   ```

   pmpasswd gibt das verschlüsselte Passwort zurück.

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

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

INFA_NODE_KEYSTORE_PASSWORD

Die Umgebungsvariable INFA_NODE_KEYSTORE_PASSWORD gilt für das infasetup-Befehlszeilenprogramm.

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

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

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

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

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

Konfigurieren von INFA_NODE_KEYSTORE_PASSWORD unter UNIX

So konfigurieren Sie INFA_NODE_KEYSTORE_PASSWORD unter UNIX:

1. Geben Sie an der Befehlszeile Folgendes ein:

   ```
   pmpasswd <database password>
   ```

   pmpasswd gibt das verschlüsselte Passwort zurück.

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

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

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

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

Konfigurieren von INFA_NODE_KEYSTORE_PASSWORD unter Windows

So konfigurieren Sie INFA_NODE_KEYSTORE_PASSWORD unter Windows:

1. Geben Sie an der Befehlszeile Folgendes ein:

   ```
   pmpasswd <database password>
   ```

   pmpasswd gibt das verschlüsselte Passwort zurück.

2. Geben Sie die Umgebungsvariable INFA_NODE_KEYSTORE_PASSWORD ein und legen Sie das *verschlüsselte* Passwort als Wert fest.

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

INFA_NODE_TRUSTSTORE_PASSWORD

Die Umgebungsvariable INFA_NODE_TRUSTSTORE_PASSWORD gilt für das infasetup-Befehlszeilenprogramm.

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

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

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

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

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

Konfigurieren von INFA_NODE_TRUSTSTORE_PASSWORD unter UNIX

So konfigurieren Sie INFA_NODE_TRUSTSTORE_PASSWORD unter UNIX:

1. Geben Sie an der Befehlszeile Folgendes ein:

   ```
   pmpasswd <database password>
   ```

   pmpasswd gibt das verschlüsselte Passwort zurück.

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

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

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

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

Konfigurieren von INFA_NODE_TRUSTSTORE_PASSWORD unter Windows

So konfigurieren Sie INFA_NODE_TRUSTSTORE_PASSWORD unter Windows:

1. Geben Sie an der Befehlszeile Folgendes ein:

   ```
   pmpasswd <database password>
   ```

   pmpasswd gibt das verschlüsselte Passwort zurück.

2. Geben Sie die Umgebungsvariable INFA_NODE_TRUSTSTORE_PASSWORD ein und legen Sie das *verschlüsselte* Passwort als Wert fest.

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

INFA_REPCNX_INFO

Die INFA_REPCNX_INFO-Umgebungsvariable gilt für das pmrep-Befehlszeilenprogramm.

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

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

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

Konfigurieren von INFA_REPCNX_INFO unter UNIX

So konfigurieren Sie INFA_REPCNX_INFO unter UNIX:

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

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

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

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

Konfigurieren von INFA_REPCNX_INFO unter Windows

So konfigurieren Sie INFA_REPCNX_INFO unter Windows:

- Geben Sie in einer DOS-Shell Folgendes ein:

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

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

INFA_REPOSITORY_PASSWORD

Die INFA_REPOSITORY_PASSWORD- Umgebungsvariable gilt für das infacmd-Befehlszeilenprogramm.

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

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

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

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

Verwandte Themen:

- "Verschlüsseln von Passwörtern" auf Seite 56

Konfigurieren von INFA_REPOSITORY_PASSWORD unter UNIX

So konfigurieren Sie INFA_REPOSITORY_PASSWORD unter UNIX:

1. Geben Sie an der Befehlszeile Folgendes ein:

   ```
   pmpasswd <password>
   ```

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

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

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

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

Konfigurieren von INFA_REPOSITORY_PASSWORD unter Windows

So konfigurieren Sie INFA_REPOSITORY_PASSWORD unter Windows:

1. Geben Sie an der Befehlszeile Folgendes ein:

   ```
   pmpasswd <repository password>
   ```

   pmpasswd gibt das verschlüsselte Passwort zurück.
2. Geben Sie die Umgebungsvariable INFA_REPOSITORY_PASSWORD ein und legen Sie das *verschlüsselte* Passwort als Wert fest.

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

INFATOOL_DATEFORMAT

Die INFATOOL_DATEFORMAT-Umgebungsvariable gilt für das pmcmd-Befehlszeilenprogramm.

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

Konfigurieren von INFATOOL_DATEFORMAT unter UNIX

So konfigurieren Sie INFATOOL_DATEFORMAT unter UNIX:

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

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

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

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

Konfigurieren von INFATOOL_DATEFORMAT unter Windows

So konfigurieren Sie INFATOOL_DATEFORMAT unter Windows:

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

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

Verschlüsseln von Passwörtern

Sie können Passwörter zum Erstellen einer Umgebungsvariable zur Verwendung mit infacmd, infasetup, pmcmd und pmrep oder zum Definieren eines Passworts in einer Parameterdatei verschlüsseln.

Beispielsweise können Sie die Repository- und Datenbankpasswörter für pmrep verschlüsseln, um Sicherheit bei der Verwendung von pmrep in Skripts zu gewährleisten. Anschließend können Sie eine Umgebungsvariable zum Speichern des verschlüsselten Passworts erstellen. Oder Sie können ein Passwort für ein Verbindungsobjekt einer relationalen Datenbank in einer Parameterdatei festlegen.

Verwenden Sie das Befehlszeilenprogramm pmpasswd zum Verschlüsseln von Passwörtern. Das pmpasswd-Dienstprogramm wird in folgendem Verzeichnis installiert:

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

Das pmpasswd-Dienstprogramm verwendet die folgende Syntax:

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

In der folgenden Tabelle werden die pmpasswd-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-	Passwort	Erforderlich. Das Passwort zum Verschlüsseln.
-e	CRYPT_DATA, CRYPT_SYSTEM	Optional. Verschlüsselungstyp: - CRYPT_DATA. Verwenden, um die in einer Parameterdatei festgelegten Verbindungsobjektpasswörter zu verschlüsseln. - CRYPT_SYSTEM. Für alle anderen Passwörter verwenden. Standardwert ist CRYPT_SYSTEM.

Verwenden eines Passworts als eine Umgebungsvariable

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

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

   pmpasswd generiert und zeigt das verschlüsselte Passwort an. Wenn Sie beispielsweise das Passwort "monday" eingeben, wird das Passwort als "f/wRb5PZsZnqESTDPeos7Q==" verschlüsselt.

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

Konfigurieren eines Passworts als Umgebungsvariable unter UNIX

So konfigurieren Sie ein Passwort als Umgebungsvariable unter UNIX:

1. Geben Sie an der Befehlszeile Folgendes ein:

   ```
   pmpasswd <password>
   ```

   pmpasswd gibt das verschlüsselte Passwort zurück.

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

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

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

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

   Sie können der Umgebungsvariable jeden gültigen UNIX-Namen zuweisen.

Konfigurieren eines Passworts als Umgebungsvariable unter Windows

So konfigurieren Sie ein Passwort als Umgebungsvariable unter Windows:

1. Geben Sie an der Befehlszeile Folgendes ein:

   ```
   pmpasswd <password>
   ```

   pmpasswd gibt das verschlüsselte Passwort zurück.

2. Geben Sie die Passwort-Umgebungsvariable im Variablenfeld ein. Geben Sie das Passwort *verschlüsselt* im Wertfeld ein.

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

Festlegen des Benutzernamens

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

Konfigurieren eines Benutzernamens als eine Umgebungsvariable unter UNIX

So konfigurieren Sie einen Benutzernamen als eine Umgebungsvariable unter UNIX:

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

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

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

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

  Sie können der Umgebungsvariable jeden gültigen UNIX-Namen zuweisen.

Konfigurieren eines Benutzernamens als eine Umgebungsvariable unter Windows

So konfigurieren Sie einen Benutzernamen als eine Umgebungsvariable unter Windows:

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

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

KAPITEL 5

Verwenden von infacmd

Dieses Kapitel umfasst die folgenden Themen:

- Verwenden von infacmd - Übersicht, 59
- infacmd-Befehlsprogramme, 60
- Ausführen von Befehlen, 61
- infacmd-Rückgabewerte, 62
- infacmd UpdateGatewayInfo, 62

Verwenden von infacmd - Übersicht

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

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

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

infacmd-Befehlsprogramme

Das infacmd-Programm unterstützt alle Informatica-Anwendungsdienste. Die Informatica-Domäne verfügt über separate infacmd-Programme für jeden Anwendungsdienst.

Die Befehlszeilenschnittstelle verfügt über die folgenden infacmd-Programme:

- infacmd advanced verwaltet erweiterte Funktionen wie Kontosperre und Plug-In-Validierung.
- infacmd as verwaltet Analyst Services.
- infacmd cms verwaltet Content Management Services.
- infacmd csm verwaltet die CSM-Diagnose.
- infacmd dis verwaltet Data Integration Services.
- Iinfacmd ide migriert alte Daten-Explorer-Objekte in Informatica Data Explorer.
- infacmd ipc exportiert Mappings aus dem Modellrepository in das PowerCenter Repository.
- infacmd isp verwaltet die Domäne, Sicherheit und PowerCenter-Anwendungsdienste.
- Infacmd isp aktualisiert die Konnektivitätsinformationen des Gateway-Knotens und gibt den Namen des Knotens zurück.
- infacmd mrs verwaltet Model Repository Services.
- infacmd ms listet bereitgestellte Mappings auf und führt diese aus.
- infacmd oie verwaltet das Exportieren von Objekten aus dem Modellrepository und das Importieren von Objekten in das Modellrepository.
- infacmd ps verwaltet die Profiling Warehouse-Inhalte, Profile und Scorecards.
- Infacmd ps erstellt oder löscht die Inhalte des Profiling Warehouse.
- infacmd pwx verwaltet PowerExchange Listener und Logger Services.
- infacmd rds verwaltet den Berichterstellungs- und Dashboard-Dienst.
- infacmd rms verwaltet den Ressourcenmanager-Dienst.
- infacmd rtm verwaltet Import- und Exportoperationen für Referenztabellendaten.
- infacmd sch verwaltet den Scheduler-Dienst.
- Infacmd search verwaltet den Suchdienst.
- infacmd sql verwaltet SQL-Datendienste, die Sie für den Data Integration Service bereitstellen.
- infacmd wfs verwaltet Arbeitsabläufe, die Sie für den Data Integration Service bereitstellen.
- infacmd ws verwaltet Web-Dienste, die Sie dem Data Integration Service bereitstellen.
- infacmd xrf verwaltet aus dem Modellrepository exportierte XML-Dateien.

infacmd ListPlugins

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

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

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

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

Ms ist beispielsweise die Plugin-ID für den Mapping Service des infacmd-Programms.

Um beispielsweise einen Befehl auszuführen, der die Zuordnungen in einer Anwendung auflistet, verwenden Sie den infacmd ms ListMappings-Befehl:

```
infacmd ms ListMappings -dn domain_name -un user_name -pd password -sdn security_domain -sn
service_name -a application_name
```

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

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

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

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

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

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

Ausführen von Befehlen

Rufen Sie infacmd über die Befehlszeile auf. Sie können Befehle direkt oder aus einem Skript, einer Batchdatei oder einem anderen Programm ausführen.

So führen Sie infacmd-Befehle aus:

1. Wechseln Sie an der Eingabeaufforderung zu dem Verzeichnis, in dem sich die ausführbare infacmd-Datei befindet.

   Standardmäßig wird infacmd in folgendem Installationsverzeichnis der Informatica-Dienste installiert: `<Informatica-Installationsverzeichnis>/isp/bin`

   Sie können infacmd auch über die Informatica Installations-DVD installieren.

2. Geben Sie `infacmd` unter Windows oder `infacmd.sh` unter UNIX gefolgt von der Plugin-ID, dem Befehlsnamen sowie den erforderlichen Optionen und Argumenten ein. Bei Befehlsnamen spielt die Groß- und Kleinschreibung keine Rolle.

   Beispiel:

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

Beim Ausführen von infacmd geben Sie Optionen für jeden Befehl gefolgt von den erforderlichen Argumenten ein. Die meisten Befehle erfordern beispielsweise die Eingabe des Passworts sowie des Domänen- und Benutzernamens mithilfe von Befehlsoptionen. Befehlsoptionen wird unter Missachtung der Groß-/Kleinschreibung ein Bindestrich vorangestellt. Argumente folgen der Option.

Zur Eingabe eines Arguments mit einem vorangestellten Bindestrich schließen Sie das Argument in Anführungszeichen ein und verwenden Sie den umgekehrten Schrägstrich (\) als Escape-Zeichen vor jedem

Anführungszeichen. Der folgende Befehl schreibt beispielsweise das Protokoll für die Zuordnungsausführung mit der Job-ID „-qnLI7G_TEeW9olHBkc9hoA“ in die Datei „MyLog.log“ im infacmd-Verzeichnis unter Windows:

```
infacmd ms GetRequestLog -dn MyDomain -sn MyDIS -un AdminUser -pd password -id \"-
qnLI7G_TEeW9olHBkc9hoA\" -f MyLog.log
```

Wenn Sie eine der erforderlichen Optionen weglassen oder falsch eingeben, schlägt der Befehl fehl und von infacmd wird eine Fehlermeldung zurückgegeben.

Sie können Umgebungsvariablen für bestimmte Befehlsoptionen mit infacmd verwenden. Sie können beispielsweise den Standardbenutzernamen und das Standardpasswort für eine Domäne als Umgebungsvariablen speichern, damit diese nicht mithilfe von Befehlsoptionen eingegeben werden müssen. Sie können beispielsweise den Standardbenutzernamen für eine Domäne als Umgebungsvariable speichern, damit dieser nicht mithilfe von Befehlsoptionen eingegeben werden muss. Konfigurieren Sie diese Variablen vor der Verwendung von infacmd.

infacmd-Rückgabewerte

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

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

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

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

infacmd UpdateGatewayInfo

Aktualisiert die Domäneninformationsdatei über die Befehlszeile.

Führen Sie infacmd isp UpdateGatewayInfo zum Erstellen einer domains.infa-Datei oder zum Aktualisieren einer domains.infa-Datei aus. Die Datei domains.infa enthält die Verbindungsdaten für einen Gateway-Knoten in einer Domäne zusammen mit der TLS- und Kerberos-Konfiguration der Domäne. Zu den Konnektivitätsinformationen gehören der Domänenname sowie Name und HTTP-Port des Domänenhosts.

Unter Umständen müssen Sie eine domains.infa-Datei erzeugen, um infacmd oie-Befehle auf einem Client-Computer auszuführen. Führen Sie zum Erzeugen der Datei "domains.infa" den infacmd isp UpdateGatewayInfo-Befehl aus. Der updateGatewayInfo-Befehl erzeugt eine domains.infa-Datei im DeveloperClient-Verzeichnis. Definieren Sie den Hostnamen und Port des Domänengateways, wenn Sie den Befehl ausführen.

Der infacmd UpdateGatewayInfo-Befehl verwendet die folgende Syntax:

```
UpdateGatewayInfo

<-DomainName|-dn> domain_name
```

```
<-GatewayAddress|-dg> domain_gateway_host:port

[<-Force|-f>]
```

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

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-GatewayAddress -dg	domain_gateway_host:port	Erforderlich. Geben Sie die Gateway-Adresse im folgenden Format ein: `domain_gateway_host:port`
-Force -f	-	Optional. Aktualisiert oder erstellt die Datei „domains.infa“ auch dann, wenn die Verbindung zur Domäne fehlschlägt. Die -Force-Option legt die Kerberos- und TLS-fähigen Optionen in der Datei „domains.infa“ als „false“ fest, wenn die Verbindung zur Domäne fehlschlägt. Wenn Sie die -Force-Option nicht angeben, aktualisiert der Befehl die Datei „domains.infa“ nicht, wenn die Verbindung zur Domäne fehlschlägt.

KAPITEL 6

infacmd as-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- CreateService, 64
- ListServiceOptions, 67
- ListServiceProcessOptions, 69
- UpdateServiceOptions, 71
- UpdateServiceProcessOptions, 73

CreateService

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

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

```
CreateService

<-DomainName|-dn> domain_name

<-NodeName|-nn> node_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-RepositoryService|-rs> model_repository_service_name]

[<-DataIntegrationService|-ds> data_integration_service_name]

[<-HumanTaskDataIntegrationService|-htds> human_task_data_integration_service_name]

[<-MetadataManagerService|-mm> metadata_manager_service_name]

[<-FlatFileCacheLocation|-ffl> flat_file_location]

[<-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
```

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

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Analyst-Dienst ausgeführt wird.
-ServiceName -sn	service_name	Erforderlich. Name des Analyst-Diensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositorys kompatibel sein. Der Name darf nicht länger als 230 Zeichen sein und keine führenden oder abschließenden Leerzeichen, Wagenrückläufe, Tabulatoren oder die folgenden Zeichen enthalten: `/ * ? < > " |`
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang. Standardwert ist „180 Sekunden“.
-RepositoryService -rs	model_repository_service_name	Optional. Name des Modellrepository-Dienst. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositorys kompatibel sein. Der Name darf nicht länger als 230 Zeichen sein und keine führenden oder abschließenden Leerzeichen, Wagenrückläufe, Tabulatoren oder die folgenden Zeichen enthalten: `/ * ? < > " |`
-DataIntegrationService -ds	data_integration_service_name	Optional. Der mit dem Analyst-Dienst verbundene Name des Datenintegrationsdiensts.
-HumanTaskDataIntegrationService -htds	human_task_data_integration_service_name	Optional. Datenintegrationsdienst, der Human-Tasks ausführt.
-MetadataManagerService -mm	metadata_manager_service_name	Optional. Der mit dem Analyst-Dienst verbundene Name des Metadata Manager-Diensts.
-FlatFileCacheLocation -ffl	flat_file_location	Optional. Vollständiger Pfad (ohne Domänenname) des Ordners, in dem die Einfachdateien zwischengespeichert werden sollen. Folgendes Format ist erforderlich: */parent_folder/child_folder*

Option	Argument	Beschreibung
-RepositoryUserName -au	model_repository_user_name	Erforderlich, wenn Sie einen Modellrepository-Dienst angeben. Benutzername für die Verbindung zum Modellrepository. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RepositorySecurityDomain -rssdn	model_repository_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Administrator-Benutzer gehört.
-RepositoryPassword -ap	model_repository_password	Erforderlich, wenn Sie einen Modellrepository-Dienst angeben. Benutzerpasswort für den Modellrepository-Dienst.
-BusinessGlossaryExportFileDirectory -bgefd	business_glossary_export_file_directory	Optional. Speicherort des Verzeichnisses zum Exportieren von Geschäftsglossardateien.
-HttpPort	http_port	Erforderlich. Portnummer für den Analyst-Dienst.

ListServiceOptions

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

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

```
ListServiceOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd as ListServiceOptions“ beschrieben:

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

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

ListServiceProcessOptions

Listet die Analyst-Dienst-Prozessoptionen auf.

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

```
ListServiceProcessOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd as ListServiceProcessOptions“ beschrieben:

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

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

UpdateServiceOptions

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

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

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

```
UpdateServiceOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-Options |-o> options]
```

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

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie den Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Options -o	options	Optional. Liste der zu konfigurierenden Optionen. Trennen Sie die einzelnen Optionen mit einem Leerzeichen. Führen Sie zum Anzeigen der Optionen den infacmd as ListServiceOptions-Befehl aus.

UpdateServiceProcessOptions

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

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

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

```
UpdateServiceProcessOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name

<-Options|-o> options
```

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

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

Option	Argument	Beschreibung
-NodeName -nn	node_name	Erforderlich. Knoten, auf dem der Analyst-Dienstprozess ausgeführt wird.
-Options -o	options	Erforderlich. Liste der zu konfigurierenden Optionen. Trennen Sie die einzelnen Optionen mit einem Leerzeichen. Führen Sie zum Anzeigen der Optionen den infacmd as ListServiceProcessOptions-Befehl aus.

KAPITEL 7

infacmd aud-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- getDomainObjectPermissions, 76
- getPrivilegeAssociation, 78
- getUserGroupAssociation, 80
- getUserGroupAssociationForRoles, 83
- getUsersPersonalInfo, 85

getDomainObjectPermissions

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

Benutzer mit der Administratorrolle können diesen Befehl ausführen.

Der Befehl „infacmd aud getDomainObjectPermissions“ verwendet folgende Syntax:

```
getDomainObjectPermissions

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<<-ExistingUserNames|-eu> existing_user_names|

<-ExistingGroupNames|-eg> existing_group_names>

[<-ExistingSecurityDomain|-esd> existing_security_domain]

[<-Format|-fm> format_TEXT_CSV]

[<-OutputFile|-lo> output_file_name]
```

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

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Name der Sicherheitsdomäne, die Sie erstellen möchten und zu dem der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Sie können einen Wert für -sdn angeben oder den Standardwert basierend auf dem Authentifizierungsmodus verwenden: - Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Standardwert ist „Native“. Zum Arbeiten mit der LDAP-Authentifizierung müssen Sie den Wert für -sdn angeben. - Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Standardwert ist „Native“ für native Authentifizierung. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
–Gateway –hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Geben Sie die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne an.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ExistingUserNames -eu	existing_user_names	Erforderlich, wenn Sie -ExistingGroupNames (-eg) nicht verwenden. Name des Benutzers oder einer Liste von Benutzern zum Ausführen der Berichte. Bei mehreren Benutzern trennen Sie jeden Benutzer durch ein Komma in der Befehlszeile.
-ExistingGroupNames -eg	existing_group_names	Erforderlich, wenn Sie -ExistingUserName (-eu) nicht verwenden. Name der Gruppe oder einer Liste mit Gruppen zum Ausführen der Berichte. Bei mehreren Benutzern trennen Sie jede Gruppe durch ein Komma in der Befehlszeile.
-ExistingSecurityDomain -esd	existing_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Sicherheitsdomäne, zu der der Benutzer oder die Gruppe gehört. Standardwert ist „Native“.
-Format -fm	format_TEXT_CSV	Optional. Format der Ausgabedatei. Gültige Typen umfassen: - Text - CSV Wenn Sie kein Format angeben, verwendet infacmd Textformat mit einer Zeilenlänge von 80 Zeichen.
-OutputFile -lo	output_file_name	Optional. Name und Dateipfad für die Ausgabedatei. Wenn Sie keinen Ausgabedateinamen angeben, zeigt infacmd die Protokollereignisse auf dem Bildschirm an.

getPrivilegeAssociation

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

Benutzer mit der Administratorrolle können diesen Befehl ausführen.

Der Befehl „infacmd aud getPrivilegeAssociation“ verwendet folgende Syntax:

```
getPrivilegeAssociation

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]
```

```
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<<-ExistingUserNames|-eu> existing_user_names|

<-ExistingGroupNames|-eg> existing_group_names>

[<-ExistingSecurityDomain|-esd> existing_security_domain]

[<-Format|-fm> format_TEXT_CSV]

[<-OutputFile|-lo> output_file_name]
```

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

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

Option	Argument	Beschreibung
–Gateway –hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ExistingUserNames -eu	existing_user_names	Erforderlich, wenn Sie -ExistingGroupNames (-eg) nicht verwenden. Name des Benutzers oder einer Liste von Benutzern zum Ausführen der Berichte. Bei mehreren Benutzern trennen Sie jeden Benutzer durch ein Komma in der Befehlszeile.
-ExistingGroupNames -eg	existing_group_names	Erforderlich, wenn Sie -ExistingUserName (-eu) nicht verwenden. Name der Gruppe oder einer Liste mit Gruppen zum Ausführen der Berichte. Bei mehreren Benutzern trennen Sie jede Gruppe durch ein Komma in der Befehlszeile.
-ExistingSecurityDomain -esd	existing_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Sicherheitsdomäne, zu der der Benutzer oder die Gruppe gehört. Standardwert ist „Native“.
-Format -fm	format_TEXT_CSV	Optional. Format der Ausgabedatei. Gültige Typen umfassen: - Text - CSV Wenn Sie kein Format angeben, verwendet infacmd Textformat mit einer Zeilenlänge von 80 Zeichen.
-OutputFile -lo	output_file_name	Optional. Name und Dateipfad für die Ausgabedatei. Wenn Sie keinen Ausgabedateinamen angeben, zeigt infacmd die Protokollereignisse auf dem Bildschirm an.

getUserGroupAssociation

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

Benutzer mit der Administratorrolle können diesen Befehl ausführen.

Der Befehl „infacmd aud getUserGroupAssociation“ verwendet folgende Syntax:

```
getUserGroupAssociation
```

```
<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<<-ExistingUserNames|-eu> existing_user_names|

<-ExistingGroupNames|-eg> existing_group_names>

[<-ExistingSecurityDomain|-esd> existing_security_domain]

[<-Format|-fm> format_TEXT_CSV]

[<-OutputFile|-lo> output_file_name]
```

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

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne die Kerberos-Authentifizierung verwendet, gilt der während der Installation festgelegte Benutzerbereichsname als Standardeinstellung.
–Gateway –hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ExistingUserNames -eu	existing_user_names	Erforderlich, wenn Sie -ExistingGroupNames (-eg) nicht verwenden. Name des Benutzers oder einer Liste von Benutzern zum Ausführen der Berichte. Bei mehreren Benutzern trennen Sie jeden Benutzer durch ein Komma in der Befehlszeile.
-ExistingGroupNames -eg	existing_group_names	Erforderlich, wenn Sie -ExistingUserName (-eu) nicht verwenden. Name der Gruppe oder einer Liste mit Gruppen zum Ausführen der Berichte. Bei mehreren Benutzern trennen Sie jede Gruppe durch ein Komma in der Befehlszeile.
-ExistingSecurityDomain -esd	existing_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Sicherheitsdomäne, zu der der Benutzer oder die Gruppe gehört. Standardwert ist „Native“.

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

getUserGroupAssociationForRoles

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

Benutzer mit der Administratorrolle können diesen Befehl ausführen.

Der Befehl „infacmd aud getUserGroupAssociationForRoles“ verwendet folgende Syntax:

```
getUserGroupAssociationForRoles

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-RoleNames|-en> role_names

[<-Format|-fm> format_TEXT_CSV]

[<-OutputFile|-lo> output_file_name]
```

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

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne die Kerberos-Authentifizierung verwendet, gilt der während der Installation festgelegte Benutzerbereichsname als Standardeinstellung.
–Gateway –hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-RoleNames -en	role_names	Erforderlich. Name der zugewiesenen Rolle für Benutzer oder Gruppen in der Domäne, für die Sie den Bericht generieren möchten. Bei mehreren Rollen trennen Sie jede Rolle durch ein Komma in der Befehlszeile.
-Format -fm	format_TEXT_CSV	Optional. Format der Ausgabedatei. Gültige Typen umfassen: - Text - CSV Wenn Sie kein Format angeben, verwendet infacmd Textformat mit einer Zeilenlänge von 80 Zeichen.
-OutputFile -lo	output_file_name	Optional. Name und Dateipfad für die Ausgabedatei. Wenn Sie keinen Ausgabedateinamen angeben, zeigt infacmd die Protokollereignisse auf dem Bildschirm an.

getUsersPersonalInfo

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

Benutzer mit der Administratorrolle können diesen Befehl ausführen.

Der Befehl „infacmd aud getUsersPersonalInfo“ verwendet folgende Syntax:

```
getUsersPersonalInfo

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<<-ExistingUserNames|-eu> existing_user_names|

<-ExistingGroupNames|-eg> existing_group_names>
```

```
[<-ExistingSecurityDomain|-esd> existing_security_domain]

[<-Format|-fm> format_TEXT_CSV]

[<-OutputFile|-lo> output_file_name]
```

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

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne die Kerberos-Authentifizierung verwendet, gilt der während der Installation festgelegte Benutzerbereichsname als Standardeinstellung.
–Gateway –hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ExistingUserNames -eu	existing_user_names	Erforderlich, wenn Sie -ExistingGroupNames (-eg) nicht verwenden. Name des Benutzers oder einer Liste von Benutzern zum Ausführen der Berichte. Bei mehreren Benutzern trennen Sie jeden Benutzer durch ein Komma in der Befehlszeile.
-ExistingGroupNames -eg	existing_group_names	Erforderlich, wenn Sie -ExistingUserName (-eu) nicht verwenden. Name der Gruppe oder einer Liste mit Gruppen zum Ausführen der Berichte. Bei mehreren Benutzern trennen Sie jede Gruppe durch ein Komma in der Befehlszeile.
-ExistingSecurityDomain -esd	existing_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Sicherheitsdomäne, zu der der Benutzer oder die Gruppe gehört. Standardwert ist „Native“.
-Format -fm	format_TEXT_CSV	Optional. Format der Ausgabedatei. Gültige Typen umfassen: - Text - CSV Wenn Sie kein Format angeben, verwendet infacmd Textformat mit einer Zeilenlänge von 80 Zeichen.
-OutputFile -lo	output_file_name	Optional. Name und Dateipfad für die Ausgabedatei. Wenn Sie keinen Ausgabedateinamen angeben, zeigt infacmd die Protokollereignisse auf dem Bildschirm an.

KAPITEL 8

Infacmd bg-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- upgradeRepository, 88
- listGlossary, 90
- exportGlossary, 91
- importGlossary, 95

upgradeRepository

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

Der infacmd bg upgradeRepository-Befehl verwendet die folgende Syntax:

```
upgradeRepository

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> Password

[<-SecurityDomain|-sdn> security_domain]

<-AtServiceName|-atn> Analyst_service_name
```

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

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne native, Kerberos- oder LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.
-Password -pd	Password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Optional, wenn die Domäne LDAP-Authentifizierung, native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
AtServiceName -atn	Analyst_service_name	Erforderlich. Name des Analyst-Diensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositorys kompatibel sein. Der Name darf maximal 230 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten: `/ * ? < > " |`

listGlossary

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

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

```
listGlossary

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> Password

[<-SecurityDomain|-sdn> security_domain]

<-AtServiceName|-atn> Analyst_service_name
```

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

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Optional, wenn die Domäne LDAP-Authentifizierung, native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne native, Kerberos- oder LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
AtServiceName -atn	Analyst_service_name	Erforderlich. Name des Analyst-Diensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositorys kompatibel sein. Der Name darf maximal 230 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten: `/ * ? < > " |`

exportGlossary

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

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

```
exportGlossary

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> Password

[<-SecurityDomain|-sdn> security_domain]

<-AtServiceName|-atn> Analyst_service_name

[<-GlossaryList|-gl> Glossary_list]

[<-Delimiter|-dl> Glossary_name_delimiter]

[<-IncludeCrossGlossaryLinks|-cgl> Include_cross_glossary_links_true_false]

[<-IncludeAuditHistory|-ah> Include_audit_history_true_false]

[<-IncludeAttachment|-att> Include_attachments_true_false]

[<-IncludeOnlyTemplate|-tem> Include_templates_only_true_false]
```

```
[<-status|-s> Status_of_assets]

[<-phase|-p> Phase_of_assets]

<-ExportFilePath|-ep> Export_path
```

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

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Optional, wenn die Domäne LDAP-Authentifizierung, native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne native, Kerberos- oder LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
AtServiceName -atn	Analyst_service_name	Erforderlich. Name des Analyst-Diensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositorys kompatibel sein. Der Name darf maximal 230 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten: `/ * ? < > " |`
-GlossaryList -gl	Glossary_list	Optional. Die Namen von einem oder mehreren Glossaren, die Sie exportieren möchten und auf die Sie gemäß der im Analyst Tool festgelegten Berechtigungen Zugriff haben. Trennen Sie bei mehreren Glossaren die Namen durch das benutzerdefinierte Delimiter-Zeichen. Wenn Sie die Namen der Glossare nicht angeben, exportiert das Analyst Tool alle Glossare, auf die Sie gemäß der im Analyst Tool festgelegten Berechtigungen Zugriff haben.

Option	Argument	Beschreibung
-Delimiter -dl	Glossary_name_delimiter	Optional. Geben Sie einen benutzerdefinierten Delimiter an, wenn Sie mehrere Glossare exportieren und eines davon das Standard-Delimiter-Zeichen im Glossarnamen enthält. Der Standard-Delimiter ist ein Komma. Definieren Sie einen benutzerdefinierten Delimiter mit maximal einem Sonderzeichen. Verwenden Sie den benutzerdefinierten Delimiter zum Trennen der Namen von mehreren Glossaren.
-IncludeCrossGlossaryLinks -cgl	Include_cross_glossary_links_true_false	Optional. Geben Sie einen der folgenden Werte ein: - `True`, um Querverweise des Glossars in die Exportdatei einzuschließen. - `False`, um Querverweise des Glossars in der Exportdatei zu überspringen. Standardwert ist „true“.
-IncludeAuditHistory -ah	Include_audit_history_true_false	Optional. Geben Sie einen der folgenden Werte ein: - `True`, um die Audit-Trail-Historie in die Exportdatei einzuschließen. - `False`, um die Audit-Trail-Historie in der Exportdatei zu überspringen. Standardwert ist „False“.
-IncludeAttachments -att	Include_attachments_true_false	Optional. Geben Sie einen der folgenden Werte ein: - `True`, um Anhänge in die Exportdatei einzuschließen. - Geben Sie `False` an, um Anhänge in der Exportdatei zu überspringen. Standardwert ist „False“.
-IncludeOnlyTemplates -tem	Include_only_templates_true_false	Optional. Geben Sie einen der folgenden Werte ein: - `True`, um nur Vorlagen in die Exportdatei einzuschließen. - `False`, um sowohl Vorlagen als auch Glossardaten in die Exportdatei einzuschließen. Standardwert ist „False“.

Option	Argument	Beschreibung
-status -s	Status_of_assets	Optional. Geben Sie einen oder alle der folgenden Werte durch ein Komma abgetrennt ein: - `Active`, um Objekte zu exportieren, die aktiv sind. - `Inactive`, um Objekte zu exportieren, die inaktiv sind. Das Analyst Tool exportiert Objekte, die sowohl aktiv als auch inaktiv sind, wenn Sie keinen Wert angeben.
-phase -p	Phase_of_assets	Optional. Geben Sie einen oder alle der folgenden Werte durch ein Komma abgetrennt ein: - `Draft`, um Objekte zu exportieren, die sich in der Phase „Entwurf“ befinden. - `In_Review`, um Objekte zu exportieren, die sich in der Phase „Überprüfung“ befinden. - `Published`, um Objekte zu exportieren, die sich in der Phase „Veröffentlicht“ befinden. - `Rejected`, um Objekte zu exportieren, die sich in der Phase „Abgelehnt“ befinden. - `Pending_publish`, um Objekte zu exportieren, die sich in der Phase „Zur Veröffentlichung ausstehend“ befinden. Das Analyst Tool exportiert Objekte, die sich in allen Phasen befinden, wenn Sie keinen Wert angeben.
-ExportFilePath -ep	Export_path	Erforderlich. Geben Sie den Pfad an, in dem das Befehlszeilenprogramm die exportierten Dateien speichern muss.

importGlossary

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

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

```
importGlossary

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> Password
```

```
[<-SecurityDomain|-sdn> security_domain]
 <-AtServiceName|-atn> Analyst_service_name
[<-GlossaryList|-gl> Glossary_list]
[<-Delimiter|-dl> Glossary_name_delimiter]
[<-IncludeCrossGlossaryLinks|-cgl> Include_cross_glossary_links_true_false]
[<-IncludeAuditHistory|-ah> Include_audit_history_true_false]
[<-IncludeAttachment|-att> Include_attachments_true_false]
[<-IncludeOnlyTemplate|-tem> Include_templates_only_true_false]
<-ImportFilePath|-ip> Import_path
[<-ResolutionOnMatchByName|-rmn> Copy_or_replace_or_skip_assets_by_name]
[<-ResolutionOnMatchById|-rmi> Copy_or_replace_or_skip_assets_by_id]
```

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

Option	Argument	Beschreibung
-DomainName -dn	Argument	Beschreibung
-UserName -un	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-Password -pd	Password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Optional, wenn die Domäne LDAP-Authentifizierung, native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne native, Kerberos- oder LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
AtServiceName -atn	Analyst_service_name	Erforderlich. Name des Analyst-Diensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositorys kompatibel sein. Der Name darf maximal 230 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten: `/ * ? < > " |`

Option	Argument	Beschreibung
GlossaryList -gl	Glossary_list	Optional. Die Namen von einem oder mehreren Glossaren, die Sie importieren möchten und auf die Sie gemäß der im Analyst Tool festgelegten Berechtigungen Zugriff haben. Die Glossare müssen sich in der XLSX-Datei befinden. Trennen Sie bei mehreren Glossaren die Namen durch das benutzerdefinierte Delimiter-Zeichen. Wenn Sie die Namen der Glossare nicht angeben, importiert das Analyst Tool alle Glossare, auf die Sie gemäß der im Analyst Tool festgelegten Berechtigungen Zugriff haben.
-Delimiter -dl	Glossary_name_delimiter	Optional. Geben Sie einen benutzerdefinierten Delimiter an, wenn Sie mehrere Glossare importieren und eines davon das Standard-Delimiter-Zeichen im Glossarnamen enthält. Der Standard-Delimiter ist ein Komma. Definieren Sie einen benutzerdefinierten Delimiter mit maximal einem Sonderzeichen. Verwenden Sie den benutzerdefinierten Delimiter zum Trennen der Namen von mehreren Glossaren.
IncludeCrossGlossaryLinks -cgl	Include_cross_glossary_links_true_false	Optional. Geben Sie einen der folgenden Werte ein: - `True`, um Querverweise des Glossars aus der Exportdatei zu importieren. - `False`, um das Importieren von Querverweisen des Glossars aus der Exportdatei zu überspringen. Standardwert ist „true“.

Option	Argument	Beschreibung
-IncludeAuditHistory -ah	Include_audit_history_true_false	Optional. Geben Sie einen der folgenden Werte ein: - `True`, um die Audit-Trail-Historie aus der Exportdatei zu importieren. - `False`, um das Importieren der Audit-Trail-Historie aus der Exportdatei zu überspringen. Standardwert ist „False“.
-IncludeAttachments -att	Include_attachments_true_false	Optional. Geben Sie einen der folgenden Werte ein: - `True`, um beim Importieren von Unternehmensglossaren Anhänge einzuschließen. - `False`, um beim Importieren von Unternehmensglossaren sowohl Vorlagen als auch Glossardaten einzuschließen. Standardwert ist „true“.
-IncludeOnlyTemplates -tem	Include_only_templates_true_false	Erforderlich. Geben Sie einen der folgenden Werte ein: - `True`, um beim Importieren von Unternehmensglossaren nur Vorlagen einzuschließen. - `False`, um beim Importieren von Unternehmensglossaren sowohl Vorlagen als auch Glossardaten einzuschließen. Standardwert ist „False“.
-ImportFilePath -ip	Import_path	Erforderlich. Geben Sie den Pfad an, in dem die Importdatei verfügbar ist.

Option	Argument	Beschreibung
-ResolutionOnMatchByName -rmn	Copy_or_replace_or_skip_assets_by_name	Optional. Geben Sie einen der folgenden Werte ein: - `Copy`, um alle Objekte zu kopieren, wenn ein auf dem Namen basierender Konflikt vorhanden ist. - `Replace`, um alle Objekte zu ersetzen, wenn ein auf dem Namen basierender Konflikt vorhanden ist. Dies ist der Standardwert. - `Skip`, um alle Objekte zu überspringen, wenn ein auf dem Namen basierender Konflikt vorhanden ist.
-ResolutionOnMatchById -rmi	Copy_or_replace_or_skip_assets_by_id	Optional. Geben Sie einen der folgenden Werte ein: - `Copy`, um alle Objekte zu kopieren, wenn ein auf der Objekt-ID basierender Konflikt vorhanden ist. - `Replace`, um alle Objekte zu ersetzen, wenn ein auf der Objekt-ID basierender Konflikt vorhanden ist. Dies ist der Standardwert. - `Skip`, um alle Objekte zu überspringen, wenn ein auf der Objekt-ID basierender Konflikt vorhanden ist.

KAPITEL 9

infacmd cms-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- CreateAuditTables, 101
- CreateService, 103
- DeleteAuditTables, 106
- ListServiceOptions, 108
- ListServiceProcessOptions, 110
- Löschen, 112
- RemoveService, 115
- ResyncData, 116
- UpdateServiceOptions, 118
- UpdateServiceProcessOptions, 120
- Upgrade, 122

CreateAuditTables

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

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

```
CreateAuditTables

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

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

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

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

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

CreateService

Erstellt einen Content-Managementdienst in einer Domäne.

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

```
CreateService

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name

<-DataServer|-ds> data_service_name

<-RepositoryService|-rs> repository_service_name

<-RepositoryUsername|-rsu> repository_user_name

<-RepositoryPassword|-rsp> repository_password
```

```
[<-RepositorySecurityDomain|-rssd> repository_security_domain]
<-ReferenceDataLocation|-rdl> reference_data_location
[<-HttpPort> http_port]
[<-HttpsPort> https_port]
[<-KeystoreFile|-kf> keystore_file_location]
[<-KeystorePassword|-kp> keystore_password]
```

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

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

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

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

DeleteAuditTables

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

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

```
DeleteAuditTables

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

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

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

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

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

ListServiceOptions

Listet die Optionen für einen Content Management Service auf.

Der Befehl infacmd cms ListServiceOptions verwendet die folgende Syntax:

```
ListServiceOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

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

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

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

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

ListServiceProcessOptions

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

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

```
ListServiceProcessOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name
```

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

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

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

Löschen

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

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

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

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

- Der im Befehl angegebene Benutzername verfügt über die Berechtigung zum Verwalten von Diensten in der Domäne.
- Der vom Content-Managementdienst angegebene Modellrepository-Benutzer weist im Modellrepository-Dienst die Administratorrolle auf.
- Alle Datenintegrationsdienste, die mit dem Modellrepository verbunden sind, stehen zur Verfügung.
- Im Referenzdaten-Warehouse finden aktuell keine Datenvorgänge statt.
- Das Referenzdaten-Warehouse speichert Daten für die Referenztabellenobjekte in einem einzelnen Modellrepository.
- Sie haben den Suchindex aktualisiert, der vom Modellrepository-Dienst zur Angabe der Objekte im Modellrepository verwendet wird. Aktualisieren Sie den Index, um sicherzustellen, dass der Modellrepository-Dienst die aktuelle Liste mit Referenztabellenobjekten im Referenzdaten-Warehouse verwendet.

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

```
Purge

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password
```

```
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

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

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

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

Aktualisieren des Suchindexes des Modellrepository

Aktualisieren Sie vor dem Ausführen von „infacmd cms Purge“ den Suchindex, den der Modellrepository-Dienst zur Identifizierung der Objekte im Modellrepository verwendet. Aktualisieren Sie den Index, um sicherzustellen, dass der Modellrepository-Dienst die aktuellen Referenztabellenobjekte im Repository identifizieren kann.

Die für die Neuindizierung benötigte Zeit hängt von der Anzahl der Objekte im Modellrepository ab. Sie sollten den Suchindex zu einem Zeitpunkt aktualisieren, zu dem möglichst wenige Benutzer angemeldet sind. Während der Neuindizierung sind Entwicklungszeitobjekte im Modellrepository schreibgeschützt.

1. Klicken Sie im Administrator Tool auf **Verwalten** > **Dienste und Knoten**.
2. Wählen Sie im Domänennavigator den Modellrepository-Dienst aus.
3. Klicken Sie auf der Registerkarte **Verwalten** auf **Aktionen** > **Suchindex** > **Erneute Indizierung**.

RemoveService

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

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

```
RemoveService

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

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

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

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

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

ResyncData

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

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

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

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

```
ResyncData

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

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

```
<-Type|-t> type
<-StartTime|-st> start_time
```

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

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie den Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Type -t	type	Erforderlich. Identifiziert den Datendateityp zum Kopieren vom Master-Content-Managementdienst-Rechner aus. Geben Sie eine der folgenden Optionen ein: - NER. Gibt probabilistische Modelldatendateien an. - Klassifizierer. Gibt klassifizierende Modelldatendateien an.
-StartTime -st	start_time	Erforderlich. Identifiziert die Dateien zum Kopieren vom Master-Content-Managementdienst-Rechner auf den Content-Managementdienst-Rechner, den Sie in der Eigenschaft ServiceName angeben. Mit dem Befehl werden nur Dateien kopiert, die einen späteren Zeitstempel als den Wert StartTime haben. Der Befehl verwendet die Systemuhr im Master-Content-Managementdienst-Rechner, um die Uhrzeit festzustellen. Geben Sie das Datum im lokalen Standardformat ein.

UpdateServiceOptions

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

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

```
UpdateServiceOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Options|-o> options
```

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

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

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

Benutzername- und Passwort-Optionen

Sie können die Option „UpdateServiceProcessOptions -o“ verwenden, um den Benutzernamen und das Passwort zu aktualisieren, welche der Content-Managementdienst nutzt, um eine Verbindung zum Modellrepository-Dienst herzustellen.
Verwenden Sie die Optionen RepositoryUsername und DataServiceOptions.RepositoryPassword zum Aktualisieren der Werte von Benutzername und Passwort. Sie können die Werte auch im Informatica Administrator einstellen.

Option des Referenzdaten-Speicherorts

Sie können die Option UpdateServiceProcessOptions -o zum Aktualisieren des Pfades zum Staging-Verzeichnis der Referenzdaten verwenden. Der Content-Managementdienst verwendet das Verzeichnis zum Staging von Daten, das er einer Referenztabelle hinzufügt.

Verwenden Sie die Option FileTransferOptions.TempLocation, um den Verzeichnisspeicherort für das Staging zu aktualisieren. Sie können den Speicherort auch im Informatica Administrator einstellen.

UpdateServiceProcessOptions

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

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

```
UpdateServiceProcessOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

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

```
<-NodeName|-nn> node_name
```

```
<-Options|-o> options
```

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

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie den Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Dienstprozess ausgeführt wird.
-Options -o	options	Erforderlich. Geben Sie jede zu aktualisierende Option und jeden zu aktualisierenden Wert ein. Trennen Sie jede Option mit einem Leerzeichen. Zum Anzeigen der Anwendungsoptionen führen Sie den Befehl infacmd cms ListServiceProcessOptions aus.

Optionen für Identitätsvergleichsanalyse

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

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

Sie können die Eigenschaften auch im Informatica Administrator einstellen.

Upgrade

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

Der Befehl infacmd cms Upgrade verwendet die folgende Syntax:

```
Upgrade

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

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

Der Befehl infacmd cms Upgrade prüft die Dienstkonfiguration auf der Domäne und überprüft die folgenden Dienstoptionen:

Master-Content Management Service

Der Upgrade-Befehl überprüft, dass das Modellrepository in der Domäne einen Master-Content Management Service verwendet. Wenn der Model Repository Service keinen Master-Content Management Service angibt, dann stellt der Upgrade Befehl den aktuellen Dienst als Master-Content Management Service ein. Standardmäßig wird der erste Content Management Service, der sich mit einem Model Repository Service verbindet, zum Master-Content Management Service.

Model Repository Service

Der Upgrade-Befehl verwendet den Data Integration Service, der mit dem Content Management Service verbunden ist, um den Model Repository Service in der Domäne zu ermitteln.

Der Upgrade-Befehl überprüft, ob der Content Management Service einen gültigen Benutzernamen, ein gültiges Passwort und eine Sicherheitsdomäne hat, um eine Verbindung zum Model Repository Service herzustellen. Wenn diese Optionen sind nicht eingestellt sind, verwendet der Upgrade-Befehl die Werte von Benutzernamen, Passwort und Sicherheitsdomäne im verbundenen Data Integration Service, um eine Verbindung zum Model Repository Service herzustellen.

Referenzdaten-Speicherort

Der Upgrade-Befehl überprüft, ob der Content Management Service einen Referenzdaten-Speicherort angibt. Wenn der Dienst keinen Referenzdaten-Speicherort angibt, stellt der Upgrade-Befehl den Speicherort auf die Staging-Datenbank ein, die im Analyst Service definiert ist.

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

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

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

KAPITEL 10

infacmd dis-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- AddParameterSetEntries, 126
- BackupApplication, 128
- CancelDataObjectCacheRefresh, 130
- CreateService, 132
- DeleteParameterSetEntries, 135
- DeployApplication, 137
- ListApplicationObjectPermissions, 139
- ListApplicationObjects, 141
- ListApplicationOptions, 143
- ListApplications, 145
- ListComputeOptions, 146
- ListDataObjectOptions, 148
- ListParameterSetEntries, 150
- ListParameterSetObjects, 152
- ListParameterSets, 154
- ListSequenceObjectProperties, 155
- ListSequenceObjects, 157
- ListServiceOptions, 159
- ListServiceProcessOptions, 161
- PurgeDataObjectCache, 162
- PurgeResultSetCache, 165
- RefreshDataObjectCache, 166
- RenameApplication, 168
- RestoreApplication, 170
- SetApplicationPermissions, 172
- SetApplicationObjectPermissions, 174
- SetSequenceState, 177
- StartApplication, 179
- StopApplication, 181
- stopBlazeService, 183

- UndeployApplication, 185
- UpdateApplication, 186
- UpdateApplicationOptions, 188
- UpdateComputeOptions, 190
- UpdateDataObjectOptions, 192
- UpdateParameterSetEntries, 195
- UpdateServiceOptions , 197
- UpdateServiceProcessOptions , 210

AddParameterSetEntries

Fügt einem Parametersatz Einträge hinzu. Führen Sie diesen Befehl aus, um Parameter aus einer Zuordnung oder einem Arbeitsablauf hinzuzufügen, der als Anwendung bereitgestellt wurde.

Der infacmd dis AddParameterSetEntries-Befehl verwendet die folgende Syntax:

```
AddParameterSetEntries

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Application|-a> application

<-parameterSetName|-ps> parameter set name

<-projectScope|-prs> path to the mapping or workflow that contains the parameters. For a
mapping, M1, in project P1 and folder F1, the path is P1/F1/mapping/M1.

<-paramNameValues|-pnv> parameter name-value pairs, separated by space
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis AddParameterSetEntries“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.

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

Option	Argument	Beschreibung
-projectScope -prs	project scope	Erforderlich. Pfad der Zuordnung oder des Arbeitsablaufs, der die Parameter enthält. Für die Zuordnung M1 in Projekt P1 und Ordner F1 lautet der Pfad: P1/F1/Zuordnung/M1.
-paramNames -pnv	parameter names	Erforderlich. Namen-Wert-Paare des Parameters getrennt durch Leerzeichen. Setzen Sie Namen-Wert-Paare in doppelte Anführungszeichen. Versehen Sie jeden Wert mit einfachen Anführungszeichen. Verwenden Sie folgende Syntax: `"parm1='valueA'" "parm2='valueB'" "parm3='valueC"` . Sie können Leerzeichen in einem Parameterwert verwenden. Sie können ein Apostroph (') oder einen Doppelpunkt (:) im Wert verwenden, wenn Sie für diese Zeichen einen umgekehrten Schrägstrich (\) als Escape-Zeichen verwenden. `'C:\Verzeichnis'`

BackupApplication

Sichert eine bereitgestellte Anwendung aus einem Datenintegrationsdienst in einer XML-Datei.

Die Backup-Datei enthält alle Eigenschafteneinstellungen für die Anwendung. Sie können die Anwendung in einem anderen Datenintegrationsdienst wiederherstellen. Sie müssen die Anwendung beenden, bevor Sie sie sichern.

Der Befehl „infacmd dis BackupApplication“ verwendet die folgende Syntax:

```
BackupApplication

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Application|-a> application

<-FileName|-f> file_name
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd dis BackupApplication“ beschrieben:

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

Option	Argument	Beschreibung
-Application -a	anwendung	Erforderlich. Name der zu sichernden Anwendung.
Filename -f	file_name	Erforderlich. Name und Dateipfad der Backup-Datei für die Anwendung.

CancelDataObjectCacheRefresh

Stoppt die letzte Anfrage zum Aktualisieren des logischen Datenobjekt-Cache. Wenn das Cache-Mapping ausgeführt wird, stoppt der Befehl die aktuelle Anfrage, um den logischen Datenobjekt-Cache zu aktualisieren. Zukünftige periodische Anfragen zum Aktualisieren des logischen Datenobjekt-Cache sind davon nicht betroffen.

Der Befehl „infacmd dis CancelDataObjectCacheRefresh“ verwendet die folgende Syntax:

```
CancelDataObjectCacheRefresh

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-Application|-a> application

<-Folder|-f> folder

<-DataObject|-do> data_model.data_object
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd dis CancelDataObjectCacheRefresh“ beschrieben:

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

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdienst.
Application -a	application	Erforderlich. Name der Anwendung.
-Folder -f	folder	Ordner in der Anwendung, die das Datenobjekt enthält.
-DataObject -do	data_model.data_object	Erforderlich. Name des logischen Datenobjekts. Der Name muss die folgende Syntax aufweisen: `<data_model>.<data_object>`

CreateService

Erstellt einen Datenintegrationsdienst. Der Datenintegrationsdienst wird standardmäßig aktiviert, wenn Sie ihn erstellen.

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

```
CreateService

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name | <-GridName|-gn> grid_name

[<-BackupNodes|-bn> node_name1,node_name2,...]

<-RepositoryService|-rs> model_repository_service_name

<-RepositoryUserName|-rsun> model_repository_user_name

<-RepositoryPassword|-rspd> model_repository_password

[<-RepositorySecurityDomain|-rssdn> model_repository_security_domain]

[<-HttpPort> http_port]

[<-HttpsPort> https_port]

[<-KeystoreFile|-kf> keystore_file_location]

[<-KeystorePassword|-kp> keystore_password]

[<-httpProtocolType|-pt> http_protocol_type]
```

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

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdienst. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codeseite des verbundenen Repositorys kompatibel sein. Der Name darf nicht länger als 230 Zeichen sein und keine Leerzeichen, Wagenrückläufe, Tabulatoren oder die folgenden Zeichen enthalten: `/ * ? < > " |`
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-NodeName -nn	node_name	Erforderlich, wenn Sie den Gitternamen nicht angeben. Knoten, auf dem der Datenintegrationsdienst ausgeführt wird. Sie können den Datenintegrationsdienst auf einem Knoten oder Gitter ausführen.
-GridName -gn	grid_name	Erforderlich, wenn Sie den Knotennamen nicht angeben. Gitter, in dem der Datenintegrationsdienst ausgeführt wird. Sie können den Datenintegrationsdienst auf einem Knoten oder Gitter ausführen.
-BackupNodes -bn	node_name1,node_name2,...	Optional. Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist. Sie können Sicherungsknoten konfigurieren, wenn Sie hohe Verfügbarkeit haben.
-RepositoryService -rs	model_repository_service_name	Modellrepository-Dienst, der Laufzeit-Metadaten speichert, die zur Ausführung der Mappings und SQL-Datendienste erforderlich sind.
-RepositoryUserName -rsun	model_repository_user_name	Benutzername zum Zugriff auf den Modellrepository-Dienst.
-RepositoryPassword -rspd	model_repository_password	Benutzerpasswort zum Zugriff auf den Modellrepository-Dienst.
-RepositorySecurityDomain -rssdn	model_repository_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer des Modellrepository gehört.
-HttpPort	http_port	Erforderlich, wenn Sie keinen HTTPS-Port angeben. Eindeutige HTTP-Portnummer, die für jeden Datenintegrationsdienst-Prozess verwendet wird. Nachdem Sie den Dienst erstellt haben, können Sie unterschiedliche Portnummern für jeden Datenintegrationsdienst-Prozess definieren. Der Standardwert ist 8095.
-HttpsPort	https_port	Erforderlich, wenn Sie keinen HTTP-Port angeben. Eindeutige HTTPS-Portnummer wird für jeden Datenintegrationsdienst-Prozess verwendet. Nachdem Sie den Dienst erstellt haben, können Sie unterschiedliche Portnummern für jeden Datenintegrationsdienst-Prozess definieren.

Option	Argument	Beschreibung
-KeystoreFile -kf	keystore_file_location	Pfad und Dateiname der Schlüsselspeicherdatei, die die Schlüssel und Zertifikate enthält, die zur Verwendung des HTTPS-Protokolls für den Datenintegrationsdienst erforderlich sind. Sie können eine Schlüsselspeicherdatei mit einem Keytool erstellen. Keytool ist ein Dienstprogramm, das private oder öffentliche Schlüsselpaare und verknüpfte Zertifikate in einer Schlüsselspeicherdatei generiert und speichert. Sie können das selbstsignierte Zertifikat oder ein von einer Zertifizierungsbehörde signiertes Zertifikat verwenden. Wenn Sie den Datenintegrationsdienst auf einem Gitter ausführen, muss die Schlüsselspeicherdatei auf jedem Knoten im Gitter die gleichen Schlüssel enthalten.
-KeystorePassword -kp	keystore_password	Passwort für die Schlüsselspeicherdatei.
-httpProtocolType -pt	http_protocol_type	Sicherheitsprotokoll, das vom Datenintegrationsdienst verwendet wird. Geben Sie einen der folgenden Werte ein: - HTTP. Anfragen an den Dienst müssen eine HTTP-URL verwenden. - HTTPS. Anfragen an den Dienst müssen eine HTTPS-URL verwenden. - Both. Anfragen an den Dienst, die entweder eine HTTP- oder eine HTTPS-URL verwenden können. Wenn Sie den HTTP-Protokolltyp auf HTTPS oder Both einstellen, aktivieren Sie TLS (Transport Layer Security) für den Dienst. Sie können TLS auch für jeden Webdienst aktivieren, der einer Anwendung bereitgestellt ist. Wenn Sie HTTPS für den Data Integration Service und TLS für den Webdienst aktivieren, verwendet der Webdienst eine HTTPS-URL. Wenn Sie HTTPS für den Data Integration Service und nicht für den Webdienst aktivieren, kann der Webdienst eine HTTP-URL oder eine HTTPS-URL nutzen. Wenn Sie TLS für einen Webdienst aktivieren, aber HTTPS nicht für den Data Integration Service aktivieren, startet der Webdienst nicht. Der Standardwert ist HTTP.

DeleteParameterSetEntries

Löscht Einträge aus einem Parametersatz. Führen Sie diesen Befehl aus, um Parametersatzeinträge für eine Zuordnung oder einen Arbeitsablauf zu löschen, der als Anwendung bereitgestellt wurde. Sie können bestimmte oder alle Parametersatzeinträge löschen.

Wenn ein zu löschender Parameter nicht im Parametersatz vorhanden ist, gibt infacmd eine Warnmeldung zurück. Die Meldung gibt an, dass der Parameter nicht gelöscht wird, weil er nicht im Parametersatz vorhanden ist.

Der infacmd dis DeleteParameterSetEntries-Befehl verwendet die folgende Syntax:

```
DeleteParameterSetEntries

<-DomainName|-dn> domain_name
```

```
<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Application|-a> application

<-parameterSetName|-ps> parameter set name

<-projectScope|-prs> path to the mapping or workflow that contains the parameters

<-paramNames|-pnv> parameter names to delete, separated by spaces. For a mapping, M1, in
project P1 and folder F1, the path is P1/F1/mapping/M1.

<-all|> Delete all the parameters in the project scope.
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis DeleteParameterSetEntries“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	application	Erforderlich. Name der Anwendung, die den Parametersatz enthält.
parametersetname - ps	parameterset name	Erforderlich. Name des Parametersatzes.
-projectScope -prs	project scope	Erforderlich. Pfad der Zuordnung oder des Arbeitsablaufs, der die Parameter enthält. Für die Zuordnung M1 in Projekt P1 und Ordner F1 lautet der Pfad: P1/F1/Zuordnung/M1.
-paramNames -pnv	parameter names	Erforderlich. Durch Leerzeichen getrennte Namen von Parametersätzen, die gelöscht werden sollen. Verwenden Sie zum Löschen aller Parameter statt dieser Option die Option -all.
-all	all	Löschen Sie alle Parameter im Parametersatz.

DeployApplication

Stellt einem Datenintegrationsdienst eine Anwendung bereit.

Der Befehl „infacmd dis DeployApplication“ verwendet die folgende Syntax:

```
DeployApplication
```

```
<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-FileName|-f> file_name

<-Application|-a> application
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis DeployApplication“ beschrieben:

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

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

ListApplicationObjectPermissions

Listet die Berechtigungen auf, über die ein Benutzer bzw. eine Gruppe für ein Anwendungsobjekt verfügt, wie z. B. ein Mapping oder ein Arbeitsablauf.

Der Befehl „infacmd dis ListApplicationObjectPermissions“ verwendet die folgende Syntax:

```
ListApplicationPermissions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

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

```
<-Application|-a> application_name

<-ApplicationObjectType|-t> application_object_type_Mapping_Workflow

<-ApplicationObject|-ao> application_object_name

<<-Direct> direct_permission_only|<-Effective> effective_permission_only>
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis ListApplicationPermissions“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	application_name	Erforderlich. Name der Anwendung.
-ApplicationObjectType -t	application_object_type	Erforderlich. Typ des Anwendungsobjekttyps. Geben Sie einen der folgenden Werte ein: - Mapping - Arbeitsablauf
-ApplicationObject -ao	application_object_name	Erforderlich. Name des Anwendungsobjekts.
-Direct | -Effective	direct | effective	Erforderlich. Ebene der aufzulistenden Berechtigungen. Direkte Berechtigungen sind Berechtigungen, die dem Benutzer oder der Gruppe direkt zugewiesen werden. Effektive Berechtigungen umfassen direkte Berechtigungen und geerbte Berechtigungen.

ListApplicationObjects

Listet die Objekte auf, die eine Anwendung enthält.

Wenn Sie die Option -ListObjectTypes verwenden, listet der Befehl auch den Typ jedes Objekts auf.

Der infacmd dis ListApplicationObjects-Befehl verwendet die folgende Syntax:

```
ListApplicationObjects
[<-DomainName|-dn> domain_name]
[<-DomainAddress|-da> domain_address. syntax - host:port]
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application
[<-ObjectType|-t> object_type]
[<-ListObjectType|-lt> list_object_type]
[<-PageSize|-ps> page_size]
[<-PageIndex|-pi> page_index]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis ListApplicationObjects“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	application	Erforderlich. Name der Anwendung.
-ObjectType -t	object_type	Optional. Typ des aufzulistenden Objekts. Sie können diese Option zum Filtern der Ergebnisse nach Objekttyp verwenden.
-ListObjectType -lt	true | false	Optional. Geben Sie einen der folgenden Werte ein: - True - Falsch
-PageSize -ps	page_size	Erforderlich, wenn Sie die Option „PageIndex“ angeben. Die Anzahl der anzuzeigenden Ergebnisse in jeder Gruppe. Wenn Sie eine Seitengröße angeben, verwalten Sie Befehlsergebnisse in Gruppen. Wenn Sie beispielsweise `-PageSize 5` angeben, gibt der Befehl Ergebnisse in Fünfer- oder kleineren Gruppen zurück.
-PageIndex -pi	page_index	Optional. Beginnend mit null, die Anzahl der anzuzeigenden Seitenergebnisse. Wenn Sie beispielsweise `-PageSize 5 -PageIndex 0` angeben, gibt der Befehl die erste Seite mit fünf Ergebnissen zurück, die Ergebnisse eins bis fünf. Wenn Sie diese Option auslassen, gibt der Befehl die erste PageSize mit Ergebnissen zurück. Standardwert ist Null.

ListApplicationOptions

Listet die Eigenschaften für eine Anwendung auf.

Der Befehl „infacmd dis ListApplicationOptions“ verwendet die folgende Syntax:

```
ListApplicationOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]
```

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

<-Application|-a> application
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis ListApplicationOptions“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	anwendung	Erforderlich. Name der Anwendung.

ListApplications

Listet die Anwendungen auf, die in einem Datenintegrationsdienst bereitgestellt werden.

Der Befehl „infacmd dis ListApplications“ verwendet die folgende Syntax:

```
ListApplications

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis ListApplications“ beschrieben:

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

Option	Argument	Beschreibung
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, für den Anwendungen aufgelistet werden sollen.

ListComputeOptions

Listet Eigenschaften des Datenintegrationsdiensts für einen Knoten mit der Berechnungsrolle auf.

Der infacmd dis ListComputeOptions-Befehl verwendet die folgende Syntax:

```
ListComputeOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password
```

```
[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „dis ListComputeOptions“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
NodeName -nn	node_name	Erforderlich. Knoten mit der Berechnungsrolle, die dem Datenintegrationsdienst oder dem Datenintegrationsdienstgitter zugewiesen ist.

ListDataObjectOptions

Listet Eigenschaften eines Datenobjekts auf.

Der Befehl „infacmd dis ListDataObjectOptions“ verwendet die folgende Syntax:

```
ListDataObjectOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Application|-a> application

<-Folder|-f> folder

<-DataObject|-do> data_model.data_object
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis ListDataObjectOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdienst.

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

Option	Argument	Beschreibung
-Folder -f	folder	Erforderlich. Repository-Ordner, der das Datenobjekt enthält.
DataObject -do	data_model.data_object	Erforderlich. Name des Datenobjekts.

ListParameterSetEntries

Listet die Einträge in einem Parametersatz auf.

Der infacmd dis ListParameterSetEntries-Befehl verwendet die folgende Syntax:

```
ListParameterSetEntries

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Application|-a> application

<-parameterSetName|-ps> parameter set name

<-projectScope|-prs> path to the mapping or workflow that contains the parameters. For a
mapping, M1, in project P1 and folder F1, the path is P1/F1/mapping/M1.
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis ListParameterSetEntries“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.

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

Option	Argument	Beschreibung
parametersetname - ps	parameterset name	Erforderlich. Name des Parametersatzes.
-projectScope -prs	project scope	Erforderlich. Pfad der Zuordnung oder des Arbeitsablaufs, der die Parameter enthält. Für die Zuordnung M1 in Projekt P1 und Ordner F1 lautet der Pfad: P1/F1/Zuordnung/M1.

ListParameterSetObjects

Listet die Objekte in einem bestimmten Parametersatz auf.

Der infacmd dis ListParameterSetObjects-Befehl verwendet die folgende Syntax:

```
ListParameterSetObjects

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Password|-ps> parameter set

<-Application|-a> application that contains the parameter set
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis ListParameterSetObjects“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.

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

ListParameterSets

Listet die Parametersätze in einer Anwendung auf.

Der infacmd dis ListParameterSets-Befehl verwendet die folgende Syntax:

```
ListParameterSets

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Application|-a> application
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis ListParameterSets“ beschrieben:

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

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

ListSequenceObjectProperties

Listet die Eigenschaften für ein Sequenzdatenobjekt auf.

Der Befehl „infacmd dis listsequenceobjectproperties“ verwendet die folgende Syntax:

```
ListSequenceObjectProperties
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application
<-SequenceObjectPath|-sop> sequence_object_path
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis ListSequenceObjectProperties“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Integrationsdiensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositorys kompatibel sein. Der Name darf nicht länger als 230 Zeichen sein und keine voran- bzw. nachgestellten Leerzeichen, Wagenrückläufe, Tabulatoren oder folgende Zeichen enthalten: / * ? < > " |
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	application	Erforderlich. Name der Anwendung.
-SequenceObjectPath -sop	Sequenzobjekt-Pfad	Erforderlich. Pfad zum Sequenzdatenobjekt. Der Pfad muss die folgenden Objekte in der angegebenen Reihenfolge enthalten, sofern zutreffend: - Projekt - Ordner - SQL-Datendienst oder Webdienst - Mapping - Sequenzgeneratorumwandlung - Sequenzdatenobjekt Befindet sich das Sequenzdatenobjekt in einem Mapping, SQL-Datendienst oder Webdienst, müssen Sie vor dem Mapping-, SQL-Datendienst- oder Webdienstnamen ein Präfix angeben. Verwenden Sie die folgenden Präfixe mit Optionen im Befehl: - Mapping:<Mapping-Name> - SQLDS:<SQL-Datendienstname> - WS:<Webdienstname> Trennen Sie die Optionen mit einem Schrägstrich (/). Beispiel: `<Projektname>/<Ordner>/SQLDS:<SQL-Datendienstname>/Mapping:<virtuelle Tabellenzuordnung>/<Sequenzgenerator-Umwandlung>/<Sequenzdatenobjekt-Name>`

.

ListSequenceObjects

Listet die für eine Anwendung bereitgestellten Sequenzdatenobjekte auf.

Der Befehl „infacmd dis ListSequenceObjects“ verwendet die folgende Syntax:

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis ListSequenceObjects“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Integrationsdiensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codeseite des verbundenen Repositorys kompatibel sein. Der Name darf nicht länger als 230 Zeichen sein und keine Leerzeichen, Wagenrückläufe, Tabulatoren oder die folgenden Zeichen enthalten: / * ? < > " |
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	anwendung	Erforderlich. Name der Anwendung.

.

ListServiceOptions

Listet die Eigenschaften für einen Datenintegrationsdienst auf.

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

```
ListServiceOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis ListServiceOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdienst.

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

ListServiceProcessOptions

Listet die Eigenschaften eines Datenintegrationsdienst-Prozesses auf.

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

```
ListServiceProcessOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis ListServiceProcessOptions“ beschrieben:

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

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

.

PurgeDataObjectCache

Bereinigt den Cache für ein logisches Datenobjekt. Wenn Caching für logische Datenobjekte aktiviert ist, löscht dieser Befehl bis auf die letzte Cache-Ausführung den gesamten Cache für ein logisches Datenobjekt. Wenn die aktuelle Cache-Ausführung vor dem in der Eigenschaft für den Cache-Aktualisierungszeitraum festgelegten Datum liegt, wird der aktuelle Cache ebenfalls gelöscht. Wenn Caching für logische Datenobjekte nicht aktiviert ist, löscht dieser Befehl den gesamten Cache für das logische Datenobjekt.

Sie müssen die Anwendung für ein logisches Datenobjekt deaktivieren, bevor Sie den Cache für Datenobjekte löschen.

Der Befehl „infacmd dis PurgeDataObjectCache“ verwendet die folgende Syntax:

```
PurgeDataObjectCache

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password
```

```
[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-Application|-a> application

<-Folder|-f> folder

<-DataObject|-do> data_model.data_object

[<-PurgeAll|-pa> true|false]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis PurgeDataObjectCache“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.
Application -a	anwendung	Name der Anwendung, die das Datenobjekt enthält.
Folder -f	folder	Name des Ordners, der das Datenobjektmodell enthält.
DataObject -do	data_model.data_object	Name des Datenobjekts mit dem Cache, der bereinigt werden soll.
-PurgeAll -pa	true | false	Optional. Löscht den gesamten Cache für ein logisches Datenobjekt.

PurgeResultSetCache

Bereinigt die Ergebnissatz-Caches für eine Anwendung. Sie können den Cache für eine Anwendung bereinigen, wenn Sie die vorhandenen Ergebnissatz-Caches für die SQL-Datendienste und die Webdienste in der Anwendung nicht benötigen.

Der Befehl „infacmd dis PurgeResultSetCache“ verwendet die folgende Syntax:

```
PurgeResultSetCache

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-Application|-a> application
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis PurgeResultSetCache“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.
Application -a	anwendung	Name der Anwendung, deren Ergebnissatz-Cache bereinigt werden soll.

RefreshDataObjectCache

Aktualisiert einen Datenobjekt-Cache.

Der Befehl „infacmd dis RefreshDataObjectCache“ verwendet die folgende Syntax:

```
RefreshDataObjectCache

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-Application|-a> application
```

```
<-Folder|-f> folder

<-DataObject|-do> data_model.data_object
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis RefreshDataObjectCache“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, für den die Anwendungen aufgelistet werden sollen.
-Application -a	anwendung	Erforderlich. Name der Anwendung, die das Datenobjekt enthält.
-Folder -f	folder	Erforderlich. Name des Ordners, der das Datenobjekt enthält.
-DataObject -do	data_model.data_object	Erforderlich. Name des Datenobjekts mit einem zu aktualisierenden Cache.

RenameApplication

Benennt eine bereitgestellte Anwendung um. Bevor Sie eine Anwendung umbenennen, führen Sie infacmd dis StopApplication aus, um die Anwendung zu beenden.

Der Befehl „infacmd dis RenameApplication“ verwendet die folgende Syntax:

```
RenameApplication

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-Application|-a> application

<-NewName|-n> new_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis RenameApplication“ beschrieben:

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

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.
-Application -a	anwendung	Erforderlich. Name der aktuellen Anwendung.
-NewName -n	new_name	Erforderlich. Neuer Name für die Anwendung.

RestoreApplication

Stellt eine Anwendung aus einer Backup-Datei wieder her. Wenn Sie eine wiederhergestellte Anwendung bereitstellen, richtet sich der Anwendungsstatus nach dem standardmäßigen Bereitstellungsmodus. Die Anwendungseigenschaften werden in der wiederhergestellten Anwendung beibehalten.

Der Befehl „infacmd dis RestoreApplication“ verwendet die folgende Syntax:

```
RestoreApplication

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-FileName|-f> file_name

[<-Application|-a> application]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis RestoreApplication“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdienst, in dem die Anwendung wiederhergestellt werden soll.

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

SetApplicationPermissions

Weist Berechtigungen für eine Anwendung einem Benutzer oder einer Gruppe zu oder verweigert diese.

Mit den Optionen -ap oder -dp des SetApplicationPermissions-Befehls können Sie Berechtigungen für Benutzer erteilen oder verweigern. Wenn Sie mit einer der Optionen Berechtigungen nicht explizit erteilen oder verweigern, werden alle Berechtigungen für die Anwendung widerrufen.

Der Befehl „infacmd dis SetApplicationPermissions“ verwendet die folgende Syntax:

```
SetApplicationPermissions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Application|-a> application_name

<<-GranteeUserName|-gun> grantee_user_name|<-GranteeGroupName|-ggn> grantee_group_name>

[<-GranteeSecurityDomain|-gsdn> grantee_security_domain]

[<-AllowedPermissions|-ap> allowed_permissions]

[<-DeniedPermissions|-dp> denied_permissions]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis SetApplicationPermissions“ beschrieben:

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

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	application_name	Erforderlich. Name der Anwendung.
-GranteeUserName| GranteeGroupName -gun|-ggn	grantee_user_name| grantee_group_name	Erforderlich. Benutzername bzw. Gruppenname, für den Berechtigungen festgelegt oder verweigert werden sollen.
-GranteeSecurityDomain -gsdn	grantee_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden und Benutzerberechtigungen gewähren. Name der Sicherheitsdomäne, zu der der Benutzer gehört.

Option	Argument	Beschreibung
-AllowedPermissions -ap	allowed_permissions	Optional. Liste der zulässigen Berechtigungen. Geben Sie eine der folgenden Berechtigungen durch Leerzeichen getrennt ein: - View. Benutzer können die Anwendung anzeigen. - Grant. Benutzer können Berechtigungen für die Anwendung gewähren und entziehen. - Execute. Benutzer können die Anwendung ausführen.
-DeniedPermissions -dp	denied_permissions	Optional. Liste der Berechtigungen, die Benutzern verweigert werden sollen. Trennen Sie jeden Parameter durch ein Leerzeichen. Geben Sie eine der folgenden Berechtigungen durch Leerzeichen getrennt ein: - View. Benutzer können die Anwendung anzeigen. - Grant. Benutzer können Berechtigungen für die Anwendung weder gewähren noch entziehen. - Execute. Benutzer können die Anwendung nicht ausführen.

SetApplicationObjectPermissions

Weist Berechtigungen für ein Anwendungsobjekt zu bzw. lehnt diese ab, wie z. B. ein Mapping oder Arbeitsablauf zu einem Benutzer bzw. einer Gruppe.

Mit den Optionen -ap oder -dp des SetApplicationObjectPermissions-Befehls können Sie Berechtigungen für Benutzer erteilen oder verweigern. Wenn Sie mit einer der Optionen Berechtigungen nicht explizit erteilen oder verweigern, erbt der Benutzer die Berechtigung auf Anwendungsebene für die Zuordnung oder den Arbeitsablauf.

Der Befehl „infacmd dis SetApplicationObjectPermissions“ verwendet die folgende Syntax:

```
SetApplicationObjectPermissions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Application|-a> application_name

<-ApplicationObjectType|-t> application_object_type_Mapping_Workflow

<-ApplicationObject|-ao> application_object_name

<<-GranteeUserName|-gun> grantee_user_name|<-GranteeGroupName|-ggn> grantee_group_name>

[<-GranteeSecurityDomain|-gsdn> grantee_security_domain]

[<-AllowedPermissions|-ap> allowed_permissions]

[<-DeniedPermissions|-dp> denied_permissions]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis SetApplicationObjectPermissions“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	application_name	Erforderlich. Name der Anwendung.
-ApplicationObjectType -t	application_object_type	Erforderlich. Typ des Anwendungsobjekttyps. Geben Sie einen der folgenden Werte ein: - Mapping - Arbeitsablauf
-ApplicationObject -ao	application_object_name	Erforderlich. Name des Anwendungsobjekts.
-GranteeUserName| GranteeGroupName -gun|-ggn	grantee_user_name| grantee_group_name	Erforderlich. Benutzername bzw. Gruppenname, für den Berechtigungen festgelegt oder verweigert werden sollen.
-GranteeSecurityDomain -gsdn	grantee_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden und Benutzerberechtigungen gewähren. Name der Sicherheitsdomäne, zu der der Benutzer gehört.
-AllowedPermissions -ap	allowed_permissions	Optional. Liste der zulässigen Berechtigungen. Geben Sie eine der folgenden Berechtigungen durch Leerzeichen getrennt ein: - View. Benutzer können die Anwendung anzeigen. - Grant. Benutzer können Berechtigungen für die Anwendung gewähren und entziehen. - Execute. Benutzer können die Anwendung ausführen.
-DeniedPermissions -dp	denied_permissions	Optional. Liste der Berechtigungen, die Benutzern verweigert werden sollen. Trennen Sie jeden Parameter durch ein Leerzeichen. Geben Sie eine der folgenden Berechtigungen durch Leerzeichen getrennt ein: - View. Benutzer können die Anwendung anzeigen. - Grant. Benutzer können Berechtigungen für die Anwendung weder gewähren noch entziehen. - Execute. Benutzer können die Anwendung nicht ausführen.

SetSequenceState

Aktualisiert den aktuellen Wert des Sequenzdatenobjekts.

Der Befehl „infacmd dis setsequencestate“ verwendet die folgende Syntax:

```
SetSequenceState
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application
<-SequenceObjectPath|-sop> sequence_object_path
<-SequenceValue|-sv> sequence_value
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis SetSequenceState“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Integrationsdiensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositorys kompatibel sein. Der Name darf nicht länger als 230 Zeichen sein und keine voran- bzw. nachgestellten Leerzeichen, Wagenrückläufe, Tabulatoren oder folgende Zeichen enthalten: / * ? < > " |
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

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

Option	Argument	Beschreibung
-SequenceObjectPath -sop	Sequenzobjekt-Pfad	Erforderlich. Pfad zum Sequenzdatenobjekt. Der Pfad muss die folgenden Objekte in der angegebenen Reihenfolge enthalten, sofern zutreffend: - Projekt - Ordner - SQL-Datendienst oder Webdienst - Mapping - Sequenzgeneratorumwandlung - Sequenzdatenobjekt Befindet sich das Sequenzdatenobjekt in einem Mapping, SQL-Datendienst oder Webdienst, müssen Sie vor dem Mapping-, SQL-Datendienst- oder Webdienstnamen ein Präfix angeben. Verwenden Sie die folgenden Präfixe mit Optionen im Befehl: - Mapping:<Mapping-Name> - SQLDS:<SQL-Datendienstname> - WS:<Webdienstname> Trennen Sie die Optionen mit einem Schrägstrich (/). Beispiel: `<Projektname>/<Ordner>/SQLDS:<SQL-Datendienstname>/Mapping:<virtuelle Tabellenzuordnung>/<Sequenzgenerator-Umwandlung>/<Sequenzdatenobjekt-Name>`
-SequenceValue -sv	sequence_value	Erforderlich. Der neue Wert für Sequenzdatenobjekt. Geben Sie einen Wert ein, der größer oder gleich dem Startwert des Sequenzdatenobjekts und kleiner oder gleich dem Endwert ist.

.

StartApplication

Startet eine bereitgestellte Anwendung. Sie müssen die Anwendung vor dem Starten aktivieren. Der Datenintegrationsdienst muss ausgeführt werden.

Der Befehl „infacmd dis StartApplication“ verwendet die folgende Syntax:

```
StartApplication

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Application|-a> application
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis StartApplication“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	anwendung	Erforderlich. Name der zu startenden Anwendung.

StopApplication

Hält eine Anwendung an. Sie können eine Anwendung anhalten, wenn sie gesichert werden muss oder wenn Benutzern der Zugriff auf die Anwendung verweigert werden soll.

Der Befehl „infacmd dis StopApplication“ verwendet die folgende Syntax:

```
StopApplication

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-Application|-a> application
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis StopApplication“ beschrieben:

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

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.
-Application -a	anwendung	Erforderlich. Name der anzuhaltenden Anwendung.

stopBlazeService

Hält die Ausführung der Komponenten der Blaze-Engine an. Sie möchten die Ausführung der Blaze-Engine-Komponenten unter Umständen anhalten, wenn Sie den Hadoop-Cluster warten, wie z. B. beim Bereinigen von Ressourcen oder Anwenden von Software-Patches.

Der infacmd dis stopBlazeService-Befehl verwendet die folgende Syntax:

```
stopBlazeService

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis stopBlazeService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.

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

UndeployApplication

Entfernt eine Anwendung aus einem Datenintegrationsdienst.

Der Befehl „infacmd dis UndeployApplication“ verwendet die folgende Syntax:

```
UndeployApplication

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-Application|-a> application
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis UndeployApplication“ beschrieben:

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

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

UpdateApplication

Aktualisiert eine Anwendung über eine Anwendungsdatei und verwaltet die Konfiguration. Die Anwendung muss in einem Datenintegrationsdienst bereitgestellt werden. Endanwender können auf die neueste Version der Anwendung zugreifen.

Der Befehl „infacmd dis UpdateApplication“ verwendet die folgende Syntax:

```
UpdateApplication

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-FileName|-f> file_name
```

```
[<-Application|-a> application]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis UpdateApplication“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-FileName -f	file_name	Erforderlich. Name und Pfad der Anwendungsdatei, mit der die bereitgestellte Anwendung aktualisiert wird.
-Application -a	anwendung	Optional. Name der bereitgestellten Anwendung.

UpdateApplicationOptions

Aktualisiert die Anwendungseigenschaften.

Trennen Sie die einzelnen Optionen und Werte mit einem Leerzeichen. Führen Sie zum Anzeigen der aktuellen Eigenschaften infacmd dis ListApplicationOptions aus.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

Der Befehl „infacmd dis UpdateApplicationOptions“ verwendet die folgende Syntax:

```
UpdateApplicationOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Application|-a> application

<-Options|-o> options
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis UpdateApplicationOptions“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	anwendung	Erforderlich. Name der zu aktualisierenden Anwendung.
-Options -o	optionen	Erforderlich. Geben Sie alle zu aktualisierenden Optionen und Werte ein. Trennen Sie jede Option mit einem Leerzeichen. Führen Sie zum Anzeigen der Anwendungsoptionen den infacmd dis ListApplicationOptions-Befehl aus.

UpdateComputeOptions

Aktualisiert Datenintegrationsdienst-Eigenschaften für einen Knoten mit der Berechnungsrolle. Verwenden Sie den Befehl, um Datenintegrationsdienst-Eigenschaften für einen bestimmten Berechnungsknoten zu überschreiben.

Geben Sie die Optionen in folgendem Format ein:

```
... -o option_name=value option_name=value ...
```

Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

Der infacmd dis UpdateComputeOptions-Befehl verwendet die folgende Syntax:

```
UpdateComputeOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name

<-Options|-o> options
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis UpdateComputeOptions“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
NodeName -nn	node_name	Erforderlich. Knoten mit der Berechnungsrolle, die dem Datenintegrationsdienst oder dem Datenintegrationsdienstgitter zugewiesen ist.
-Options -o	options	Erforderlich. Geben Sie jede Option durch ein Leerzeichen getrennt ein. Führen Sie zum Anzeigen der Optionen den infacmd dis ListComputeOptions-Befehl aus. Sie können die folgenden Optionen des Datenintegrationsdiensts aktualisieren: - ExecutionOptions.TemporaryDirectories - ExecutionOptions.DISHomeDirectory - ExecutionOptions.CacheDirectory - ExecutionOptions.SourceDirectory - ExecutionOptions.TargetDirectory - ExecutionOptions.RejectFilesDirectory

UpdateDataObjectOptions

Aktualisiert Datenobjekteigenschaften. Führen Sie den infacmd dis ListDataObjectOptions-Befehl aus, um die aktuellen Optionen anzuzeigen.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

Der Befehl „infacmd dis UpdateDataObjectOptions“ verwendet die folgende Syntax:

```
UpdateDataObjectOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Application|-a> application

<-Folder|-f> folder
```

```
<-DataObject|-do> data_model.data_object

<-Options|-o> options
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis UpdateDataObjectOptions“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	anwendung	Erforderlich. Anwendung, in der das Datenobjekt enthalten ist.
-Folder -f	Folder	Erforderlich. Name des Ordners, der das Datenobjektmodell enthält.
-DataObject -do	data_model.data_object	Erforderlich. Name des Datenobjekts, das Sie aktualisieren möchten.
-Options -o	optionen	Erforderlich. Geben Sie Optionen und Werte durch Leerzeichen getrennt ein. Führen Sie den infacmd dis ListDataObjectOptions-Befehl aus, um die aktuellen Optionen anzuzeigen.

Datenobjektoptionen

Verwenden Sie die Datenobjektoptionen, um das Zwischenspeichern für ein logisches Datenobjekt zu konfigurieren. Verwenden Sie die Datenobjektoptionen mit dem infacmd dis UpdateDataObjectOptions-Befehl.

Geben Sie Datenobjektoptionen im folgenden Format ein:

```
... -o option_type.option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

Die folgende Tabelle beschreibt die Datenobjektoptionen:

Option	Beschreibung
DataObjectOptions.CachingEnabled	Zwischenspeichern des logischen Datenobjekts in der Cache-Datenbank des Datenobjekts. „True“ oder „False“. Standardwert ist „True“.
DataObjectOptions.CacheRefreshPeriod	Anzahl der Minuten zwischen den Cache-Aktualisierungen. Standardwert ist Null.
DataObjectOptions.CacheTableName	Der Name der benutzerverwalteten Tabelle, aus der der Datenintegrationsdienst auf den Cache des logischen Datenobjekts zugreift. Eine benutzerverwaltete Cache-Tabelle ist eine Tabelle in der Cache-Datenbank des Datenobjekts, die Sie bei Bedarf erstellen, füllen und manuell aktualisieren können. Wenn Sie einen Cache-Tabellennamen angeben, verwaltet der Datenobjekt-Cache-Manager den Cache für das Objekt nicht und ignoriert den Cache-Aktualisierungszeitraum. Wenn Sie keinen Cache-Tabellennamen angeben, verwaltet der Datenobjekt-Cache-Manager den Cache für das Objekt.

UpdateParameterSetEntries

Aktualisiert Einträge aus einem Parametersatz. Führen Sie diesen Befehl aus, um die Werte in Parametersatzeinträgen für eine Zuordnung oder einen Arbeitsablauf in einer Anwendung zu aktualisieren.

Der infacmd dis UpdateParameterSetEntries-Befehl verwendet die folgende Syntax:

```
UpdateParameterSetEntries

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Application|-a> application

<-parameterSetName|-ps> parameter set name

<-projectScope|-prs> path to the mapping or workflow that contains the parameters. For a
mapping, M1, in project P1 and folder F1, the path is P1/F1/mapping/M1.

<-paramNames|-pnv> parameter name-value pairs, separated by double quotes
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd dis UpdateParameterSetEntries“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	application	Erforderlich. Name der Anwendung, die den Parametersatz enthält.
parametersetname - ps	parameterset name	Erforderlich. Name des Parametersatzes.
-projectScope -prs	project scope	Erforderlich. Pfad der Zuordnung oder des Arbeitsablaufs, der die Parameter enthält. Für die Zuordnung M1 in Projekt P1 und Ordner F1 lautet der Pfad: P1/F1/Zuordnung/M1.
-paramNames -pnv	parameter names	Erforderlich. Namen-Wert-Paare des Parameters getrennt durch Leerzeichen. Setzen Sie Namen-Wert-Paare in doppelte Anführungszeichen. Versehen Sie jeden Wert mit einfachen Anführungszeichen. Verwenden Sie folgende Syntax: `"parm1='valueA'" "parm2='valueB'" "parm3='valueC'"` . Sie können Leerzeichen in einem Parameterwert verwenden. Sie können ein Apostroph (') oder einen Doppelpunkt (:) im Wert verwenden, wenn Sie für diese Zeichen einen umgekehrten Schrägstrich (\) als Escape-Zeichen verwenden. `'C:\Verzeichnis'`

UpdateServiceOptions

Aktualisiert Datenintegrationsdienst-Eigenschaften. Führen Sie zum Anzeigen der aktuellen Eigenschaften den infacmd dis ListServiceOptions-Befehl aus.

Sie können die Eigenschaften ändern, während der Dienst ausgeführt wird, aber Sie müssen den Dienst neu starten, damit die geänderten Eigenschaften wirksam werden.

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

```
UpdateServiceOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-Options|-o> options]
```

```
[<-NodeName|-nn> node_name | <-GridName|-gn> grid_name]

[<-BackupNodes|-bn> node_name1,node_name2,...]
```

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

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Options -o	optionen	Optional. Geben Sie jede Option durch ein Leerzeichen getrennt ein. Führen Sie zum Anzeigen der Optionen den infacmd dis ListServiceOptions-Befehl aus.
-NodeName -nn -GridName -gn	node_name grid_name	Optional. Geben Sie den Knoten oder das Gitter ein, auf dem der Datenintegrationsdienst ausgeführt wird. Der Datenintegrationsdienst kann auf einem Knoten oder auf einem Gitter ausgeführt werden.
-BackupNodes -bn	node_name1,node_name2,...	Optional. Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist. Sie können Sicherungsknoten konfigurieren, wenn Sie hohe Verfügbarkeit haben.

Optionen des Datenintegrationsdiensts

Verwenden Sie die Optionen des Datenintegrationsdiensts mit dem infacmd dis-Befehl UpdateServiceOptions.

Geben Sie die Optionen des Datenintegrationsdiensts in folgendem Format ein:

```
... -o option_type.option_name=value
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Optionen des Datenintegrationsdiensts beschrieben:

Option	Beschreibung
LoggingOptions.LogLevel	Ebene der Fehlermeldungen, die der Datenintegrationsdienst in das Dienstprotokoll schreibt. Wählen Sie eine der folgenden Meldungsebenen aus: Fatal, Error, Warning, Info, Trace oder Debug.
ExecutionOptions.OutOfProcessExecution	Führt Jobs im Datenintegrationsdienstprozess, in separaten DTM-Prozessen auf dem lokalen Knoten oder in separaten DTM-Prozessen auf Remoteknoten aus. Konfigurieren Sie die Eigenschaft basierend auf den vom Datenintegrationsdienst ausgeführten Jobtypen sowie basierend darauf, ob der Datenintegrationsdienst auf einem Einzelknoten oder Gitter ausgeführt wird. Geben Sie eine der folgenden Optionen ein: - IN_PROCESS. Führt Jobs im Datenintegrationsdienstprozess aus. Konfigurieren Sie diese Option, wenn Sie Jobs des SQL-Datendiensts und des Webdiensts auf einem Einzelknoten oder Gitter ausführen, in dem jeder Knoten sowohl über die Dienst- als auch über die Berechnungsrolle verfügt. - OUT_OF_PROCESS. Führt Jobs in separaten DTM-Prozessen auf dem lokalen Knoten aus. Konfigurieren Sie diese Option, wenn Sie Zuordnungs-, Profil- und Arbeitsablaufjobs auf einem Einzelknoten oder Gitter ausführen, in dem jeder Knoten sowohl über die Dienst- als auch über die Berechnungsrolle verfügt. - OUT_OF_PROCESS_REMOTE. Führt Jobs in separaten DTM-Prozessen auf Remoteknoten aus. Konfigurieren Sie diese Option, wenn Sie Zuordnungs-, Profil- und Arbeitsablaufjobs auf einem Gitter ausführen, in dem Knoten eine andere Kombination der Rollen aufweisen können. Wenn Sie diese Option konfigurieren und der Datenintegrationsdienst auf einem Einzelknoten ausgeführt wird, führt der Dienst Jobs in separaten lokalen Prozessen aus. Standardwert ist OUT_OF_PROCESS.
ExecutionOptions.MaxExecutionPoolSize	Maximale Anzahl an Jobs, die pro Datenintegrationsdienstprozess gleichzeitig ausgeführt werden können. Zu den Jobs gehören Datenvorschauen, Zuordnungen, Profilerstellungsjobs, SQL-Abfragen und Webdienstanfragen. Ein Datenintegrationsdienstgitter umfasst beispielsweise drei laufende Dienstprozesse. Wenn Sie den Wert auf 10 festlegen, kann jeder Datenintegrationsdienst bis zu 10 Jobs gleichzeitig ausführen. Insgesamt 30 Jobs können gleichzeitig auf dem Gitter ausgeführt werden. Standardwert ist 10.

Option	Beschreibung
ExecutionOptions.MaxMemorySize	Die maximale Speichermenge in Byte, die der Datenintegrationsdienst für die gleichzeitige Ausführung aller Anfragen zuordnen kann, wenn der Dienst Jobs in dem Prozess des Datenintegrationsdiensts ausführt. Wenn der Datenintegrationsdienst Jobs in separaten lokalen Prozessen oder Remoteprozessen ausführt, ignoriert der Dienst diesen Wert. Wenn Sie die Speichergröße, die der Datenintegrationsdienst zuordnen kann, nicht einschränken möchten, legen Sie diese Eigenschaft auf 0 fest. Wenn der Wert größer als 0 ist, verwendet der Datenintegrationsdienst die Eigenschaft zur Berechnung des maximalen Gesamtspeicherplatzes, der für die gleichzeitige Ausführung aller Anfragen zulässig ist. Der Datenintegrationsdienst berechnet den maximalen Gesamtspeicherplatz folgendermaßen: Maximale Speichergröße + maximale Heap-Größe + zum Laden von Programmkomponenten erforderlicher Speicherplatz Standardwert ist 0. **Hinweis:** Wenn Sie Profile oder Datenqualitäts-Mappings ausführen, müssen Sie diese Eigenschaft auf 0 festlegen.
ExecutionOptions.MaxMappingParallelism	Maximale Anzahl paralleler Threads, die eine einzelne Zuordnungs-Pipeline-Stage verarbeiten. Wenn Sie den Wert auf größer als eins festlegen, aktiviert der Datenintegrationsdienst Partitionierung für Zuordnungen sowie für aus Profilen umgewandelte Zuordnungen. Der Dienst führt eine dynamische Skalierung der Anzahl an Partitionen für eine Zuordnungs-Pipeline zur Laufzeit durch. Erhöhen Sie den Wert basierend auf der Anzahl der CPUs, die auf den Knoten verfügbar sind, auf denen Zuordnungen ausgeführt werden. Im Developer Tool können Entwickler den Wert für den maximalen Parallelismus je Zuordnung festlegen. Wenn maximaler Parallelismus sowohl für den Datenintegrationsdienstprozess als auch für die Zuordnung eingerichtet wurde, verwendet der Datenintegrationsdienst den Minimalwert beim Ausführen der Zuordnung. Standardwert ist 1. Der Maximalwert ist 64.
ExecutionOptions.DisHadoopPrincipal	Dienstprinzipalname (SPN) des Datenintegrationsdiensts zum Herstellen einer Verbindung zu einem Hadoop-Cluster, der Kerberos-Authentifizierung verwendet.
ExecutionOptions.DisHadoopKeytab	Der Dateipfad der Kerberos-Keytab-Datei auf dem Computer, auf dem der Datenintegrationsdienst ausgeführt wird.
ExecutionOptions.TemporaryDirectories	Verzeichnis für temporäre Dateien, die während der Ausführung von Jobs erstellt werden. Standardwert ist `<Basisverzeichnis>/disTemp`. Geben Sie eine Liste mit durch Semikola getrennten Verzeichnissen ein, um die Leistung während Profilvorgängen und während der Cache-Partitionierung für Sortierumwandlungen zu optimieren. Die folgenden Zeichen dürfen nicht im Verzeichnispfad verwendet werden: `* ? < > " | , [ ]`

Option	Beschreibung
ExecutionOptions.DISHomeDirectory	Root-Verzeichnis, auf das vom Knoten aus zugegriffen werden kann. Dies ist das Root-Verzeichnis für andere Dienstverzeichnisse. Standardwert ist `<Informatica-Installationsverzeichnis>/tomcat/bin`. Wenn Sie den Standardwert ändern, stellen Sie sicher, dass das Verzeichnis vorhanden ist. Die folgenden Zeichen dürfen nicht im Verzeichnispfad verwendet werden: `* ? < > " | ,`
ExecutionOptions.CacheDirectory	Verzeichnis für Index- und Daten-Cache-Dateien für Umwandlungen. Standardwert ist `<Basisverzeichnis>/cache`. Geben Sie eine Liste mit durch Semikola getrennten Verzeichnissen ein, um die Leistung während der Cache-Partitionierung für Aggregator-, Joiner- und Rangumwandlungen zu optimieren. Die folgenden Zeichen dürfen nicht im Verzeichnispfad verwendet werden: `* ? < > " | ,`
ExecutionOptions.SourceDirectory	Verzeichnis für Einfachdateien der Quelle, die in einem Mapping verwendet werden. Standardwert ist `<Basisverzeichnis>/source`. Wenn der Datenintegrationsdienst auf einem Gitter ausgeführt wird, können Sie ein freigegebenes Verzeichnis zum Erstellen eines Verzeichnisses für Quelldateien verwenden. Wenn Sie für jeden Knoten mit der Berechnungsrolle ein anderes Verzeichnis konfigurieren, stellen Sie sicher, dass die Quelldateien in allen Quellverzeichnissen konsistent sind. Die folgenden Zeichen dürfen nicht im Verzeichnispfad verwendet werden: `* ? < > " | ,`
ExecutionOptions.TargetDirectory	Standardverzeichnis für Zieleinfachdateien, die in einem Mapping verwendet werden. Standardwert ist `<Basisverzeichnis>/target`. Geben Sie eine Liste mit durch Semikola getrennten Verzeichnissen ein, um die Leistung zu steigern, wenn mehrere Partitionen in das Einfachdateiziel schreiben. Wenn der Datenintegrationsdienst auf einem Gitter ausgeführt wird, verwenden Sie zum Erstellen eines Verzeichnisses für Zieldateien ein freigegebenes Verzeichnis. Wenn Sie für jeden Knoten mit der Berechnungsrolle ein anderes Verzeichnis konfigurieren, stellen Sie sicher, dass die Zieldateien in allen Zielverzeichnissen konsistent sind. Die folgenden Zeichen dürfen nicht im Verzeichnispfad verwendet werden: `* ? < > " | ,`

Option	Beschreibung
ExecutionOptions.RejectFilesDirectory	Verzeichnis für Ablehnungsdateien. Ablehnungsdateien enthalten Zeilen, die beim Ausführen eines Mappings zurückgewiesen wurden. Standardwert ist `<Basisverzeichnis>/reject`. Die folgenden Zeichen dürfen nicht im Verzeichnispfad verwendet werden: `* ? < > " | ,`
ExecutionOptions.HadoopInfaHomeDir	Das PowerCenter Big Data Edition-Basisverzeichnis auf jedem von der Hadoop RPM-Installation erstellten Datenknoten. Geben Sie `/<PowerCenterBigDataEditionInstallationDirectory>/Informatica` ein.
ExecutionOptions.HadoopDistributionDir	Das Verzeichnis enthält eine Sammlung von Hive- und Hadoop-JARS im Cluster aus den RPM-Installationsspeicherorten. Das Verzeichnis enthält den minimalen Satz an JARs, die für die Verarbeitung von Informatica-Mappings in einer Hadoop-Umgebung erforderlich sind. Geben Sie `/<PowerCenterBigDataEditionInstallationDirectory>/Informatica/services/shared/hadoop/[Hadoop_distribution_name]` ein.
ExecutionOptions.DisHadoopDistributionDir	Das Hadoop-Distributionsverzeichnis auf dem Datenintegrationsdienst-Knoten. Die Inhalte des Datenintegrationsdienst-Hadoop-Distributionsverzeichnisses müssen mit den Inhalten des Hadoop-Distributionsverzeichnisses auf den Datenknoten identisch sein. Geben Sie `<Informatica-Installationsverzeichnis>/Informatica/services/shared/hadoop/[Hadoop_distribution_name]` ein.
RepositoryOptions.RepositoryServiceName	Dienst, der Laufzeitmetadaten speichert, die zur Ausführung von Zuordnungen und SQL-Datendiensten erforderlich sind.
RepositoryOptions.RepositoryUserName	Benutzername für den Zugriff auf das Modellrepository. Der Benutzer muss über die Berechtigung zum Erstellen von Projekten für den Modellrepository-Dienst verfügen.
RepositoryOptions.RepositoryPassword	Benutzerpasswort für den Zugriff auf das Modellrepository.
RepositoryOptions.RepositorySecurityDomain	Name der LDAP-Sicherheitsdomäne, wenn Sie LDAP verwenden. Wenn Sie LDAP nicht verwenden, ist die Standarddomäne nativ.
DataObjectCacheOptions.CacheRemovalTime	Die Anzahl von Millisekunden, die der Datenintegrationsdienst wartet, ehe er den Cache-Speicher nach einer Aktualisierung bereinigt. Standardwert ist 3.600.000.
DataObjectCacheOptions.CacheConnection	Der Datenbankverbindungsname für die Datenbank, in der der Datenobjekt-Cache gespeichert wird. Geben Sie einen gültigen Namen für das Verbindungsobjekt ein.
DataObjectCacheOptions.MaxConcurrentRefreshRequests	Maximale Anzahl an Cache-Aktualisierungen, die gleichzeitig stattfinden können.

Option	Beschreibung
DataObjectCacheOptions.EnableNestedLDOCache	Gibt an, dass der Datenintegrationsdienst Cache-Daten für ein logisches Datenobjekt verwenden kann, das während einer Cache-Aktualisierung in einem anderen logischen Datenobjekt als Quelle oder als Lookup verwendet wird. Bei false greift der Datenintegrationsdienst auf die Quellressourcen zu, auch wenn das Caching für das als Quelle oder Lookup verwendete logische Datenobjekt aktiviert wurde. Beispiel: Das logische Datenobjekt LDO3 vereint Daten aus den logischen Datenobjekten LDO1 und LDO2. Ein Entwickler erstellt ein Mapping, das LDO3 als Eingabe verwendet, und bezieht das Mapping in einer Anwendung mit ein. Sie aktivieren das Caching für LDO1, LDO2, LDO3. Wenn Sie das Caching für verschachtelte logische Datenobjekte aktivieren, verwendet der Datenintegrationsdienst bei der Aktualisierung der Cache-Tabelle für LDO3 auch Cache-Daten für LDO1 und LDO2. Wenn Sie das Caching für verschachtelte logische Datenobjekte nicht aktivieren, greift der Datenintegrationsdienst bei der Aktualisierung der Cache-Tabelle für LDO3 auf die Quellressourcen für LDO1 und LDO2 zu. Standardwert ist „false“.
DeploymentOptions.DefaultDeploymentMode	Gibt an, ob eine Anwendung aktiviert und gestartet werden soll, nachdem sie einem Datenintegrationsdienst bereitgestellt wurde. Geben Sie eine der folgenden Optionen ein: - EnableandStart. Aktivieren und starten Sie die Anwendung. - EnableOnly. Aktivieren Sie die Anwendung, ohne sie zu starten. - Disable. Aktivieren Sie die Anwendung nicht.
PassThroughSecurityOptions.AllowCaching	Ermöglicht Datenobjekt-Caching für alle Pass-Through-Verbindungen im Datenintegrationsdienst. Befüllt den Datenobjekt-Cache mithilfe der Anmeldedaten im Verbindungsobjekt. **Hinweis:** Wenn Sie Datenobjekt-Caching mit Pass-Through-Sicherheit aktivieren, lassen Sie unter Umständen nicht autorisierten Zugriff auf bestimmte Daten zu.
HttpProxyServerOptions.HttpProxyServerHost	Name des HTTP-Proxy-Servers.
HttpProxyServerOptions.HttpProxyServerPort	Portnummer des HTTP-Proxy-Servers. Standardwert ist 8080.
HttpProxyServerOptions.HttpServerUser	Authentifizierter Benutzername für den HTTP-Proxy-Server. Dies ist erforderlich, wenn der Proxy-Server Authentifizierung verlangt.
HttpProxyServerOptions.HttpProxyServerPassword	Passwort für den authentifizierten Benutzer. Der Dienstmanager verschlüsselt das Passwort. Dies ist erforderlich, wenn der Proxy-Server Authentifizierung verlangt.
HttpProxyServerOptions.HttpProxyServerDomain	Domäne für die Authentifizierung.

Option	Beschreibung
HttpConfigurationOptions.AllowedIPAddresses	Liste der Konstanten oder regulären Java-Expressionsmuster im Vergleich zur IP-Adresse des anfragenden Computers. Trennen Sie mehrere Konstanten oder Expressionen durch ein Leerzeichen. Wenn Sie diese Eigenschaft konfigurieren, nimmt der Datenintegrationsdienst Anfragen von IP-Adressen an, die mit dem zulässigen Adressmuster übereinstimmen. Wenn Sie diese Eigenschaft nicht konfigurieren, verwendet der Datenintegrationsdienst die Eigenschaft „Abgelehnte IP-Adressen“ zum Bestimmen der Clients, die Anfragen senden können.
HttpConfigurationOptions.AllowedHostNames	Liste der Konstanten oder regulären Java-Expressionsmuster im Vergleich zu den Hostnamen des anfragenden Computers. Die Hostnamen unterliegen der Groß-/Kleinschreibung. Trennen Sie mehrere Konstanten oder Expressionen durch ein Leerzeichen. Wenn Sie diese Eigenschaft konfigurieren, nimmt der Datenintegrationsdienst Anfragen von Hosts an, deren Namen mit dem Muster der zulässigen Hostnamen übereinstimmen. Wenn Sie diese Eigenschaft nicht konfigurieren, verwendet der Datenintegrationsdienst die Eigenschaft „Abgelehnte Hostnamen“ zum Bestimmen der Clients, die Anfragen senden können.
HttpConfigurationOptions.DeniedIPAddresses	Liste der Konstanten oder regulären Java-Expressionsmuster im Vergleich zur IP-Adresse des anfragenden Computers. Trennen Sie mehrere Konstanten oder Expressionen durch ein Leerzeichen. Wenn Sie diese Eigenschaft konfigurieren, nimmt der Datenintegrationsdienst Anfragen von IP-Adressen an, die nicht mit dem Muster der abgelehnten IP-Adresse übereinstimmen. Wenn Sie diese Eigenschaft nicht konfigurieren, verwendet der Datenintegrationsdienst die Eigenschaft „Zulässige IP-Adressen“ zum Bestimmen der Clients, die Anfragen senden können.
HttpConfigurationOptions.DeniedHostNames	Liste der Konstanten oder regulären Java-Expressionsmuster im Vergleich zu den Hostnamen des anfragenden Computers. Die Hostnamen unterliegen der Groß-/Kleinschreibung. Trennen Sie mehrere Konstanten oder Expressionen durch ein Leerzeichen. Wenn Sie diese Eigenschaft konfigurieren, nimmt der Datenintegrationsdienst Anfragen von Hosts an, deren Namen nicht mit dem Muster der abgelehnten Hostnamen übereinstimmen. Wenn Sie diese Eigenschaft nicht konfigurieren, verwendet der Datenintegrationsdienst die Eigenschaft „Zulässige Hostnamen“ zum Bestimmen der Clients, die Anfragen senden können.

Option	Beschreibung
HttpConfigurationOptions.HTTPProtocolType	Sicherheitsprotokoll, das vom Datenintegrationsdienst verwendet wird. Geben Sie einen der folgenden Werte ein: - HTTP. In Anfragen an den Dienst muss eine HTTP-URL verwendet werden.. - HTTPS. In Anfragen an den Dienst muss eine HTTPS-URL verwendet werden. - Beide. In Anfragen an den Dienst kann entweder eine HTTP- oder eine HTTPS-URL verwendet werden. Wenn Sie den HTTP-Protokolltyp auf „HTTPS“ oder „Beide“ einstellen, aktivieren Sie TLS (Transport Layer Security) für den Dienst. Sie können TLS auch für jeden Webdienst aktivieren, der einer Anwendung bereitgestellt ist. Wenn Sie HTTPS für den Data Integration Service und TLS für den Webdienst aktivieren, verwendet der Webdienst eine HTTPS-URL. Wenn Sie HTTPS für den Data Integration Service und nicht für den Webdienst aktivieren, kann der Webdienst eine HTTP-URL oder eine HTTPS-URL nutzen. Wenn Sie TLS für einen Webdienst aktivieren, aber HTTPS nicht für den Data Integration Service aktivieren, startet der Webdienst nicht. Standardwert ist „HTTP“.
ResultSetCacheOptions.FileNamePrefix	Das Präfix für die Namen aller Ergebnissatz-Cachedateien, die auf dem Datenträger gespeichert sind. Standardwert ist RSCACHE.
ResultSetCacheOptions.EnableEncryption	Gibt an, ob die Ergebnissatz-Cachedateien mit der 128-Bit-AES-Verschlüsselung verschlüsselt werden. Gültige Werte sind „True“ oder „False“. Standardwert ist „True“.
MappingServiceOptions.MaxNotificationThreadPoolSize	Weist die Anzahl an Threads zu, die Benachrichtigungen an den Client senden.
MappingServiceOptions.MaxMemPerRequest	Das Verhalten von „Maximale Speichergröße pro Anfrage“ richtet sich nach den folgenden Datenintegrationsdienst-Konfigurationen: - Der Dienst führt Jobs in lokalen Prozessen oder Remoteprozessen aus oder die Diensteigenschaft „Maximale Speichergröße“ lautet 0 (Standardeinstellung). „Maximale Speichergröße pro Anfrage“ ist die maximale Speichermenge in Byte, die der Datenintegrationsdienst allen Umwandlungen zuordnen kann, die den automatischen Cache-Modus in einer einzelnen Anfrage verwenden. Der Dienst weist Arbeitspeicher separat zu Umwandlungen zu, die über eine bestimmte Cache-Größe verfügen. Der von der Anfrage verwendete Gesamtspeicher kann den Wert für „Maximale Speichergröße pro Anfrage“ überschreiten. - Der Dienst führt Jobs in dem Prozess des Datenintegrationsdiensts aus und die Diensteigenschaft „Maximale Speichergröße“ ist größer als 0. „Maximale Speichergröße pro Anfrage“ ist die maximale Speichermenge in Byte, die der Datenintegrationsdienst einer einzelnen Anfrage zuordnen kann. Der von der Anfrage verwendete Gesamtspeicher darf den Wert für „Maximale Speichergröße pro Anfrage“ nicht überschreiten. Standardwert ist 536.870.912.

Option	Beschreibung
ProfilingServiceOptions.ProfileWarehouseConnectionName	Name des Verbindungsobjekts für die Verbindung mit dem Profiling Warehouse.
ProfilingServiceOptions.MaxRanks	Anzahl der Höchst- und Minimalwerte, die für ein Profil angezeigt werden sollen. Standardwert ist 5. Standardwert ist 10.
ProfilingServiceOptions.MaxPatterns	Maximale Anzahl der für ein Profil anzuzeigenden Muster
ProfilingServiceOptions.MaxProfileExecutionPoolSize	Maximale Anzahl an Threads zum Ausführen des Profiling.
ProfilingServiceOptions.MaxExecutionConnections	Maximale Anzahl an Datenbankverbindungen für jeden Profiling-Job.
ProfilingServiceOptions.ExportPath	Speicherort zum Exportieren von Profilergebnissen. Geben Sie den Dateisystempfad ein. Standardwert ist „./ProfileExport“.
AdvancedProfilingServiceOptions.MinPatternFrequency	Mindestanzahl an Mustern, die für ein Profil angezeigt werden sollen.
AdvancedProfilingServiceOptions.MaxValueFrequencyPairs	Maximale Anzahl an im Profiling Warehouse zu speichernden Wert-/Frequenzpaaren. Standardwert ist 16.000.
AdvancedProfilingServiceOptions.MaxStringLength	Maximale Länge einer Zeichenfolge, die vom Profilerstellungsdienst verarbeitet werden kann.
AdvancedProfilingServiceOptions.MaxNumericPrecision	Maximale Anzahl an Ziffern für einen numerischen Wert.
AdvancedProfilingServiceOptions.ExecutionPoolSize	Maximale Anzahl an Threads zum Ausführen von Zuordnungen.
AdvancedProfilingServiceOptions.ColumnsPerMapping	Begrenzt die Anzahl der Spalten, für die in einer einzelnen Zuordnung ein Profil erstellt werden kann, um Arbeits- und Festplattenspeicher einzusparen. Standardwert ist 5. Wenn Sie ein Profil für eine Quelle mit über 100 Millionen Zeilen erstellen, verringern Sie den Wert auf 1.
AdvancedProfilingServiceOptions.MaxParallelColumnBatches	Anzahl der Threads, die gleichzeitig Zuordnungen ausführen können. Standardwert ist 1.
AdvancedProfilingServiceOptions.ValueFrequencyMemSize	Zulässige Speichermenge für Wert-/Frequenzpaare. Standardwert ist 64 Megabyte.
AdvancedProfilingServiceOptions.ReservedThreads	Anzahl der Threads der maximalen Ausführungspoolgröße für Prioritätsanfragen. Standardwert ist 1.
AdvancedProfilingServiceOptions.MaxMemPerRequest	Die maximale Speichermenge in Byte, die der Datenintegrationsdienst für jede Mapping-Ausführung für eine einzelne Profilanfrage zuordnen kann. Standardwert ist 536.870.912.

Option	Beschreibung
SQLServiceOptions.DTMKeepAliveTime	Anzahl an Millisekunden, die der DTM-Prozess geöffnet bleibt, nachdem er die letzte Anfrage abgeschlossen hat. Identische SQL-Abfragen können den offenen Prozess wiederverwenden. Verwenden Sie die Keep Alive-Zeit, um die Leistung zu erhöhen, wenn die für die Verarbeitung der SQL-Abfrage erforderliche Zeit im Vergleich zur Dauer der Initialisierung des DTM-Prozesses gering ist. Wenn die Abfrage fehlschlägt, wird der DTM-Prozess beendet. Muss größer oder gleich 0 sein. 0 bedeutet, dass der Datenintegrationsdienst den DTM-Prozess nicht im Speicher beibehält. Standardwert ist 0. Sie können diese Eigenschaft auch für jeden SQL-Datendienst festlegen, der auf dem Datenintegrationsdienst bereitgestellt wird. Wenn Sie diese Eigenschaft für einen bereitgestellten SQL-Datendienst festlegen, überschreibt der Wert für den bereitgestellten SQL-Datendienst den Wert, den Sie für den Datenintegrationsdienst festgelegt haben.
SQLServiceOptions.TableStorageConnection	Relationale Datenbankverbindung, die temporäre Tabellen für SQL-Datendienste speichert. Standardmäßig ist keine Verbindung ausgewählt.
SQLServiceOptions.SkipLogFiles	Hindert den Datenintegrationsdienst daran, Protokolldateien zu erstellen, wenn die SQL-Datendienstanfrage erfolgreich abgeschlossen wird und die Tracing-Ebene auf INFO oder höher festgelegt ist. Standardwert ist „false“.
SQLServiceOptions.MaxMemPerRequest	Das Verhalten von „Maximale Speichergröße pro Anfrage“ richtet sich nach den folgenden Datenintegrationsdienst-Konfigurationen: - Der Dienst führt Jobs in lokalen Prozessen oder Remoteprozessen aus oder die Diensteigenschaft „Maximale Speichergröße“ lautet 0 (Standardeinstellung). „Maximale Speichergröße pro Anfrage“ ist die maximale Speichermenge in Byte, die der Datenintegrationsdienst allen Umwandlungen zuordnen kann, die den automatischen Cache-Modus in einer einzelnen Anfrage verwenden. Der Dienst weist Arbeitsspeicher separat zu Umwandlungen zu, die über eine bestimmte Cache-Größe verfügen. Der von der Anfrage verwendete Gesamtspeicher kann den Wert für „Maximale Speichergröße pro Anfrage“ überschreiten. - Der Dienst führt Jobs in dem Prozess des Datenintegrationsdiensts aus und die Diensteigenschaft „Maximale Speichergröße“ ist größer als 0. „Maximale Speichergröße pro Anfrage“ ist die maximale Speichermenge in Byte, die der Datenintegrationsdienst einer einzelnen Anfrage zuordnen kann. Der von der Anfrage verwendete Gesamtspeicher darf den Wert für „Maximale Speichergröße pro Anfrage“ nicht überschreiten. Standardwert ist 50.000.000.
WorkflowOrchestrationServiceOptions.DBName	Verbindungsname der Datenbank, in der Laufzeitmetadaten für Arbeitsabläufe gespeichert werden.

Option	Beschreibung
WSServiceOptions.DTMKeepAliveTime	Anzahl an Millisekunden, die der DTM-Prozess geöffnet bleibt, nachdem er die letzte Anfrage abgeschlossen hat. Web-Dienst-Anfragen für dieselbe Operation können den offenen Prozess wiederverwenden. Verwenden Sie die Keep Alive-Zeit, um die Leistung zu erhöhen, wenn die für die Verarbeitung der Anfrage erforderliche Zeit im Vergleich zur Dauer der Initialisierung des DTM-Prozesses gering ist. Wenn die Anfrage fehlschlägt, wird der DTM-Prozess beendet. Muss größer oder gleich 0 sein. 0 bedeutet, dass der Datenintegrationsdienst den DTM-Prozess nicht im Speicher beibehält. Standardwert ist 5000. Sie können diese Eigenschaft auch für jeden Webdienst festlegen, der auf dem Datenintegrationsdienst bereitgestellt wird. Wenn Sie diese Eigenschaft für einen bereitgestellten Webdienst festlegen, überschreibt der Wert für den bereitgestellten Webdienst den Wert, den Sie für den Datenintegrationsdienst festgelegt haben.
WSServiceOptions.WSDLLogicalURL	Präfix für die WSDL-URL, wenn Sie einen externen HTTP-Load Balancer verwenden. Beispiel: http://loadbalancer:8080 Der Datenintegrationsdienst benötigt einen externen HTTP-Load Balancer, um einen Webdienst auf einem Gitter auszuführen. Wenn Sie den Datenintegrationsdienst auf einem Einzelknoten ausführen, müssen Sie keine logische URL angeben.
WSServiceOptions.SkipLogFiles	Hindert den Datenintegrationsdienst daran, Protokolldateien zu erstellen, wenn die Webdienstanfrage erfolgreich abgeschlossen wird und die Tracing-Ebene auf INFO oder höher festgelegt ist. Standardwert ist „False“.
WSServiceOptions.MaxMemPerRequest	Das Verhalten von „Maximale Speichergröße pro Anfrage“ richtet sich nach den folgenden Datenintegrationsdienst-Konfigurationen: - Der Dienst führt Jobs in lokalen Prozessen oder Remoteprozessen aus oder die Diensteigenschaft „Maximale Speichergröße“ lautet 0 (Standardeinstellung). „Maximale Speichergröße pro Anfrage“ ist die maximale Speichermenge in Byte, die der Datenintegrationsdienst allen Umwandlungen zuordnen kann, die den automatischen Cache-Modus in einer einzelnen Anfrage verwenden. Der Dienst weist Arbeitspeicher separat zu Umwandlungen zu, die über eine bestimmte Cache-Größe verfügen. Der von der Anfrage verwendete Gesamtspeicher kann den Wert für „Maximale Speichergröße pro Anfrage“ überschreiten. - Der Dienst führt Jobs in dem Prozess des Datenintegrationsdiensts aus und die Diensteigenschaft „Maximale Speichergröße“ ist größer als 0. „Maximale Speichergröße pro Anfrage“ ist die maximale Speichermenge in Byte, die der Datenintegrationsdienst einer einzelnen Anfrage zuordnen kann. Der von der Anfrage verwendete Gesamtspeicher darf den Wert für „Maximale Speichergröße pro Anfrage“ nicht überschreiten. Standardwert ist 50.000.000.
Modules.MappingService	Geben Sie FALSE ein, um das Modul zu deaktivieren, das Zuordnungen und Vorschauen ausführt. Standardwert ist „True“.

Option	Beschreibung
Modules.ProfilingService	Geben Sie FALSE ein, um das Modul zu deaktivieren, das Profile ausführt und Scorecards erzeugt. Standardwert ist „True“.
Modules.SQLService	Geben Sie FALSE ein, um das Modul zu deaktivieren, das SQL-Abfragen anhand eines SQL-Datendiensts ausführt. Standardwert ist „True“.
Modules.WebService	Geben Sie FALSE ein, um das Modul zu deaktivieren, das Webdienst-Vorgangszuordnungen ausführt. Standardwert ist „True“.
Modules.WorkflowOrchestrationService	Geben Sie FALSE ein, um das Modul zu deaktivieren, das Arbeitsabläufe ausführt. Standardwert ist „True“.

UpdateServiceProcessOptions

Aktualisiert Eigenschaften für einen Datenintegrationsdienst-Prozess. Führen Sie zum Anzeigen der aktuellen Eigenschaften den infacmd dis ListServiceProcessOptions-Befehl aus.

Geben Sie die Optionen in folgendem Format ein:

```
... -o option_name=value option_name=value ...
```

Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

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

```
UpdateServiceProcessOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name

<-Options|-o> options
```

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

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
NodeName -nn	node_name	Erforderlich. Knoten, auf dem der Datenintegrationsdienst ausgeführt wird.
-Options -o	options	Erforderlich. Geben Sie jede Option durch ein Leerzeichen getrennt ein. Führen Sie zum Anzeigen der Optionen den infacmd dis ListServiceProcessOptions-Befehl aus.

Data Integration Service-Prozessoptionen

Verwenden Sie die Data Integration Service-Prozessoptionen mit dem infacmd dis UpdateServiceProcessOptions-Befehl.

Geben Sie die Data Integration Service-Prozessoptionen in folgendem Format ein:

```
... -o option_type.option_name=value
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Data Integration Service-Prozessoptionen beschrieben:

Option	Beschreibung
GeneralOptions.JVMOptions	Java Virtual Machine (JVM)-Befehlszeilenoptionen zum Ausführen von Java-basierten Programmen. Bei der Konfiguration von JVM-Optionen müssen Sie die Eigenschaften für den Java SDK-Klassenpfad, den Java SDK-Minimalspeicher und den Java SDK-Maximalspeicher festlegen.
GeneralOptions.HttpPort	Eindeutige HTTP-Portnummer für den Datenintegrationsdienstprozess, wenn der Dienst das HTTP-Protokoll verwendet.
GeneralOptions.HttpsPort	Eindeutige HTTPS-Portnummer für den Datenintegrationsdienstprozess, wenn der Dienst das HTTPS-Protokoll verwendet.

Option	Beschreibung
LoggingOptions.LogDirectory	Verzeichnis der Knotenprozessprotokolle des Datenintegrationsdiensts. Standardwert ist `<INFA_HOME>\logs\dislogs`. Wenn der Datenintegrationsdienst in einem Gitter ausgeführt wird, verwenden Sie zum Erstellen eines Verzeichnisses für Protokolldateien ein gemeinsam genutztes Verzeichnis. Durch ein gemeinsam genutztes Verzeichnis stellen Sie sicher, dass bei einem Failover des Master-Dienstprozesses auf einen anderen Knoten der neue Master-Dienstprozess auf frühere Protokolldateien zugreifen kann.
ResultSetCacheOptions.MaxTotalDiskSize	Maximale Byte-Anzahl, die für den Dateispeicher des Ergebnissatz-Caches zulässig ist. Standardwert ist 0.
ResultSetCacheOptions.MaxPerCacheMemorySize	Maximale Byte-Anzahl, die einer einzelnen Ergebnissatz-Cache-Instanz im Arbeitsspeicher zugewiesen ist. Standardwert ist 0.
ResultSetCacheOptions.MaxTotalMemorySize	Maximale Byte-Anzahl, die dem Speicher des Ergebnissatz-Caches im Arbeitsspeicher insgesamt zugewiesen ist. Standardwert ist 0.
ResultSetCacheOptions.MaxNumCaches	Maximale Anzahl an Ergebnissatz-Cache-Instanzen, die für diesen Datenintegrationsdienstprozess zulässig sind. Standardwert ist 0.
HttpConfigurationOptions.MaxConcurrentRequests	Anzahl der HTTP- oder HTTPS-Verbindungen, die zu diesem Datenintegrationsdienst-Prozess hergestellt werden können. Standardwert ist 200.
HttpConfigurationOptions.MaxBacklogRequests	Anzahl der HTTP- oder HTTPS-Verbindungen, die in der Warteschlange für diesen Datenintegrationsdienst-Prozess warten können. Standardwert ist 100.
HttpConfigurationOptions.KeyStoreFile	Pfad und Dateiname der Schlüsselspeicherdatei, die die Schlüssel und Zertifikate enthält, die zur Verwendung des HTTPS-Protokolls für den Datenintegrationsdienst erforderlich sind. Sie können eine Schlüsselspeicherdatei mit einem Keytool erstellen. Bei Keytool handelt es sich um ein Dienstprogramm, das private oder öffentliche Schlüsselpaare und zugeordnete Zertifikate in einer Schlüsselspeicherdatei erzeugt und speichert. Sie können das selbstsignierte Zertifikat nutzen oder ein Zertifikat verwenden, das von einer Zertifizierungsstelle signiert wurde. Wenn Sie den Datenintegrationsdienst in einem Gitter ausführen, muss die Schlüsselspeicherdatei auf jedem Knoten im Gitter die gleichen Schlüssel enthalten.
HttpConfigurationOptions.KeyStorePassword	Passwort für die Schlüsselspeicherdatei.
HttpConfigurationOptions.TrustStoreFile	Pfad und Dateiname der Truststore-Datei, die Authentifizierungszertifikate enthält, die vom Datenintegrationsdienst als vertrauenswürdig eingestuft werden. Wenn Sie den Datenintegrationsdienst in einem Gitter ausführen, muss die Truststore-Datei auf jedem Knoten im Gitter die gleichen Schlüssel enthalten.

Option	Beschreibung
HttpConfigurationOptions.TrustStorePassword	Passwort für die Truststore-Datei.
HttpConfigurationOptions.SSLProtocol	Zu verwendendes Secure Sockets Layer-Protokoll. Standardwert ist TLS.
SQLServiceOptions.MaxConcurrentConnections	Begrenzt die Anzahl der Datenbankverbindungen, die der Datenintegrationsdienst für SQL-Datendienste herstellen kann. Standardwert ist 100.

KAPITEL 11

Infacmd es-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- ListServiceOptions, 215
- UpdateServiceOptions, 217
- UpdateSMTPOptions, 218

ListServiceOptions

Gibt eine Liste mit Eigenschaften zurück, die für den E-Mail-Dienst konfiguriert sind. Zum Konfigurieren der Eigenschaften des E-Mail-Diensts führen Sie „infacmd es updateServiceOptions“ aus. Zum Konfigurieren der E-Mail-Server-Eigenschaften des E-Mail-Diensts führen Sie „infacmd es updateSMTPOptions“ aus.

Der infacmd es listServiceOptions-Befehl verwendet die folgende Syntax:

```
ListServiceOptions

<-DomainName|-dn> domain_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password

[<-ServiceName|-sn> service_name]
```

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

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

UpdateServiceOptions

Aktualisiert die Eigenschaften des E-Mail-Diensts. Führen Sie diesen Befehl zum Konfigurieren der Domäneneigenschaften und Knoten für den E-Mail-Dienst aus. Zum Anzeigen der aktuellen Eigenschaften des E-Mail-Diensts führen Sie „infacmd es listServiceOptions“ aus.

Der infacmd es updateServiceOptions-Befehl verwendet die folgende Syntax:

```
UpdateServiceOptions

<-DomainName|-dn> domain_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password

[<-ServiceName|-sn> service_name]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-NodeName|nn> primary node name]

[<-BackupNodes|-bn> backup node names]
```

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

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Optional. Geben Sie Email_Service ein.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-Options -o	options	Geben Sie die Optionen in folgendem Format ein: `OptionGroupName.OptionName=OptionValue OptionGroupName2.OptionName2=OptionValue2` Führen Sie zum Anzeigen gültiger Optionen „infacmd isp ListServiceOptions“ aus.
-NodeName -nn	Name des primären Knotens	Optional. Primärer Knoten, auf dem der Dienst ausgeführt wird.
-BackupNodes -bn	Namen der Backup-Knoten	Optional. Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist.

UpdateSMTPOptions

Aktualisiert die SMTP-Eigenschaften für den E-Mail-Dienst. Geschäftsglossare und Arbeitsabläufe verwenden die SMTP-Konfiguration des E-Mail-Diensts zum Senden von Benachrichtigungen per E-Mail.

Die folgenden Benachrichtigungen verwenden die SMTP-Konfiguration des E-Mail-Diensts zum Senden von E-Mails:

- Business Glossary-Benachrichtigungen.
- Scorecard-Benachrichtigungen.
- Arbeitsablaufbenachrichtigungen. Zu den Arbeitsablaufbenachrichtigungen gehören E-Mails, die aus Human- und Benachrichtigungsaufgaben in Arbeitsabläufen gesendet werden, die der Datenintegrationsdienst ausführt.

Der infacmd es updateSMTPOptions-Befehl verwendet die folgende Syntax:

```
UpdateSMTPOptions

<-DomainName|-dn> domain_name
```

```
<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ServiceName|-sn> service_name]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-SMTPServerHostName|-sa> smtp_host]

[<-SMTPUsername|-su> smtp_email_password]

[<-SMTPEmailPassword|-se> smtp_email_password]

[<-SMTPEmailAddress|-ss> smtp_email_address]

[<-SMTPPort|-sp> smtp_port]

[<-SMTPAuthEnabled|-sau> smtp_auth_enabled]

[<-SMTPTLSEnabled|-stls> smtp_tls_enabled]

[<-SMTPSSLEnabled|-sssl> smtp_ssl_enabled]
```

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ServiceName -sn	service_name	Optional. Geben Sie Email_Service ein.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-SMTPServerHostName -sa	smtp_host	Optional. Hostname für ausgehenden SMTP-Mailserver. Geben Sie zum Beispiel den Microsoft Exchange-Server für Microsoft Outlook ein. Standardwert ist „localhost“.
-SMTPUsername -su	smtp_user	Optional. Benutzername für die Authentifizierung beim Senden.
-SMTPEmailPassword -se	smtp_email_password	Optional. Passwort für die Authentifizierung beim Senden, wenn dies vom ausgehenden SMTP-Mailserver gefordert wird.
-SMTPEmailAddress -ss	smtp_email_address	Optional. E-Mail-Adresse, die der E-Mail-Dienst beim Senden von Benachrichtigungs-E-Mails aus einem Arbeitsablauf im Feld „Von“ verwendet. Standardwert ist `admin@example.com`.
SMTPPort -sp	smtp_port	Optional. Portnummer, die vom ausgehenden SMTP-Mailserver verwendet wird. Die gültigen Werte liegen zwischen 1 und 65535. Standardwert ist 25.
-SMTPAuthEnabled -sau	smtp_auth_enabled	Optional. Gibt an, dass der SMTP-Server für die Authentifizierung aktiviert ist. Wenn TRUE, erfordert der ausgehende Mailserver einen Benutzernamen und ein Passwort. Wenn TRUE, müssen Sie angeben, ob der Server das TLS- (Transport Layer Security) oder das SSL-Protokoll (Secure Sockets Layer) verwenden soll. Geben Sie `TRUE` oder `FALSE` ein. Standardwert ist „false“.

Option	Argument	Beschreibung
-SMTPTLSEnabled -stls	smtp_tls_enabled	Optional. Gibt an, dass der SMTP-Server das TLS-Protokoll verwendet. Wenn TRUE, geben Sie die TLS-Portnummer für die Eigenschaft des SMTP-Serverports ein. Geben Sie `TRUE` oder `FALSE` ein. Standardwert ist „false“.
-SMTPSSLEnabled -sssl	smtp_ssl_enabled	Optional. Gibt an, dass der SMTP-Server das SSL-Protokoll verwendet. Wenn TRUE, geben Sie die SSL-Portnummer für die Eigenschaft des SMTP-Serverports an. Geben Sie `TRUE` oder `FALSE` ein. Standardwert ist „false“.

KAPITEL 12

infacmd ihs-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- createservice, 222
- ListServiceOptions, 226
- UpdateServiceOptions, 227
- BackupData, 229
- Cluster-Dienst aktualisieren, 230
- Snapshot entfernen, 232

createservice

Erstellt einen Informatica-Cluster-Dienst.

Der Befehl „infacmd ihs createService“ verwendet die folgende Syntax:

```
CreateService
<-DomainName|-dn> domain_name
<-NodeName|-nn> node_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-HttpPort|-p> port_name]
[<-HttpsPort|-sp> https_port_name]
[<-EnableTls|-tls> enable_tls true|false]
[<-KeystoreFile|-kf> keystore_file_location]
[<-KeystorePassword|-kp> keystore_password]
[<-SSLProtocol|-sslp> ssl_protocol]
<-HadoopGatewayHost|-hgh>
```

```
[<-HadoopGatewayPort|-hgp>]
<-HadoopNodes|-hn>
[<-GatewayUser|-gu>]
[<-isDomainSSLEnabled|-dssl> Is domain SSL enabled true|false]
[<-TrustStoreLocation|-tf>]
[<-TrustStorePassword|-tp>]
[<-EnableKerberos|-krb> enable_kerberos true|false]
[<-KdcType|-kt> kdc_type mit-kdc|active-directory]
[<-KdcHost|-kh> kdc_host]
[<-AdminServerHost|-ah> kdc_host]
[<-Realm|-r> realm]
[<-LdapUrl|-lu> ldap_url]
[<-ContainerDn|-cd> container_dn]
[<-AdminUserPrincipal|-au> admin_principal]
[<-AdminPassword|-ap> admin_password]
[<-OtherOptions|-oo> other options]
```

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

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-NodeName -nn	node_name	Erforderlich. Knotenname der Informatica-Domäne.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Informatica-Cluster-Diensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-HttpPort -p	port_name	Optional. Eine eindeutige HTTP-Portnummer, die für den Informatica-Cluster-Dienst verwendet wird.
-HttpsPort -sp	https_port_name	Erforderlich, wenn Sie Transport Layer Security aktivieren. Die Portnummer für die HTTPS-Verbindung.
-EnableTls -tls	enable_tls true|false	Optional. Wählen Sie diese Option zum Aktivieren von Transport Layer Security aus.
-KeystoreFile -kf	keystore_file_location	Erforderlich, wenn Sie „Transport Layer Security aktivieren“ auswählen. Pfad und Dateiname der Schlüsselspeicherdatei. Die Schlüsselspeicherdatei enthält die Schlüssel und Zertifikate, die bei Verwendung des SSL-Sicherheitsprotokolls mit dem Administrator von Live Data Map erforderlich sind.
-KeystorePassword -kp	keystore_password	Erforderlich, wenn Sie „Transport Layer Security aktivieren“ auswählen. Das Passwort für die Schlüsselspeicherdatei.
-SSLProtocol -sslp	ssl_protocol	Optional. Zu verwendendes Secure Sockets Layer-Protokoll.
-HadoopGatewayHost -hgh	Hadoop_Gateway_Host	Erforderlich. Vollständig qualifizierter Hostname des Knotens, der als Gateway zum Hadoop-Cluster dient.

Option	Argument	Beschreibung
-HadoopGatewayPort -hgp	Hadoop_Gateway_Port	Optional. Die Portnummer des Hadoop-Gateway-Knotens. Standardwert ist 8080.
-HadoopNodes -hn	Hadoop_Nodes	Erforderlich. Kommagetrennte Liste mit vollständig qualifizierten Hostnamen, die die Hadoop-Dienste hosten.
-GatewayUser -gu	Gateway_User	Optional. Benutzername für den Hadoop-Gateway-Knoten. Aktivieren Sie eine SSH-Verbindung von der Informatica-Domäne zum Hadoop-Gateway-Host. Standardwert ist root.
-isDomainSSLEnabled -dssl	is_Domain_SSL_Enabled	Optional. Geben Sie „True“ an, um die SSL-Domäne zu aktivieren. Standardwert ist „False“.
-TrustStoreLocation -tf	Trust_Store_Location	Erforderlich, wenn bei der Domäne SSL aktiviert ist. Domänenspeicherort der Truststore-Datei im Cluster.
-TrustStorePassword -tp	Trust_Store_Password	Erforderlich, wenn bei der Domäne SSL aktiviert ist. Passwort der Truststore-Domäne.
-EnableKerberos -krb	Enable_Kerberos	Optional. Geben Sie „True“ an, um Kerberos zu aktivieren. Standardwert ist „False“.
-KdcType -kt	kdc_type mit-kdc|active-directory	Erforderlich, wenn Kerberos aktiviert ist. Typ des konfigurierten Schlüsselverteilungscenters, wie z. B. MIT KDC oder Active Directory.
-KdcHost -kh	kdc_host	Erforderlich, wenn Kerberos aktiviert ist. Vollständig qualifizierter Domänenname für den Host des Schlüsselverteilungscenters.
-AdminServerHost -ah	kdc_host	Erforderlich, wenn Kerberos aktiviert ist. Vollständig qualifizierter Domänenname für den administrativen Serverhost für KDC Kerberos.
-Realm -r	realm	Erforderlich, wenn Kerberos aktiviert ist. Name des Kerberos-Bereichs.
-LdapUrl -lu	ldap_url	Erforderlich, wenn Kerberos aktiviert ist. URL zum Active Directory.
-ContainerDn -cd	container_dn	Erforderlich, wenn Kerberos aktiviert ist. Name des Containers, der zum Speichern von Dienstprinzipalen verwendet wird.
-AdminUserPrincipal -au	admin_principal	Erforderlich, wenn Kerberos aktiviert ist. Administrator-Benutzerprinzipal, der zum Erstellen von Prinzipalen und Schlüsseltabellen verwendet wird.

Option	Argument	Beschreibung
-AdminPassword -ap	admin_password	Erforderlich, wenn Kerberos aktiviert ist. Administratorpasswort für den Administrator-Benutzerprinzipal.
-OtherOptions -oo	other options	Optional. Geben Sie Name-Wert-Paare durch Leerzeichen getrennt ein. Zur Eingabe eines Optionswerts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

ListServiceOptions

Listet Optionen für den Informatica-Cluster-Dienst auf.

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

```
ListServiceOptions

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

[<-SecurityDomain|-sdn> security_domain]

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ihs ListServiceOptions“ beschrieben:

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

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Informatica-Cluster-Diensts.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

UpdateServiceOptions

Aktualisiert Optionen für den Informatica-Cluster-Dienst. Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

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

```
UpdateServiceOptions

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

[<-SecurityDomain|-sdn> security_domain]
```

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

<-Options|-o> options
```

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

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Options -o	options	Erforderlich. Geben Sie Name-Wert-Paare durch Leerzeichen getrennt ein.

BackupData

Sichert die HDFS-Daten des internen Hadoop-Clusters in einer ZIP-Datei. Beim Sichern der Daten speichert der Informatica-Cluster-Dienst alle durch Live Data Map erstellten Daten, z. B. HBase-Daten, Scanner-Daten und Erfassungsdaten.

Hinweis: Verwenden Sie den Befehl „infacmd ihs BackupData“, wenn Sie den Informatica-Cluster-Dienst aktualisieren.

Der Befehl „infacmd ihs BackupData“ verwendet die folgende Syntax:

```
BackupData

<-InformaticaClusterServiceHost | -icsh> infa_cluster_service_host

<-InformaticaClusterServicePort | -icsp> infa_cluster_service_port

<-LocalDirectory | -ld> local_directory

[<-TLSEnabled | -tls>] TLS_enabled
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ihs BackupData“ beschrieben:

Option	Argument	Beschreibung
-InformaticaClusterServiceHost -icsh	infa_cluster_service_host	Erforderlich. Bezieht sich auf den Hostnamen der Informatica-Domäne, auf dem der Informatica-Cluster-Dienst ausgeführt wird.
-InformaticaClusterServicePort -icsp	infa_cluster_service_port	Erforderlich. Bezieht sich auf den für den Informatica-Cluster-Dienst konfigurierten HTTP- oder HTTPS-Port.

Option	Argument	Beschreibung
-LocalDirectory -ld	local_directory	Erforderlich. Bezieht sich auf den Speicherort des Verzeichnisses im Domänen-Host, an dem die Backup-Datei gespeichert werden muss. **Hinweis:** Informatica empfiehlt, den Namen der Backup-Datei „Informatica.zip“ nicht zu ändern.
-TLSEnabled -tls	TLS_enabled	Optional. Gibt an, ob bei dem Informatica-Cluster-Dienst, auf den die Sicherung übertragen werden muss, TLS aktiviert ist. Legen Sie diese Option bei einem Informatica-Cluster-Dienst mit aktiviertem TLS auf „true“ fest.

Cluster-Dienst aktualisieren

Aktualisiert die Konfiguration des Informatica-Cluster-Diensts.

Der Befehl „infacmd ihs UpgradeClusterService“ verwendet die folgende Syntax:

```
UpgradeClusterService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

<-ClusterServiceName|-sn> cluster_service_name

  [<-SecurityDomain|-sdn> security_domain]

  [<-ResilienceTimeout|-re> timeout_period_in_seconds]

  <-BackupDirectory|-bd> backup_directory
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ihs UpgradeClusterService“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-BackupDirectory -bd	backup_directory	Erforderlich. Der Speicherort des Verzeichnisses, das die Backup-Dateien auf dem Domänenhost enthält.

Snapshot entfernen

Entfernt vorhandene HDFS-Snapshots, sodass Sie den Befehl „infacmd ihs BackupData“ erfolgreich zum Sichern von HDFS-Daten ausführen können.

Hinweis: Sie müssen den Befehl „infacmd ihs removesnapshot“ ausführen, wenn der Befehl „infacmd ihs BackupData“ fehlschlägt.

Der Befehl „infacmd ihs removesnapshot“ verwendet die folgende Syntax:

```
removesnapshot

<-InformaticaClusterServiceHost | -icsh> infa_cluster_service_host

<-InformaticaClusterServicePort | -icsp> infa_cluster_service_port

[<-TlsEnabled|-tls> | ]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ihs removesnapshot“ beschrieben:

Option	Argument	Beschreibung
-InformaticaClusterServiceHost -icsh	infa_cluster_service_host	Erforderlich. Bezieht sich auf den Hostnamen für den Host des Informatica-Cluster-Diensts, auf dem der Informatica-Cluster-Dienst ausgeführt wird.
-InformaticaClusterServicePort -icsp	infa_cluster_service_port	Erforderlich. Bezieht sich auf den für den Informatica-Cluster-Dienst konfigurierten HTTP- oder HTTPS-Port.
-TlsEnabled -tls	TLS_enabled	Optional. Gibt an, ob bei dem Informatica-Cluster-Dienst TLS_enabled ist. Legen Sie diese Option bei einem Cluster mit aktiviertem TLS auf „true“ fest.

KAPITEL 13

infacmd ipc-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- ExportToPC, 233
- ImportFromPC, 237
- genReuseReportFromPC, 239

ExportToPC

Exportiert Objekte aus dem Modellrepository oder einer Exportdatei und konvertiert sie in PowerCenter-Objekte.

Mit dem Befehl ExportToPC werden Objekte aus dem Modellrepository oder aus einer aus dem Modellrepository exportierten XML-Datei konvertiert. Sie müssen entweder ein Modellrepository oder eine Quelldatei für den Export auswählen. Wenn Sie beide Optionen auswählen, hat die Quelldateioption Vorrang. Führen Sie den Befehl ExportToPC aus, um eine XML-Datei zu erstellen, die Sie mit dem pmrep-Programm in PowerCenter importieren können.

Der Befehl „infacmd ipc ExportToPC“ verwendet die folgende Syntax:

```
ExportToPC

<-Release|-rel> release_number

[<-SourceFile|-sf> source_file]

[<-SourceRepository|-sr> source_repository]

[<-SourceFolders|-f> folder1 folder2|<-SourceObjects|-so> object1 object2]

[<-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>]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ipc ExportToPC“ beschrieben:

Option	Argument	Beschreibung
-Release -rel	release_number	Erforderlich. Die PowerCenter Versionsnummer.
-SourceFile -sf	source_file	Optional. Den vollständigen Pfad zu einer XML-Datei, die mit dem Developer-Tool exportierte Quellobjekte enthält.

Option	Argument	Beschreibung

-SourceRepository
-sr
	source_repository	Optional. Das Modellrepository, das die nach PowerCenter zu exportierenden Objekte enthält.
		Verwenden Sie die folgende Befehlssyntax in einer Domäne ohne Kerberos-Authentifizierung, um den Gateway-Host und den Port für die Verbindung zum Modellrepository-Dienst anzugeben:
		`<Model repository name>@<host>:<port>#<projectname>?user=<username>[&namespace=<namespace>]&password=<password>`
		Verwenden Sie zum Angeben des Domänennamens, wenn Sie mehrere Gateway-Knoten haben, die folgende Befehlssyntax, um eine stabile Verbindung zum Modellrepository-Dienst in einer Domäne ohne Kerberos-Authentifizierung herzustellen:
		`<Model repository name>@<domainname>#<projectname>?user=<username>[&namespace=<namespace>]&password=<password>`
		Verwenden Sie die folgende Befehlssyntax zum Angeben des Domänennamens mit den eingegebenen Anmeldedaten, um den Befehl mit Single Sign-On auszuführen:
		`<Model repository name>@<domainname>#<projectname>?isloggedinuser=true[&namespace=<namespace>]`
		Verwenden Sie die folgende Befehlssyntax zum Angeben des Gateway-Hosts und des Ports mit den eingegebenen Anmeldedaten, um den Befehl mit Single Sign-On auszuführen:
		`<Model repository name>@<host>:<port>#<projectname>?isloggedinuser=true[&namespace=<namespace>]`
		Verwenden Sie die folgende Befehlssyntax in einer Kerberos-Domäne zum Angeben des Gateway-Hosts und des Ports mit den Anmeldedaten, die Sie statt der eingegebenen Anmeldedaten angeben:
		`<Model repository name>@<host>:<port>#<projectname>?iskerberos=true&user=<username>[&namespace=<namespace>]&password=<password> &Kerberosrealm=<kerberosrealm>`
		Verwenden Sie die folgende Befehlssyntax in einer Kerberos-Domäne zum Angeben des Domänennamens mit den Anmeldedaten, die Sie statt der eingegebenen Anmeldedaten angeben:
		`<Model repository name>@<domainname>#<projectname>?iskerberos=true&user=<username>[&namespace=<namespace>]&password=<password> &Kerberosrealm=<kerberosrealm>`
		Der Portparameter ist der HTTP-Port. Der &namespace-Parameter ist optional. Der Standardnamespace ist nativ.

-SourceFolders -f	source_folders	Wenn Sie -sr verwenden, müssen Sie -f oder -so verwenden. Liste der Quellordner, die aus dem Modellrepository exportiert werden sollen. Sie können Mapplets, Mappings und logische Datenobjektmodelle aus den Quellordnern nach PowerCenter exportieren. Wenn Sie mehr als ein Objekt exportieren, müssen Sie die Objekte in der Liste durch ein Leerzeichen voneinander trennen.

Option	Argument	Beschreibung
SourceObjects -so	source_objects	Wenn Sie -sr verwenden, müssen Sie -f oder -so verwenden. Liste der Quellobjekte, die aus dem Modellrepository exportiert werden sollen. Sie können Mapplets, Mappings und logische Datenobjektmodelle nach PowerCenter exportieren. Sie können das Objekt als Name beschreiben. Verwenden Sie folgende Syntax: `name=/<path>/<objectname>[&type=<typename>]` Sie müssen den vollständigen Pfad des Objekts angeben. Wenn Sie mehr als ein Objekt exportieren, müssen Sie die Objekte in der Liste durch ein Leerzeichen voneinander trennen. Sie können die folgenden Typen eingeben: - Mapping. Verwenden Sie diesen Typ zum Exportieren von Mappings und Mapplets. - DataObjectModel. Verwenden Sie diesen Typ zum Exportieren logischer Datenobjektmodelle. Bei diesem Typ wird nicht zwischen Groß- und Kleinschreibung unterschieden. Standardwert ist „Mapping“.
-Recursive -r	-	Optional. Exportiert alle Mappings und logischen Datenobjektmodelle aus den Quellordnern. Exportiert jeden Unterordner unterhalb der Objekte und alle Unterordner darunter.
-TargetLocation -tl	target_location	Optional. Der vollständige Pfad zur XML-Target-Datei.
-TargetFolder -tf	target_folder_name	Optional. Der PowerCenter-Ordner, in den die Objekte exportiert werden. Der Befehl ExportToPC platziert den Ordnernamen in der XML-Target-Datei. Wenn Sie keinen Ordnernamen konfigurieren, erstellt der Befehl ExportToPC einen Ordnernamen.
-CodePage -cp	target_code_page	Optional. Codepage des PowerCenter-Repository. Standardmäßig wird UTF-8 verwendet.
-Check -c	-	Optional. Testet die Umwandlung, ohne eine Target-Datei zu erstellen.
-ReferenceDataLocation -rdl	reference_data_output_location	Optional. Speicherort, an dem Referenztabellendaten gespeichert werden sollen. Der Befehl „ExportToPC“ speichert die Referenztabellendaten als eine oder mehrere Wörterbuch-Dateien (.dic).
-ConvertMappletTargets -cmt	-	Optional. Wandelt Ziele in Mapplets in Ausgabeumwandlungen im PowerCenter-Mapplet um. PowerCenter-Mapplets dürfen keine Targets enthalten. Wenn der Export ein Mapplet einschließt, das ein Ziel enthält und Sie diese Option nicht auswählen, schlägt der Exportprozess fehl.
-ConvertMappingstoMapplets -cmm	-	Optional. Wandelt Developer-Tool-Mappings in PowerCenter-Mapplets um. Das Developer-Tool wandelt Quellen und Ziele in den Mappings in Eingabe- und Ausgabeumwandlungen in einem PowerCenter-Mapplet um.

Option	Argument	Beschreibung
-NoValidation -nv	-	Optional. Quellobjekte werden vor ihrer Umwandlung nicht über den Befehl ExportToPC validiert.
-DSTErrorFormat -def	-	Optional. Die Fehlermeldungen werden in einem Format angezeigt, das vom Developer-Tool analysiert werden kann. Der vollständige Pfad jedes Objekts wird in den Fehlermeldungen angezeigt. Standardmäßig werden Fehler in einem benutzerfreundlichen Format angezeigt.

ImportFromPC

Wandelt eine XML-Datei eines PowerCenter-Repository-Objekts in eine XML-Datei eines Modellrepository-Objekts um. PowerCenter-Repository-Objekte in eine XML-Datei exportieren. Führen Sie den Befehl „importFromPC“ aus, um eine XML-Zieldatei mit Objekten zu erstellen, die in ein Modellrepository importiert werden können.

Sie können die XML-Zieldatei mit dem infacmd oie ImportObjects-Befehl oder über das Developer Tool in ein Modellrepository importieren. Wenn Sie die Befehlszeile zum Importieren der Ziel-XML-Datei verwenden, weist ImportFromPC den Model Repository-Objekten in der Ziel-XML-Datei keine Verbindungen zu. Sie können Verbindungen mit dem infacmd oie ImportObjects-Befehl oder über das Developer Tool zuweisen.

Der infacmd ipc importFromPC-Befehl verwendet die folgende Syntax:

```
importFromPC

<-Release|-rel> release_number

[<-SourceFile|-sf> source_file]

[<-TargetFile|-tf> target_location]

[<-Check|-c>]

[<-Db2Type|-dt> default_db2_type]

[<-Db2TypesFile|-df> db2_types_file]

[<-DefaultLookUpConType|-dl> default_lookup_con_type]

[<-LookUpConTypesFile|-lcf> lookup_connection_types_file]

[<-ConvertOverriddenProps|-orprops> recreate_transformation_with_overridden_properties_
in_mappings]

[<-LogFile|-lf> log_file]
```

In der folgenden Tabelle werden die Optionen und Argumente des infacmd ipc ImportFromPC-Befehls beschrieben:

Option	Argument	Beschreibung
-Release -rel	release_number	Erforderlich. Die Version des Modellrepositorys.
-SourceFile -sf	source_file	Erforderlich. Der vollständige Pfad einer PowerCenter-XML-Datei, die die Quellobjekte enthält.
-TargetFile -tf	target_location	Erforderlich. Der vollständige Pfad der XML-Zieldatei.
-Check -c	-	Optional. Testet die Umwandlung, ohne eine Zieldatei zu erstellen. Wenn Sie die Objektumwandlung testen, benötigen Sie keinen Zielspeicherort.
-Db2Type -dt	default_db2_type	Optional. Der für die Umwandlung verwendete DB2-Subsystemtyp. Sie können entweder Db2Type oder DB2TypesFile oder beides angeben. Wenn Sie sowohl Db2Type als auch Db2TypesFile für IBM DB2-Objekte angeben, werden die DB2-Quelle und das DB2-Ziel, die nicht in der Db2TypesFile aufgelistet sind, in den Db2Type umgewandelt. Wenn Sie keinen DB2-Subsystemtyp angeben, wird der standardmäßige DB2-Subsystemtyp verwendet. Standardwert ist LUW.
-Db2TypesFile -df	db2_types_file	Optional. Eine Eigenschaftendatei, die die PowerCenter DB2-Quelle und den Db2-Subsystemtyp enthält. Sie können eine Datei vom Typ Db2 verwenden, wenn die Db2-Quelle und das Db2-Ziel aus verschiedenen Subsystemen, wie z. B. LUW, z/OS oder i/OS, stammen. Sie können entweder Db2Type oder DB2TypesFile oder beides angeben. Wenn Sie sowohl Db2Type als auch Db2TypesFile für IBM DB2-Objekte angeben, werden die DB2-Quelle und das DB2-Ziel, die nicht in der Db2TypesFile aufgelistet sind, in den Db2Type umgewandelt. Wenn Sie den DB2-Subsystemtyp nicht angeben, wird der standardmäßige DB2-Subsystemtyp verwendet. Standardwert ist LUW.
-DefaultLookUpConType -dl	default_lookup_con_type	Optional. Der für die Umwandlung verwendete Lookup-Verbindungstyp. Sie können entweder DefaultLookUpConType oder LookUpConTypesFile oder beides angeben. Wenn Sie sowohl DefaultLookUpConType als auch LookUpConTypesFile für die Lookup-Objekte angeben, werden die in der LookUpConTypesFile nicht aufgelisteten Lookup-Umwandlungen in den DefaultLookUpConType konvertiert. Wenn Sie den DefaultLookUpConType für ein Lookup-Objekt während der Umwandlung nicht angeben, wird der Standardverbindungstyp verwendet. Standardwert ist ODBC.

Option	Argument	Beschreibung
-LookUpConTypesFile -lcf	lookup_connection_type_file	Optional. Eine Eigenschaftendatei, die die Lookup-Quelle und den Lookup-Verbindungstyp enthält. Sie können eine Lookup-Verbindungstypdatei verwenden, wenn die Lookup-Objekte aus verschiedenen Datenbanken, wie z. B. Oracle oder IBM DB2, stammen. Sie können entweder DefaultLookUpConType oder LookUpConTypesFile oder beides angeben. Wenn Sie sowohl DefaultLookUpConType als auch LookUpConTypesFile für die Lookup-Objekte angeben, werden die in der LookUpConTypesFile nicht aufgelisteten Lookup-Umwandlungen in den DefaultLookUpConType konvertiert. Wenn Sie den DefaultLookUpConType für ein Lookup-Objekt während der Umwandlung nicht angeben, wird der Standardverbindungstyp verwendet. Standardwert ist ODBC.
-ConvertOverridenprops -orprops	True|False	Optional. Behält Überschreibungseigenschaften für die wiederverwendbare PowerCenter-Quelle, das Ziel sowie für Umwandlungen während der Konvertierung bei. Der Befehl erstellt nicht wiederverwendbare Umwandlungen für PowerCenter-Umwandlungen mit Überschreibungseigenschaften. Er erstellt auch wiederverwendbare Datenobjekte für PowerCenter-Quellen und -Ziele mit Überschreibungseigenschaften. Gültige Werte sind „True“ oder „False“. Standardwert ist „True“.
-LogFile -lf	log_file	Optional. Pfad und Dateiname der Ausgabeprotokolldatei. Standardwert ist „STDOUT“.

genReuseReportFromPC

Erzeugt einen Bericht, in dem die Anzahl der PowerCenter-Mappings geschätzt wird, die im Modellrepository für eine native oder Hadoop-Umgebung wiederverwendet werden können. Sie können den Bericht als PDF-Dokument drucken.

Stellen Sie vor dem Ausführen des Befehls „infacmd ipc genReuseReportFromPC“ sicher, dass Sie die folgenden Aufgaben ausführen:

- Konfigurieren Sie die erforderlichen Umgebungsvariablen für den Befehl „pmrep“.
- Wenn Sie eine Linux-Umgebung verwenden, gewähren Sie die Berechtigungen zum Lesen, Schreiben und Ausführen für jeden Versionsordner, der sich in folgendem Verzeichnis befindet: `<informatica server installation directory>/tools/pcutils`

Der Befehl „infacmd ipc genReuseReportFromPC“ verwendet die folgende Syntax:

```
genReuseReportFromPC

<-RepositoryName|-r> Pc_Repository_Name

<-HostName|-h> Pc_Domain_HostName

<-PortNumber|-o> Pc_Domain_PortNumber

[<-UserName|-n> Domain_UserName]

[<-Password|-x> Domain_Password]

[<-SecurityDomain|-s> Pc_Repository_Security_domain]
```

```
<-folderNames|-f> Pc_Folder_Names

<-SrcRelease|-srel> Pc_Release_version

[<-targetRelease|-trel> Target_Release_version]

[<-CodePage|-cp>  Pc_Repository_code_page]

<-targetDir|-td> Target_Directory

<-authenticationType> -at Authentication_Type

[<-LogFile|-lf> Log_file_Name]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ipc genreusereportfrompc“ beschrieben:

Option	Argument	Beschreibung
-RepositoryName -r	Pc_Repository_Name	Erforderlich. Der Name des PowerCenter-Repository.
-HostName -h	Pc_Domain_Host Name	Erforderlich. Der Domänenname des PowerCenter-Repository.
-PortNumber -o	Pc_Domain_PortNumber	Erforderlich. Die Portnummer des PowerCenter-Repository.
-UserName -n	Domain_UserName	Optional. Benutzername der PowerCenter-Domäne. Wenn Sie keinen Benutzernamen eingeben, verwendet der Befehl den Wert in der Umgebungsvariablen INFA_DEFAULT_DOMAIN_USER.
Passwort -x	Domain_Password	Optional. Passwort für die PowerCenter-Domäne. Wenn Sie keinen Benutzernamen eingeben, verwendet der Befehl den Wert in der Umgebungsvariablen INFA_DEFAULT_DOMAIN_PASSWORD.
-SecurityDomain -s	Pc_Repository_Security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wenn Sie keine Sicherheitsdomäne eingeben, verwendet der Befehl den Wert in der Umgebungsvariablen INFA_DEFAULT_SECURITY_DOMAIN. Sie können als Wert „Native“, „LDAP“ oder „SSO“ verwenden. Der Standardwert ist „Native“.
-folderNames -f	Pc_Folder_Names	Erforderlich. PowerCenter-Ordner, die die wiederzuverwendenden Objekte enthalten. Die Ordnernamen können Ausdrücke enthalten. Die Ordnernamen können * als Ausdrücke enthalten. **Hinweis:** Wenn Sie die Linux-Umgebung verwenden, dürfen Sie „$“ nicht im Ordnernamen verwenden.

-SrcRelease
-srel
	Pc_Release_version	Erforderlich. Die Release-Version des PowerCenter-Repository-Diensts.
		Geben Sie die Version im folgenden Format ein:
		`9.6.x`
		Geben Sie beispielsweise eine Version im folgenden Format ein:
		`9.6.1`

Option	Argument	Beschreibung

-targetRelease
-trel
	Target_Release_version	Optional. Die Release-Version von Big Data Management. Wenn Sie keine Version eingeben, verwendet der Befehl die Produktversion. Sie können Versionen ab 10.0.0 eingeben.
		Geben Sie die Version im folgenden Format ein:
		`10.0.x`
		Geben Sie beispielsweise eine Version im folgenden Format ein:
		`10.0.0`

-CodePage -cp	Pc_Repository_code_page	Optional. Codepage des PowerCenter-Repository. Standardwert ist UTF-8.

-targetDir
-td
	Target_Directory	Erforderlich. Speicherort des Zielverzeichnisses im Modellrepository auf dem Computer, auf dem infacmd-Client und -Server ausgeführt werden. Sie müssen im Zielverzeichnisordner über Berechtigungen zum Lesen, Schreiben und Ausführen verfügen.
		Geben Sie beispielsweise den Speicherort des infacmd-Clients im folgenden Format ein:
		`installed_location_of_client\clients\DeveloperClient\infacmd`
		Geben Sie beispielsweise den Speicherort des infacmd-Servers im folgenden Format ein:
		`installed_location_of_server\isp\bin`
		Hinweis: Wenn Sie die Linux-Umgebung verwenden, dürfen Sie „$“ nicht im Namen des Zielverzeichnisses verwenden.

authenticationType -at	Authentication_Type	Erforderlich. Der Typ der Benutzerauthentifizierung für die Domäne. Geben Sie einen der folgenden Werte ein: „LDAP“, „Native“ oder „Kerberos Single Sign On“.
-LogFile -lf	Log_file_Name	Optional. Name der generierten Protokolldatei. Wenn Sie keinen Namen eingeben, druckt der Befehl die Protokolle auf der Konsole. Verwendet den Wert von file_path/file_name. Wenn Sie einen Dateinamen eingeben, wird die Protokolldatei mit demselben Namen im infacmd-Ordner angezeigt. Wenn Sie einen Verzeichnispfad eingeben, der nicht gültig ist, wird die Protokolldatei mit dem Pfadnamen im infacmd-Ordner angezeigt. Wenn Sie beispielsweise „x“ als Verzeichnispfad eingeben, wird die Protokolldatei mit dem Namen „x“ im infacmd-Ordner angezeigt.

KAPITEL 14

Infacmd isp-Befehlsreferenz

Das infacmd isp-Programm verwaltet die Informatica-Domäne, die Sicherheit und die PowerCenter-Anwendungsdienste. Sie können Informatica-Dienste mit infacmd isp-Befehlen aktivieren und deaktivieren.

Das infacmd isp-Programm aktualisiert die Konnektivitätsinformationen des Gateway-Knotens und gibt den Namen des Knotens zurück.

Dieses Kapitel umfasst die Befehle, die Sie mit dem infacmd isp-Programm verwenden können.

AddAlertUser

Abonniert Alarm-E-Mail-Nachrichten für einen Benutzer. Bevor Sie Alarme für einen Benutzer abonnieren können, müssen Sie die SMTP-Einstellungen für den ausgehende Mailserver konfigurieren. Sie können „infacmd isp AddAlertUser“ für alle Benutzer ausführen.

Wenn Sie Alarme abonnieren, erhalten Sie Domänen- und Dienstbenachrichtigungen per E-Mail für diejenigen Objekte, für die Sie Berechtigungen haben.

Der Befehl „infacmd isp AddAlertUser“ verwendet die folgende Syntax:

```
AddAlertUser

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

[<-SecurityDomain|-sdn> security_domain]

<-Password|-pd> password

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-AlertUser|-au> user_name
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AddAlertUser“ beschrieben:

Option	Argument	Beschreibung
–DomainName –dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
–UserName –un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
–Gateway –hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Gateway-Konnektivitätsinformationen in der Datei „domains.infa“ veraltet sind. Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
–ResilienceTimeout –re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
–AlertUser –au	user_name	Erforderlich. Name des Benutzers, für den Sie Alarme abonnieren möchten.

Verwandte Themen:

- "UpdateSMTPOptions" auf Seite 652

AddConnectionPermissions

Weist einem Benutzer oder einer Gruppe Verbindungsberechtigungen zu.

Der Befehl „infacmd isp AddConnectionPermissions" verwendet die folgende Syntax:

```
AddConnectionPermissions

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<<-RecipientUserName|-run> recipient_user_name|<RecipientGroupName|-rgn>
recipient_group_name>

<-RecipientSecurityDomain|-rsd> recipient_security_domain]

<-ConnectionName|-cn> connection_name

[<-Permission|-p> permission_READ|WRITE|EXECUTE|GRANT|ALL
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AddConnectionPermissions" beschrieben:

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

Option	Argument	Beschreibung
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-RecipientUserName -run	recipient_user_name	Erforderlich, wenn Sie den Gruppennamen des Empfängers nicht angeben. Name des Benutzers, dem die Verbindungsberechtigung zugewiesen ist.
-RecipientGroupName -rgn	recipient_group_name	Erforderlich, wenn Sie den Benutzernamen des Empfängers nicht angeben. Name der Gruppe, der die Verbindungsberechtigung zugewiesen ist.
-RecipientSecurityDomain -rsd	recipient_security_domain_name	Erforderlich, wenn der Empfänger zu einer LDAP-Sicherheitsdomäne gehört. Name der Sicherheitsdomäne, zu der der Empfänger gehört. Standardwert ist „Native“.

Option	Argument	Beschreibung
-ConnectionName -cn	connection_name_security_domain	Erforderlich. Name der Verbindung
-Permission -p	permission	Erforderlich. Typ der zuzuweisenden Berechtigung. Geben Sie mindestens einen der folgenden Werte durch Leerzeichen getrennt ein: - READ - WRITE. Lesen und Schreiben - EXECUTE - GRANT. Lesen und Gewähren - ALL. Lesen, Schreiben, Ausführen, Gewähren

AddDomainLink

Fügt einer Domäne einen Link hinzu. Zeichnet Verbindungseigenschaften für eine Remotedomäne oder eine verknüpfte Domäne auf, sodass Sie Repository-Metadaten zwischen der lokalen Domäne und der verknüpften Domäne austauschen können.

Möglicherweise möchten Sie einen Link zu einer Domäne hinzufügen, wenn Sie auf einen PowerCenter-Repository-Dienst in dieser Domäne zugreifen müssen.

Sie können einen Link zu einer anderen Informatica-Domäne hinzufügen, wenn Sie ein lokales Repository mit einem globalen Repository in einer anderen Informatica-Domäne registrieren oder die Registrierung aufheben.

Der Befehl „infacmd isp AddDomainLink“ verwendet die folgende Syntax:

```
AddDomainLink

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-LinkedDomainName|-ld> linked_domain_name

<-DomainLink|-dl> domain_host1:port domain_host2:port...
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AddDomainLink“ beschrieben:

Option	Argument	Beschreibung
–DomainName –dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
–UserName –un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
–Password –pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
–Gateway –hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der lokalen Domäne.

Option	Argument	Beschreibung
–ResilienceTimeout –re	timeout_period_in_seconds	Optional. Zeitraum in Sekunden, in dem infacmd versucht, eine Verbindung zur lokalen Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
–LinkedDomainName –ld	linked_domain_name	Erforderlich. Name der Domäne, mit der Sie eine Verbindung herstellen möchten.
–DomainLink –dl	gateway_host1:port gateway_host2:port ...	Erforderlich. Die Hostnamen und Portnummern für die Gateway-Knoten in der verknüpften Domäne.

AddDomainNode

Fügt der Domäne einen Knoten hinzu. Bevor Sie den Knoten starten können, müssen Sie ihn definieren, indem Sie infasetup DefineGatewayNode oder DefineWorkerNode auf dem Knoten ausführen.

Der Befehl „infacmd isp AddDomainNode“ verwendet die folgende Syntax:

```
AddDomainNode

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name

[<-FolderPath|-fp> full_folder_path]

[<-EnableServiceRole|-esr> true|false]

[<-EnableComputeRole|-ecr> true|false]
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AddDomainNode“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-NodeName -nn	node_name	Erforderlich. Name des Knotens, den Sie der Domäne hinzufügen möchten.
-FolderPath -fp	full_folder_path	Optional. Vollständiger Pfad (ohne Domänenname) des Ordners, dem Sie den Knoten hinzufügen möchten. Folgendes Format ist erforderlich: */parent_folder/child_folder* Standardwert ist „/“ (die Domäne).
-EnableServiceRole -esr	true | false	Optional. Aktiviert die Dienstrolle auf dem Knoten. Bei „True“ können Anwendungsdienste auf dem Knoten ausgeführt werden. Bei „False“ können Anwendungsdienste nicht auf dem Knoten ausgeführt werden. Legen Sie den Befehl nur auf „False“ fest, wenn der Knoten einem Datenintegrationsdienst-Gitter zugewiesen ist und Sie den Knoten für ausgeführte Mappings dedizieren möchten. Standardwert ist „True“.
-EnableComputeRole -esr	true | false	Optional. Aktiviert die Berechnungsrolle auf dem Knoten. Bei „True“ kann der Knoten Berechnungen durchführen, die von Remote-Anwendungsdiensten angefragt werden. Bei „False“ kann der Knoten keine von Remote-Anwendungsdiensten angefragten Berechnungen durchführen. Für einen Knoten ist die Berechnungsrolle erforderlich, wenn der Datenintegrationsdienst Jobs auf diesem Knoten ausführt. Wenn der Datenintegrationsdienst auf diesem Knoten keine Jobs ausführt, können Sie die Berechnungsrolle deaktivieren. Eine aktivierte oder deaktivierte Berechnungsrolle hat allerdings keine Auswirkungen auf die Leistung. Standardwert ist „True“.

AddGroupPrivilege

Weist einer Gruppe in der Domäne eine Berechtigung zu. Sie können einer Gruppe Berechtigungen für die Domäne zuweisen. Sie können ebenfalls Gruppenberechtigungen für jeden Anwendungsdienst in der Domäne zuweisen.

Der Befehl „infacmd isp AddGroupPrivilege“ verwendet die folgende Syntax:

```
AddGroupPrivilege

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-GroupName|-gn> group_name
```

```
[<-GroupSecurityDomain|-gsf> group_security_domain]

<-ServiceName|-sn> service_name

<-PrivilegePath|-pp> path_of_privilege
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AddGroupPrivilege“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Bei der Sicherheitsdomäne wird die Groß-/Kleinschreibung beachtet. Standardwert ist „Native“.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-GroupName -gn	group_name	Erforderlich. Name der Gruppe, der Sie die Berechtigung zuweisen. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-GroupSecurityDomain -gsf	group_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der die Gruppe gehört, der Sie die Berechtigung zuweisen. Standardwert ist „Native“.
-ServiceName -sn	service_name	Erforderlich. Domäne oder Anwendungsdienstname, für die bzw. den Sie Berechtigungen anzeigen möchten.

-PrivilegePath
-pp
	path_of_privilege	Erforderlich. Vollqualifizierter Name der Berechtigung, die Sie der Gruppe zuweisen möchten. Ein vollqualifizierter Name enthält den Namen der Berechtigungsgruppe und den Namen der Berechtigung. Ein vollqualifizierter Berechtigungsname für den Repository-Dienst ist z. B. „folder/create“. Wenn der Berechtigungsname Leerzeichen enthält, setzen Sie den Pfad in Anführungszeichen wie folgt:
		`“Runtime Objects/Monitor/Execute/Manage Execution”`
		Wenn der Berechtigungsname das Sonderzeichen „/“ enthält, fügen Sie das Escape-Zeichen „\“ davor folgendermaßen ein:
		`“Model/View Model/Export\/Import Models”`

AddLicense

Fügt der Domäne eine Lizenz hinzu. Nachdem Sie eine Lizenz hinzugefügt haben, können Sie sie mit dem AssignLicence-Befehl zu einem Anwendungsdienst zuweisen. Sie müssen einem Dienst eine Lizenz zuweisen, bevor Sie den Dienst verwenden können.

Der Befehl „infacmd isp AddLicense“ verwendet die folgende Syntax:

```
AddLicense

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> securitydomain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-LicenseName|-ln> license_name

<-LicenseKeyFile|-lf> license_key_file

[<-FolderPath|-fp> full_folder_path]
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AddLicense“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-LicenseName -ln	license_name	Erforderlich. Name der Lizenz. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf maximal 79 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten: `/ * ? < > " |`
-LicenseKeyFile -lf	license_key_file	Erforderlich. Pfad zur Lizenzschlüsseldatei.
-FolderPath -fp	full_folder_path	Optional. Vollständiger Pfad (ohne Domänenname) des Ordners, dem Sie die Lizenz hinzufügen möchten. Folgendes Format ist erforderlich: */parent_folder/child_folder* Standardwert ist „/“ (die Domäne).

AddNamespace

Erstellt eine LDAP-Sicherheitsdomäne und setzt die Filter so, dass nach Benutzern oder Gruppen im Verzeichnisdienst gesucht wird. Erstellt die LDAP-Sicherheitsdomäne, wenn die Informatica-Domäne LDAP oder die Kerberos-Authentifizierung verwendet.

Der Befehl „infacmd isp AddNamespace“ verwendet die folgende Syntax:

```
AddNamespace
 <-DomainName|-dn> domain_name
 <-UserName|-un> user_name
 <-Password|-pd> password
 [<-SecurityDomain|-sdn> security_domain]
 [<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
 [<-ResilienceTimeout|-re> timeout_period_in_seconds]
 <-NameSpace|-ns> namespace
 [<-UserSearchBase|-usb> usersearchbase]
 [<-UserFilter|-uf> userfilter]
 [<-GroupSearchBase|-gsb> groupsearchbase]
 [<-GroupFilter|-gf> groupfilter]
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AddNamespace“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Sie können einen Wert für -sdn angeben oder den Standardwert basierend auf dem Authentifizierungsmodus verwenden: - Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Standardwert ist „Native“. Zum Arbeiten mit der LDAP-Authentifizierung müssen Sie den Wert für -sdn angeben. - Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Standardwert ist „Native“ für native Authentifizierung. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn Sie die Umgebungsvariable nicht angeben, wird der Standardwert von 180 Sekunden verwendet.
-NameSpace -ns	namespace	Erforderlich. Name der LDAP- oder Kerberos-Sicherheitsdomäne, die Sie hinzufügen möchten. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf weder Leerzeichen noch folgende Sonderzeichen enthalten: , + / < > @ ; \ % ? Der Name darf nicht länger als 128 Zeichen sein. Der Name kann ein ASCII-Leerzeichen enthalten, jedoch nicht als erstes oder letztes Zeichen. Sie können keine anderen Leerzeichen verwenden.
-UserSearchBase -usb	usersearchbase	Distinguished Name (DN) des Eintrags, der als Ausgangspunkt für die Suche nach Benutzernamen im LDAP-Verzeichnisdienst dient. Der LDAP-Verzeichnisdienst sucht nach einem Objekt im Verzeichnis entsprechend dem Pfad im Distinguished Name des Objekts. Beispiel: In Microsoft Active Directory könnte der Distinguished Name des Benutzers cn=UserName,ou=OrganizationalUnit,dc=DomainName lauten. Die Reihe der durch dc=DomainName benannten relativen Distinguished Names kennzeichnet die DNS-Domäne des Objekts.
-UserFilter -uf	userfilter	Ein LDAP-Abfragestring, der die Suchkriterien für die Suche nach Benutzern im Verzeichnisdienst festgelegt. Der Filter kann Attributtypen, Assertionswerte und Abgleichkriterien angeben. Beispiel: Der Filter `(objectclass=*)` sucht alle Objekte. Der Filter `(&(objectClass=user)(!(cn=susan)))` sucht alle Benutzerobjekte außer „susan“. Weitere Informationen über Suchfilter finden Sie in der Dokumentation für den LDAP-Verzeichnisdienst:
-GroupSearchBase -gsb	groupsearchbase	Distinguished Name (DN) des Eintrags, der als Ausgangspunkt für die Suche nach Gruppennamen im LDAP-Verzeichnisdienst dient.
-GroupFilter -gf	groupfilter	Ein LDAP-Abfragestring, der die Kriterien für die Suche nach Gruppen im Verzeichnisdienst festgelegt.

AddNodeResource

Fügt eine benutzerdefinierte Ressource oder eine Dateiverzeichnisressource zu einem Knoten hinzu.

Wenn ein PowerCenter-Integrationsdienst in einem Gitter ausgeführt wird, kann der Load Balancer Ressourcen verwenden, um Sitzungs-, Befehls- und vordefinierte Event-Wait-Aufgaben zu verteilen. Wenn der

PowerCenter-Integrationsdienst für die Überprüfung von Ressourcen konfiguriert ist, verteilt der Load Balancer Aufgaben an Knoten, auf denen Ressourcen hinzugefügt und aktiviert werden.

Der Befehl „infacmd isp AddNodeResource“ verwendet die folgende Syntax:

```
AddNodeResource

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name

[<-ResourceCategory|-rc> resource_category ("PCIS", "DIS")]

<-ResourceType|-rt> resource_type("Custom", "File Directory")

<-ResourceName|-rn> resource_name

[<-ResourceValue|-rv> resource_value]
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AddNodeResource“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem Sie eine Ressource hinzufügen möchten.
-ResourceCategory -rc	resource_category	Optional. Kategorie der Ressource. Gültige Kategorien umfassen: - PCIS. Ressource für den PowerCenter-Integrationsdienst. - DIS. Für zukünftige Verwendung reserviert. Standardwert ist PCIS.
-ResourceType -rt	resource_type	Erforderlich. Typ der Ressource. Gültige Typen umfassen: - Benutzerdefiniert - Dateiverzeichnis
-ResourceName -rn	resource_name	Erforderlich. Name der Ressource. Der Name darf maximal 79 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten: `\ / * ? < > " | $`
-ResourceValue -rv	resource_value	Optional. Für zukünftige Verwendung reserviert.

AddRolePrivilege

Weist einer Rolle in der Domäne eine Berechtigung zu. Sie können einer Rolle Berechtigungen für die Domäne zuweisen. Sie können ebenfalls Rollenberechtigungen für jeden Anwendungsdienst in der Domäne zuweisen.

Der Befehl „infacmd isp AddRolePrivilege“ verwendet die folgende Syntax:

```
AddRolePrivilege

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-RoleName|-rn> role_name

<-ServiceType|-st> service_type AS|CMS|MM|MRS|RPS|RS|DOMAIN

<-PrivilegePath|-pp> path_of_privilege
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AddRolePrivilege“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Gateway-Konnektivitätsinformationen in der Datei „domains.infa“ veraltet sind. Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-RoleName -rn	role_name	Erforderlich. Name der Rolle, der Sie die Berechtigung zuweisen. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

Option	Argument	Beschreibung
-ServiceType -st	service_type	Erforderlich. Domäne oder Anwendungsdiensttyp, der bzw. dem Sie die Berechtigung für die Rolle zuweisen. Diensttypen umfassen: - AS. Analyst-Dienst - CMS. Content-Managementdienst - MM. Metadata Manager-Dienst - MRS. Modellrepository-Dienst - RPS. Berichterstellungsdienst - RS. PowerCenter-Repository-Dienst - DOMAIN. Domäne

-PrivilegePath
-pp
	path_of_privilege	Erforderlich. Vollqualifizierter Name der Berechtigung, die Sie der Gruppe zuweisen möchten. Ein vollqualifizierter Name enthält den Namen der Berechtigungsgruppe und den Namen der Berechtigung. Ein vollqualifizierter Berechtigungsname für den Repository-Dienst ist z. B. „folder/create“. Wenn der Berechtigungsname Leerzeichen enthält, setzen Sie den Pfad wie folgt in Anführungszeichen:
		`“Runtime Objects/Monitor/Execute/Manage Execution”`
		Wenn der Berechtigungsname das Sonderzeichen „/“ enthält, fügen Sie das Escape-Zeichen „/“ davor folgendermaßen ein:
		`“Model/View Model/Export\/Import Models”`

AddServiceLevel

Fügt eine Dienstebene hinzu.

Dienstebenen geben eine Priorität unter den Aufgaben an, die darauf warten, versendet zu werden. Sie können unterschiedliche Dienstebenen erstellen, die ein Aufgabenentwickler Arbeitsabläufen zuweisen kann.

Jede Dienstebene, die Sie erstellen, hat einen Namen, eine Dispatch-Priorität und eine maximale Dispatch-Wartezeit. Die Dispatch-Priorität ist eine Zahl, mit der die Priorität für den Versand angegeben ist. Der Load Balancer versendet zuerst Aufgaben mit einer hohen Priorität, dann Aufgaben mit niedriger Priorität. Die maximale Dispatch-Wartezeit gibt an, wie lange der Load Balancer wartet, bevor die Dispatch-Priorität für eine Aufgabe in die höchste Priorität geändert wird.

Der Befehl „infacmd isp AddServiceLevel“ verwendet die folgende Syntax:

```
AddServiceLevel

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> securitydomain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceLevelName|-ln> service_level_name
```

```
<-ServiceLevel|-sl> option_name=value ...
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AddServiceLevel“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Gateway-Konnektivitätsinformationen in der Datei „domains.infa“ veraltet sind. Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-ServiceLevelName -ln	service_level_name	Erforderlich. Name der Dienstebene.
-ServiceLevel -sl	option_name=value	Erforderlich. Die Eigenschaften der Dienstebene. Sie können die folgenden Eigenschaften festlegen: - DispatchPriority. Die anfängliche Priorität für den Versand. Kleinere Zahlen haben höhere Priorität. Priorität 1 ist die höchste Priorität. Standardwert ist „5“. - MaxDispatchWaitTime. Der Zeitraum in Sekunden, bevor der Load Balancer die Dispatch-Priorität für eine Aufgabe in die höchste Priorität ändert. Standardwert ist „1800“.

AddUserPrivilege

Weist einem Benutzer in der Domäne eine Berechtigung zu. Sie können ebenfalls Benutzerberechtigungen für jeden Anwendungsdienst in der Domäne zuweisen.

Der Befehl „infacmd isp AddUserPrivilege“ verwendet die folgende Syntax:

```
AddUserPrivilege

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ExistingUserName|-eu> existing_user_Name

[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]

<-ServiceName|-sn> service_name

<-PrivilegePath|-pp> path_of_privilege
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AddUserPrivilege“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ExistingUserName -eu	existing_user_name	Erforderlich. Benutzerkonto, dem Sie die Berechtigung zuweisen. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört, dem Sie die Berechtigung zuweisen. Standardwert ist „Native“.
-ServiceName -sn	service_name	Erforderlich. Domäne oder Anwendungsdienstname, für die bzw. den Sie Berechtigungen anzeigen möchten.

-PrivilegePath
-pp
	path_of_privilege	Erforderlich. Vollqualifizierter Name der Berechtigung, die Sie der Gruppe zuweisen möchten. Ein vollqualifizierter Name enthält den Namen der Berechtigungsgruppe und den Namen der Berechtigung. Ein vollqualifizierter Berechtigungsname für den Repository-Dienst ist z. B. „folder/create“. Wenn der Berechtigungsname Leerzeichen enthält, setzen Sie den Pfad wie folgt in Anführungszeichen:
		`“Runtime Objects/Monitor/Execute/ Manage Execution”`
		Wenn der Berechtigungsname das Sonderzeichen „/“ enthält, fügen Sie das Escape-Zeichen „\“ davor folgendermaßen ein:
		`“Model/View Model/Export\ /Import Models”`

AddUserToGroup

Fügt einer nativen Gruppe in der Domäne einen nativen oder LDAP-Benutzer hinzu. Der Benutzer erbt alle Berechtigungen, die mit Gruppe verbunden sind.

Der Befehl „infacmd isp AddUserToGroup“ verwendet die folgende Syntax:

```
AddUserToGroup

<-DomainName|-dn> domain_name

<-UserName|-un> user_name
```

```
<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ExistingUserName|-eu> existing_user_Name

[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]

<-GroupName|-gn> group_name
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AddUserToGroup“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ExistingUserName -eu	existing_user_Name	Erforderlich. Name des Benutzers, den Sie hinzufügen möchten.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört, den Sie hinzufügen möchten. Standardwert ist „Native“.
-GroupName -gn	group_name	Erforderlich. Name der Gruppe, der Sie den Benutzer hinzufügen möchten.

AssignDefaultOSProfile

Weist ein Standardbetriebssystemprofil einem Benutzer oder einer Gruppe zu.

Der Befehl „infacmd isp AssignDefaultOSProfile“ verwendet die folgende Syntax:

```
AssignDefaultOSProfile

<-DomainName|-dn> domain_name
```

```
<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-OSProfileName|-on> OSProfile_name

<-RecipientName|-nm> recipient_name

<-RecipientSecurityDomain|-ns> security_domain_of_recipient

<-RecipientType|-ty> recipient_type
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp AssignDefaultOSProfile“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-OSProfileName -on	OSProfile_name	Erforderlich. Name des Betriebssystemprofils. Der Name des Betriebssystemprofils kann bis zu 80 Zeichen enthalten. Er darf weder Leerzeichen noch die folgenden Sonderzeichen enthalten: `% * + \ / ? ; < >`
-RecipientName -nm	recipient_name	Erforderlich. Benutzer- oder Gruppenname, der dem Standardbetriebssystemprofil zugewiesen wird.
-RecipientSecurityDomain -ns	security_domain_of_recipient	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden und Benutzerberechtigungen gewähren. Name der Sicherheitsdomäne, zu der der Benutzer gehört.
-RecipientType -ty	recipient_type	Erforderlich. Geben Sie an, ob das Standardbetriebssystemprofil einem Benutzer oder einer Gruppe zugewiesen werden soll. Geben Sie einen der folgenden Werte ein: - UserIdentity - GroupIdentity

AssignedToLicense

Listet die Dienste auf, die einer Lizenz zugewiesen sind. Sie können die Dienste auflisten, die einer Lizenz aktuell zugewiesen sind.

Der Befehl „infacmd isp AssignedToLicense“ verwendet die folgende Syntax:

```
AssignedToLicense

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-LicenseName|-ln> license_name
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AssignedToLicense“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-LicenseName -ln	license_name	Erforderlich. Name der Lizenz.

AssignGroupPermission

Weist einem Objekt eine Gruppenberechtigung zu.

Mit Berechtigungen kann eine Gruppe auf Objekte in einer Domäne zugreifen. Objekte beinhalten die Domäne, Ordner, Knoten, Gitter, Lizenzen und Anwendungsdienste. Wenn Sie beispielsweise eine Gruppenberechtigung einem Ordner zuweisen, erbt die Gruppe die Berechtigung für alle Objekte in diesem Ordner.

Der Befehl „infacmd isp AssignGroupPermission“ verwendet die folgende Syntax:

```
AssignGroupPermission

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ExistingGroup|-eg> existing_group_name
```

```
[<-GroupSecurityDomain|-gsf> group_security_domain]

<-ObjectName|-on> object_name

<-ObjectType|-ot> object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AssignGroupPermission“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ExistingGroup -eg	existing_group_name	Erforderlich. Name der Gruppe, der Sie eine Berechtigung für ein Objekt zuweisen möchten.
-GroupSecurityDomain -gsf	group_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der die Gruppe gehört, der Sie eine Berechtigung zuweisen möchten. Standardwert ist „Native“.
-ObjectName -on	object_name	Erforderlich. Name des Objekts, dem Sie die Gruppenzugriffsberechtigung zuweisen möchten.
-ObjectType -ot	object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE	Erforderlich. Typ des Objekts Geben Sie einen der folgenden Werte ein: - Dienst - Lizenz - Knoten - Gitter - Folder - OSProfile

AssignISToMMService

Weist den zugeordneten PowerCenter-Integrationsdienst einem Metadata Manager-Dienst zu.

Der Befehl „infacmd isp AssignISToMMService“ verwendet die folgende Syntax:

```
AssignISToMMService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> securitydomain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-IntegrationService|-is> integration_service_name

[<-RepositoryUserSecurityDomain|-rsdn> repository_user_security_domain]

<-RepositoryUser|-ru> repository_user

<-RepositoryPassword|-rp> repository_password
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AssignISToMMService“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des Metadata Manager-Diensts, dem Sie den Integrationsdienst zuweisen möchten.
-IntegrationService -is	integration_service_name	Erforderlich. Name des PowerCenter-Integrationsdiensts, den Sie dem Metadata Manager-Dienst zuweisen möchten.
-RepositoryUserSecurityDomain -rsdn	repository_user_security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung oder Kerberos-Authentifizierung verwendet. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der PowerCenter-Repository-Benutzer gehört. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn Sie diese Option nicht festlegen, setzt der Befehl die Sicherheitsdomäne des Repository-Benutzers auf die in der Option -sdn angegebene Sicherheitsdomäne.
-RepositoryUser -ru	repository_user	Erforderlich. Name des PowerCenter-Repository-Benutzers.
-RepositoryPassword -rp	repository_password	Erforderlich. Passwort für den PowerCenter-Repository-Benutzer. Benutzerpasswort. Sie können ein Passwort mit der Option -rp oder der Umgebungsvariable INFA_REPOSITORY_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -rp festgelegte Passwort Vorrang.

AssignLicense

Weist einem Anwendungsdienst eine Lizenz zu. Sie müssen einem Anwendungsdienst eine Lizenz zuweisen, bevor Sie den Dienst aktivieren können.

Hinweis: Sie können einem Dienst keine Lizenz zuweisen, wenn der Dienst einer anderen Lizenz zugeordnet ist. Um einem Dienst eine andere Lizenz zuzuweisen, entfernen Sie mit dem Befehl „RemoveLicense“ die vorhandene Lizenz aus dem Dienst und weisen dem Dienst dann die neue Lizenz zu.

Der Befehl „infacmd isp AssignLicense“ verwendet die folgende Syntax:

```
AssignLicense

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-LicenseName|-ln> license_name

<-ServiceNames|-sn> service1_name service2_name ...
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AssignLicense“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-LicenseName -ln	license_name	Erforderlich. Name der Lizenz, die Sie einem Dienst zuweisen möchten.
-ServiceNames -sn	service_name1 service_name2 ...	Erforderlich. Namen der Dienste, für die Sie eine Lizenz zuweisen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen. Starten Sie den Dienst neu, um die Änderungen anzuwenden.

AssignRoleToGroup

Weist eine Rolle zu einer Gruppe für eine Domäne oder einen Anwendungsdienst zu.

Der Befehl „infacmd isp AssignRoleToGroup“ verwendet die folgende Syntax:

```
AssignRoleToGroup

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

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

```
<-GroupName|-gn> group_name

[<-GroupSecurityDomain|-gsf> group_security_domain]

<-RoleName|-rn> role_name

<-ServiceName|-sn> service_name
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AssignRoleToGroup“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Gateway-Konnektivitätsinformationen in der Datei „domains.infa“ veraltet sind. Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-GroupName -gn	group_name	Erforderlich. Name der Gruppe, der Sie die Rolle zuweisen. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-GroupSecurityDomain -gsf	group_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der die Gruppe gehört, der Sie die Rolle zuweisen. Standardwert ist „Native“.
-RoleName -rn	role_name	Erforderlich. Name der Rolle, die Sie einer Gruppe zuweisen möchten.
-ServiceName -sn	service_name	Erforderlich. Domäne oder Anwendungsdienstname, für die bzw. den Sie die Rolle zuweisen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

AssignRoleToUser

Weist eine Rolle zu einem Benutzer für eine Domäne oder einen Anwendungsdienst zu.

Der Befehl „infacmd isp AssignRoleToUser“ verwendet die folgende Syntax:

```
AssignRoleToUser

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ExistingUserName|-eu> existing_user_Name

[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]

<-RoleName|-rn> role_name

<-ServiceName|-sn> service_name
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AssignRoleToUser“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Gateway-Konnektivitätsinformationen in der Datei „domains.infa“ veraltet sind. Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ExistingUserName -eu	existing_user_Name	Erforderlich. Benutzerkonto, dem Sie die Rolle zuweisen. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört, dem Sie die Rolle zuweisen. Standardwert ist „Native“.
-RoleName -rn	role_name	Erforderlich. Name der Rolle, die Sie dem Benutzer zuweisen möchten.
-ServiceName -sn	service_name	Erforderlich. Domäne oder Anwendungsdienstname, für die bzw. den Sie die Rolle zuweisen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

AssignRSToWSHubService

Verbindet ein PowerCenter-Repository mit einem Webdienst-Hub in der Domäne.

Der Befehl „infacmd isp AssignRSToWSHubService“ verwendet die folgende Syntax:

```
AssignRSToWSHubService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-NodeName|-nn> node_name

<-RepositoryService|-rs> repository_service_name

<-RepositoryUser|-ru> user
```

```
<-RepositoryPassword|-rp> password
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp AssignRSToWSHubService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des Webdienst-Hubs, dem Sie ein Repository zuordnen möchten.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Webdienst-Hub-Prozess ausgeführt werden soll. Wenn die PowerCenter-Umgebung für hohe Verfügbarkeit konfiguriert ist, gibt diese Option den Namen des primären Knotens an.
-RepositoryService -rs	repository_service_name	Erforderlich. Name des PowerCenter-Repository-Diensts, von dem der Webdienst-Hub abhängig ist. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RepositoryUser -ru	user	Erforderlich. Benutzername zum Herstellen einer Verbindung zum Repository. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RepositoryPassword -rp	Passwort	Erforderlich. Benutzerpasswort. Benutzerpasswort. Sie können ein Passwort mit der Option -rp oder der Umgebungsvariable INFA_REPOSITORY_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -rp festgelegte Passwort Vorrang.

AssignUserPermission

Weist einem Objekt eine Benutzerberechtigung zu.

Mit Berechtigungen kann ein Benutzer auf Objekte in einer Domäne zugreifen. Objekte beinhalten die Domäne, Ordner, Knoten, Gitter, Lizenzen und Anwendungsdienste. Wenn Sie beispielsweise eine Benutzerberechtigung einem Ordner zuweisen, erbt der Benutzer die Berechtigung für alle Objekte in diesem Ordner.

Der Befehl „infacmd isp AssignUserPermission“ verwendet die folgende Syntax:

```
AssignUserPermission

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password
```

```
[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ExistingUserName|-eu> existing_user_name

[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]

<-ObjectName|-on> object_name

<-ObjectType|-ot> object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE
```

In der folgenden Tabelle werden Optionen und Argumente für „*infacmd isp* AssignUserPermission“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Gateway-Konnektivitätsinformationen in der Datei „domains.infa“ veraltet sind. Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert.
-ExistingUserName -eu	existing_user_name	Erforderlich. Name des Benutzers, dem Sie eine Berechtigung für ein Objekt zuweisen möchten.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört, dem Sie eine Berechtigung zuweisen möchten. Standardwert ist „Native“.
-ObjectName -on	object_name	Erforderlich. Name des Objekts, dem Sie die Benutzerzugriffsberechtigung zuweisen möchten.
-ObjectType -ot	object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE	Erforderlich. Typ des Objekts Geben Sie einen der folgenden Werte ein: - Dienst - Lizenz - Knoten - Gitter - Folder - OSProfile

ConvertLogFile

Wandelt binäre Protokolldateien in Textdateien, XML-Dateien oder auf dem Bildschirm lesbaren Text um.

Der infacmd isp ConvertLogFile-Befehl verwendet die folgende Syntax:

```
ConvertLogFile

<-InputFile|-in> input_file_name

[<-Format|-fm> format_TEXT_XML]

[<-OutputFile|-lo> output_file_name]
```

In der folgenden Tabelle werden infacmd isp ConvertLogFile-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-InputFile -in	input_file_name	Erforderlich. Name und Pfad für die Protokolldatei, die Sie umwandeln möchten. Standardmäßig schreibt der Service Manager Protokolldateien in das Verzeichnis "server\infa_shared\log" auf dem Master-Gateway-Knoten.
-Format -fm	format	Optional. Format der Ausgabedatei. Gültige Typen umfassen: - Text - XML Wenn Sie kein Format angeben, verwendet infacmd Textformat mit einer Zeilenlänge von 80 Zeichen.
-OutputFile -lo	output_file_name	Optional. Name und Dateipfad für die Ausgabedatei. Wenn Sie keinen Ausgabedateinamen angeben, zeigt infacmd die Protokollereignisse auf dem Bildschirm an.

convertUserActivityLogFile

Wandelt eine mit dem getUserActivityLog-Befehl abgerufene binäre Benutzeraktivitäts-Protokolldatei in Text- oder XML-Format um.

Der infacmd isp convertUserActivityLogFile-Befehl verwendet die folgende Syntax:

```
convertUserActivityLogFile

<-InputFile|-in> input_file_name

[<-Format|-fm> format_TEXT_XML]

[<-OutputFile|-lo> output_file_name]
```

In der folgenden Tabelle werden infacmd isp convertUserActivityLogFile-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-InputFile -in	input_file_name	Erforderlich. Name der zu konvertierenden Protokolldatei.
-Format -fm	format_TEXT_XML	Optional. Format der Ausgabedatei. Gültige Formate umfassen: - Text - XML Der Standardwert lautet „Text“.
-OutputFile -lo	output_file_name	Optional. Name der Ausgabedatei. Wenn Sie keinen Ausgabedateinamen angeben, zeigt der Befehl das Protokoll in der Befehlszeile an.

CreateConnection

Definiert eine Verbindung und die Verbindungsoptionen.

Führen Sie infacmd isp ListConnectionOptions aus, um Verbindungsoptionen für eine vorhandene Verbindung aufzulisten.

Der Befehl „infacmd isp CreateConnection“ verwendet die folgende Syntax:

```
CreateConnection

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ConnectionName|-cn> connection_name

[<-ConnectionId|-cid> connection_id]

<-ConnectionType|-ct> connection_type

[<-ConnectionUserName|-cun> connection_user_name]

[<-ConnectionPassword|-cpd> connection_password]

[<-VendorId|-vid> vendor_id]

[-o options] (name-value pairs separated by space)
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp CreateConnection“ beschrieben:

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

Option	Argument	Beschreibung
-ConnectionName -cn	connection_name	Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die maximale Länge beträgt 128 Zeichen. Das Leer- und die folgenden Sonderzeichen sind möglich: `~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /`
- ConnectionId -cid	connection_id	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
-ConnectionType -ct	connection_type	Erforderlich. Typ der Verbindung. Verwenden Sie einen der folgenden Verbindungstypen: - ADABAS - DATASIFT - DB2 - DB2I - DB2Z - FACEBOOK - GreenplumPT - HADOOP - HIVE - HadoopFileSystem - IMS - JDBC - LINKEDIN - ODBC - ORACLE - SAP - SEQ - SFDC - SQLSERVER - TWITTER - TWITTERSTREAMING - VSAM - WEBCONTENT - KAPOWKATALYST Sie können den infacmd isp ListConnections-Befehl verwenden, um Verbindungstypen anzuzeigen.
ConnectionUserName -cun	connection_user_name	Erforderlich. Name des Datenbankbenutzers.

Option	Argument	Beschreibung
-ConnectionPassword -cpd	connection_password	Erforderlich. Passwort für den Datenbankbenutzernamen. Sie können ein Passwort mit der Option -cpd oder der Umgebungsvariable INFA_DEFAULT_CONNECTION_PASSWORD festlegen. Wenn Sie das Passwort mit beiden Optionen festlegen, hat das mit der Option -cpd festgelegte Passwort Vorrang. Wenn Sie eine ADABAS-, DB2I-, DB2Z-, IMS-, SEQ- oder VSAM-Verbindung erstellen, können Sie statt eines Passworts eine gültige PowerExchange-Passphrase eingeben. Passphrasen für den Zugriff auf Datenbanken und Datasets auf z/OS können zwischen 9 und 128 Zeichen umfassen. Passphrasen für den Zugriff auf DB2 für i5/OS können maximal 31 Zeichen umfassen. Passphrasen können die folgenden Zeichen enthalten: - Groß- und Kleinbuchstaben - Die Zahlen 0 bis 9 - Leerzeichen - Die folgenden Sonderzeichen: `' - ; # \ , . / ! % & * ( ) _ + { } : @ | < > ?` **Hinweis:** Das erste Zeichen ist ein Apostroph. Passphrasen dürfen keine einfachen Anführungszeichen ('), doppelten Anführungszeichen (") oder Währungssymbole enthalten. Wenn eine Passphrase Leerzeichen enthält, müssen Sie sie in doppelte Anführungszeichen setzen. Beispiel: `„Das ist eine Beispiel-Passphrase“`. Wenn eine Passphrase Sonderzeichen enthält, müssen Sie sie in dreifache doppelte Anführungszeichen (""") setzen. Beispiel: `"""Diese Passphrase enthält Sonderzeichen. % & *."""`. Wenn eine Passphrase nur alphanumerische Zeichen ohne Leerzeichen enthält, können Sie sie ohne Delimiter eingeben. **Hinweis:** Auf z/OS kann eine gültige RACF-Passphrase bis zu 100 Zeichen umfassen. PowerExchange schneidet Passphrases mit mehr als 100 Zeichen ab, wenn diese zur Validierung an RACF übergeben werden. Stellen Sie vor der Verwendung von Passphrasen sicher, dass der PowerExchange-Listenerdienst im DBMOVER-Mitglied mit der Sicherheitseinstellung SECURITY=(1,N) oder höher ausgeführt wird. Weitere Informationen finden Sie unter „SECURITY-Anweisung“ im *PowerExchange-Referenzhandbuch*. Stellen Sie zur Verwendung von Passphrasen für IMS-Verbindungen sicher, dass die folgenden zusätzlichen Anforderungen erfüllt sind: - Sie müssen ODBA-Zugriff auf IMS wie im *PowerExchange-Navigator-Benutzerhandbuch* erläutert konfigurieren. - Sie müssen IMS-Daten-Mappings verwenden, die IMS ODBA als Zugriffsmethode angeben. Verwenden Sie keine Daten-Mappings, die die DL/1 BATCH-Zugriffsmethode angeben, da diese Zugriffsmethode die Verwendung von Netport-Jobs erfordert, die keine Unterstützung für Passphrases bieten. - Die IMS-Datenbank muss im IMS-Kontrollbereich online sein, um ODBA-Zugriff auf IMS zu verwenden.

Option	Argument	Beschreibung
-VendorId -vid	vendor_id	Optional. ID des externen Partners, der den Adapter erstellt hat.
-Options -o	options	Erforderlich. Geben Sie Name-Wert-Paare durch Leerzeichen getrennt ein. Die Verbindungsoptionen sind für jeden Verbindungstyp unterschiedlich.

Adabas-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Adabas-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Adabas-Verbindungsoptionen beschrieben:

Option	Beschreibung
CodePage	Erforderlich. Code zum Lesen aus oder Schreiben in die Datenbank. Verwenden Sie den ISO-Codepage-Namen, z. B. ISO-8859-6. Der Codepage-Name berücksichtigt keine Groß- und Kleinschreibung.
ArraySize	Optional. Bestimmt die Anzahl der Datensätze im Speicher-Array für die Threads, wenn der Worker-Threads-Wert größer als 0 ist. Gültige Werte sind 1 bis 100000. Default is 25.
Compression	Optional. Komprimiert die Daten, um die Menge an Daten zu reduzieren, die Informatica-Anwendungen über das Netzwerk schreiben. TRUE oder FALSE. Die Standardeinstellung ist "false".
EncryptionLevel	Optional. Verschlüsselungsebene für RC2 oder DES für Verschlüsselungstypen. Geben Sie einen der folgenden Werte für die Verschlüsselungsebene ein: - 1. Verwenden Sie einen 56-Bit-Kodierungsschlüssel für DES und RC2. - 2. Verwenden Sie einen 168-Bit-Triple-DES-Kodierungsschlüssel für DES oder einen 64-Bit-Kodierungsschlüssel für RC2. - 3. Verwenden Sie einen 168-Bit-Triple-DES-Kodierungsschlüssel für DES oder einen 128-Bit-Kodierungsschlüssel für RC2. Default is 1. **Hinweis:** Wenn Sie für den Verschlüsselungstyp None auswählen, ignoriert der Data Integration Service den Wert für die Verschlüsselungsebene.
EncryptionType	Optional. Geben Sie einen der folgenden Werte für den Verschlüsselungstyp ein: - Keine - RC2 - DES Die Standardeinstellung ist "None".
InterpretAsRows	Optional. Bei TRUE gibt die Pacing-Größe eine Anzahl von Zeilen wieder. Bei FALSE gibt die Pacing-Größe Kilobyte wieder. Die Standardeinstellung ist "false".

Option	Beschreibung
Location	Speicherort des PowerExchange Listener-Knotens, der eine Verbindung zur Datenbank herstellen kann. Der Speicherort wird im ersten Parameter der NODE-Anweisung in der dbmover.cfg-Konfigurationsdatei von PowerExchange definiert.
OffLoadProcessing	Optional. Verschiebt die Stapeldatenverarbeitung vom Quellcomputer zum Data Integration Service-Computer. Geben Sie einen der folgenden Werte ein: - Auto. Der Data Integration Service bestimmt, ob Offload-Verarbeitung verwendet werden soll. - Yes. Offload-Verarbeitung wird verwendet. - No. Offload-Verarbeitung wird nicht verwendet. Der Standardwert ist Auto.
PacingSize	Optional. Verlangsamt die Datenübertragungsrate, um Engpässe zu reduzieren. Je geringer der Wert ist, desto höher ist die Sitzungsleistung. Der Mindestwert ist 0. Geben Sie 0 für optimale Leistung ein. Default is 0.
WorkerThread	Optional. Anzahl der vom Data Integration Service verwendeten Threads, um Stapeldaten bei aktivierter Offload-Verarbeitung zu verarbeiten. Um eine optimale Leistung zu erzielen, sollte dieser Wert die Anzahl der verfügbaren Prozessoren auf dem Data Integration Service-Computer nicht überschreiten. Gültige Werte sind 1 bis 64. Der Standardwert ist 0, der Multithreading verhindert.
WriteMode	Geben Sie einen der folgenden Schreibmodi ein: - CONFIRMWRITEON. Sendet Daten zum PowerExchange Listener und wartet auf eine Erfolgs-/Nichterfolgsreaktion, bevor weitere Daten gesendet werden. - CONFIRMWRITEOFF. Sendet Daten zum PowerExchange Listener, ohne eine Erfolgs-/Nichterfolgsreaktion abzuwarten. Verwenden Sie diese Option, wenn die Target-Tabelle bei Auftreten eines Fehlers erneut geladen werden kann. - ASYNCHRONOUSWITHFAULTT. Sendet Daten asynchron zum PowerExchange Listener mit der Möglichkeit der Fehlererkennung. Die Standardoption ist CONFIRMWRITEON.
EnableConnectionPool	Optional. Ermöglicht das Verbindungspooling. Wenn Sie Verbindungspooling aktivieren, behält der Verbindungspool inaktive Verbindungsinstanzen im Speicher. Wenn Sie Verbindungspooling deaktivieren, stoppt der Data Integration Service alle Poolingaktivitäten. TRUE oder FALSE. Die Standardeinstellung ist "false".
ConnectionPoolSize	Optional. Maximale Anzahl an inaktiven Verbindungsinstanzen, die der Data Integration Service für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert auf eine höhere Anzahl als die Mindestanzahl an inaktiven Verbindungsinstanzen fest. Default is 15.
ConnectionPoolMaxIdleTime	Optional. Anzahl der Sekunden, die eine die Mindestanzahl an Verbindungsinstanzen überschreitende Verbindung inaktiv bleiben kann, bevor sie vom Verbindungspool abgebrochen wird. Der Verbindungspool ignoriert die Leerlaufzeit, wenn die Mindestanzahl an inaktiven Verbindungsinstanzen nicht überschritten wird. Default is 120.
ConnectionPoolMinConnections	Optional. Die Mindestanzahl an inaktiven Verbindungsinstanzen, die der Pool für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert so fest, dass er der Poolgröße inaktiver Verbindungen gleicht oder kleiner als diese ist. Default is 0.

Verwandte Themen:

- "DataSift-Verbindungsoptionen" auf Seite 293
- "DB2 für i5/OS-Verbindungsoptionen" auf Seite 294
- "Facebook-Verbindungsoptionen" auf Seite 297

- “Greenplum-Verbindungsoptionen” auf Seite 299
- “HBase-Verbindungsoptionen” auf Seite 300
- “HDFS-Verbindungsoptionen” auf Seite 302
- “Hadoop Connection Options” auf Seite 304
- “Hive-Verbindungsoptionen” auf Seite 311
- “ DB2 für z/OS-Verbindungsoptionen” auf Seite 316
- “IBM DB2-Verbindungsoptionen” auf Seite 318
- “IMS-Verbindungsoptionen” auf Seite 322
- “JDBC Connection Options” auf Seite 324
- “LinkedIn-Verbindungsoptionen” auf Seite 327
- “Microsoft SQL Server-Verbindungsoptionen” auf Seite 328
- “Netezza-Verbindungsoptionen” auf Seite 332
- “OData-Verbindungsoptionen” auf Seite 334
- “ ODBC-Verbindungsoptionen” auf Seite 335
- “Oracle-Verbindungsoptionen” auf Seite 338
- “Salesforce-Verbindungsoptionen” auf Seite 341
- “SAP-Verbindungsoptionen” auf Seite 343
- “Sequentielle Verbindungs-Optionen” auf Seite 344
- “Verbindungsoptionen des parallelen Teradata-Transporters” auf Seite 346
- “Twitter-Verbindungsoptionen” auf Seite 348
- “Twitter Streaming-Verbindungsoptionen” auf Seite 350
- “VSAM-Verbindungsoptionen” auf Seite 351
- “Verbindungsoptionen von Web Content-Kapow Katalyst” auf Seite 353

DataSift-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer DataSift-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die DataSift-Verbindungsoptionen für infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Option	Beschreibung
userName	DataSift-Benutzernamen für das DataSift-Benutzerkonto.
apiKey	API-Schlüssel. Der Developer-API-Schlüssel wird auf dem Dashboard oder auf der Einstellungsseite im DataSift-Benutzerkonto angezeigt.

Verwandte Themen:

- “Adabas-Verbindungsoptionen” auf Seite 291
- “DB2 für i5/OS-Verbindungsoptionen” auf Seite 294
- “Facebook-Verbindungsoptionen” auf Seite 297
- “Greenplum-Verbindungsoptionen” auf Seite 299
- “HBase-Verbindungsoptionen” auf Seite 300
- “HDFS-Verbindungsoptionen” auf Seite 302
- “Hadoop Connection Options” auf Seite 304
- “Hive-Verbindungsoptionen” auf Seite 311
- “ DB2 für z/OS-Verbindungsoptionen” auf Seite 316
- “IBM DB2-Verbindungsoptionen” auf Seite 318
- “IMS-Verbindungsoptionen” auf Seite 322
- “JDBC Connection Options” auf Seite 324
- “LinkedIn-Verbindungsoptionen” auf Seite 327
- “Microsoft SQL Server-Verbindungsoptionen” auf Seite 328
- “Netezza-Verbindungsoptionen” auf Seite 332
- “OData-Verbindungsoptionen” auf Seite 334
- “ ODBC-Verbindungsoptionen” auf Seite 335
- “Oracle-Verbindungsoptionen” auf Seite 338
- “Salesforce-Verbindungsoptionen” auf Seite 341
- “SAP-Verbindungsoptionen” auf Seite 343
- “Sequentielle Verbindungs-Optionen” auf Seite 344
- “Verbindungsoptionen des parallelen Teradata-Transporters” auf Seite 346
- “Twitter-Verbindungsoptionen” auf Seite 348
- “Twitter Streaming-Verbindungsoptionen” auf Seite 350
- “VSAM-Verbindungsoptionen” auf Seite 351
- “Verbindungsoptionen von Web Content-Kapow Katalyst” auf Seite 353

DB2 für i5/OS-Verbindungsoptionen

Verwenden Sie DB2I-Verbindungsoptionen, um die DB2 für i5/OS-Verbindung zu definieren.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die DB2 für i5/OS-Verbindungsoptionen für infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Option	Beschreibung
DatabaseName	Datenbankinstanzname.
EnvironmentSQL	Optional. SQL-Befehle zum Einrichten der Datenbankumgebung beim Herstellen einer Verbindung zur Datenbank. Der Datenintegrationsdienst führt die SQL-Befehle zur Verbindungsumgebung jedes Mal aus, wenn er eine Verbindung zur Datenbank herstellt. **Hinweis:** Setzen Sie Sonderzeichen in doppelte Anführungszeichen.
CodePage	Erforderlich. Codepage, die zum Lesen aus einer Quell-Datenbank oder zum Schreiben auf eine Target-Datenbank oder -Datei verwendet wird.
ArraySize	Optional. Bestimmt die Anzahl der Datensätze im Speicher-Array für die Threads, wenn der Worker-Threads-Wert größer als 0 ist. Gültige Werte sind 1 bis 100000. Der Standardwert ist 25.
Compression	Optional. Komprimiert die Daten, um die Menge an Daten zu reduzieren, die über das Netzwerk geschrieben werden. Standardwert ist „false“.
EncyptionLevel	Optional. Verschlüsselungsebene für RC2 oder DES für Verschlüsselungstypen. Geben Sie einen der folgenden Werte für die Verschlüsselungsebene ein: - 1. Verwenden Sie einen 56-Bit-Kodierungsschlüssel für DES und RC2. - 2. Verwenden Sie einen 168-Bit-Triple-DES-Kodierungsschlüssel für DES oder einen 64-Bit-Kodierungsschlüssel für RC2. - 3. Verwenden Sie einen 168-Bit-Triple-DES-Kodierungsschlüssel für DES oder einen 128-Bit-Kodierungsschlüssel für RC2. Der Standardwert ist 1. **Hinweis:** Wenn Sie für den Verschlüsselungstyp „Keine“ auswählen, ignoriert der Datenintegrationsdienst den Wert für die Verschlüsselungsebene.
EncryptionType	Optional. Typ der Verschlüsselung. Geben Sie einen der folgenden Werte für den Verschlüsselungstyp ein: - Keine - RC2 - DES Der Standardwert ist „Keine“.
InterpretAsRows	Optional. Repräsentiert die Pacing-Größe als Anzahl von Zeilen. Bei FALSE gibt die Pacing-Größe Kilobyte wieder. Standardwert ist „false“.
Speicherort	Speicherort des PowerExchange Listener-Knotens, der eine Verbindung zur Datenbank herstellen kann. Der Speicherort wird im ersten Parameter der NODE-Anweisung in der dbmover.cfg-Konfigurationsdatei von PowerExchange definiert.
PacingSize	Optional. Menge der Daten, die das Quellsystem an den PowerExchange Listener weitergeben kann. Konfigurieren Sie die Pacing-Größe, wenn eine externe Anwendung, eine Datenbank oder der Datenintegrationsdienst einen Engpass darstellt. Je geringer der Wert ist, desto schneller ist die Leistung. Der Mindestwert ist 0. Geben Sie 0 für maximale Leistung ein. Standardwert ist 0.
RejectFile	Optional. Geben Sie den Namen und den Pfad der Ablehnungsdateien ein. Ablehnungsdateien enthalten Zeilen, die nicht in die Datenbank geschrieben wurden.

Option	Beschreibung
WriteMode	Geben Sie einen der folgenden Schreibmodi ein: - CONFIRMWRITEON. Sendet Daten zum PowerExchange Listener und wartet auf eine Erfolgs-/Nichterfolgsreaktion, bevor weitere Daten gesendet werden. - CONFIRMWRITEOFF. Sendet Daten zum PowerExchange Listener, ohne eine Erfolgs-/Nichterfolgsreaktion abzuwarten. Verwenden Sie diese Option, wenn die Target-Tabelle bei Auftreten eines Fehlers erneut geladen werden kann. - ASYNCHRONOUSWITHFAULTT. Sendet Daten asynchron zum PowerExchange Listener mit der Möglichkeit der Fehlererkennung. Der Standardwert ist CONFIRMWRITEON.
DatabaseFileOverrides	Gibt die i5/OS-Datenbankdateiüberschreibung an. Das Format lautet: `from_file/to_library/to_file/to_member` Dabei gilt: - *from_file* die zu überschreibende Datei ist - *to_library* die zu verwendende neue Bibliothek ist - *to_file* die zu verwendende Datei in der neuen Bibliothek ist - *to_member* ist optional und stellt das zu verwendende Glied in der neuen Bibliothek und Datei dar. *FIRST wird verwendet, wenn keine Angabe gemacht wird. Sie können bis zu 8 eindeutige Dateiüberschreibungen für eine einzelne Verbindung angeben. Eine einzelne Überschreibung gilt für eine einzelne Quelle oder ein einzelnes Target. Wenn Sie mehr als eine Dateiüberschreibung angeben, setzen Sie den String der Dateiüberschreibungen in doppelte Anführungszeichen und fügen Sie ein Leerzeichen zwischen jeder Dateiüberschreibung ein. **Hinweis:** Wenn sowohl LibraryList als auch DatabaseFileOverrides angegeben werden und eine Tabelle in beiden vorhanden ist, hat DatabaseFileOverrides Vorrang.
IsolationLevel	Commit-Umfang der Transaktion. Wählen Sie einen der folgenden Werte aus: - Keine - CS. Cursorstabilität. - RR. Repeatable Read. - CHG. Ändern. - ALLE Der Standardwert ist CS.
LibraryList	Liste der Bibliotheken, die PowerExchange durchsucht, um den Tabellennamen für Select-, Insert-, Delete- oder Update-Anweisungen zu qualifizieren. PowerExchange durchsucht die Liste, wenn der Tabellenname nicht qualifiziert ist. Trennen Sie Bibliotheken mit Semikolon. **Hinweis:** Wenn sowohl LibraryList als auch DatabaseFileOverrides angegeben werden und eine Tabelle in beiden vorhanden ist, hat DatabaseFileOverrides Vorrang.
EnableConnectionPool	Optional. Ermöglicht paralleles Verarbeiten beim Laden von Daten in einer Tabelle im Bulk-Modus. Wird für Oracle verwendet. TRUE oder FALSE. Standardwert ist „true“.
ConnectionPoolSize	Optional. Maximale Anzahl an inaktiven Verbindungsinstanzen, die der Datenintegrationsdienst für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert auf eine höhere Anzahl als die Mindestanzahl an inaktiven Verbindungsinstanzen fest.

Option	Beschreibung
ConnectionPoolMaxIdleTime	Optional. Anzahl der Sekunden, die eine die Mindestanzahl an Verbindungsinstanzen überschreitende Verbindung inaktiv bleiben kann, bevor sie vom Verbindungspool abgebrochen wird. Der Verbindungspool ignoriert die Leerlaufzeit, wenn die Mindestanzahl an inaktiven Verbindungsinstanzen nicht überschritten wird.
ConnectionPoolMinConnections	Optional. Die Mindestanzahl an inaktiven Verbindungsinstanzen, die der Pool für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert so fest, dass er der Poolgröße inaktiver Verbindungen gleicht oder kleiner als diese ist. Standardwert ist 0.

Verwandte Themen:

- "Adabas-Verbindungsoptionen" auf Seite 291
- "DataSift-Verbindungsoptionen" auf Seite 293
- "Facebook-Verbindungsoptionen" auf Seite 297
- "Greenplum-Verbindungsoptionen" auf Seite 299
- "HBase-Verbindungsoptionen" auf Seite 300
- "HDFS-Verbindungsoptionen" auf Seite 302
- "Hadoop Connection Options" auf Seite 304
- "Hive-Verbindungsoptionen" auf Seite 311
- " DB2 für z/OS-Verbindungsoptionen" auf Seite 316
- "IBM DB2-Verbindungsoptionen" auf Seite 318
- "IMS-Verbindungsoptionen" auf Seite 322
- "JDBC Connection Options" auf Seite 324
- "LinkedIn-Verbindungsoptionen" auf Seite 327
- "Microsoft SQL Server-Verbindungsoptionen" auf Seite 328
- "Netezza-Verbindungsoptionen" auf Seite 332
- "OData-Verbindungsoptionen" auf Seite 334
- " ODBC-Verbindungsoptionen" auf Seite 335
- "Oracle-Verbindungsoptionen" auf Seite 338
- "Salesforce-Verbindungsoptionen" auf Seite 341
- "SAP-Verbindungsoptionen" auf Seite 343
- "Sequentielle Verbindungs-Optionen" auf Seite 344
- "Verbindungsoptionen des parallelen Teradata-Transporters" auf Seite 346
- "Twitter-Verbindungsoptionen" auf Seite 348
- "Twitter Streaming-Verbindungsoptionen" auf Seite 350
- "VSAM-Verbindungsoptionen" auf Seite 351
- "Verbindungsoptionen von Web Content-Kapow Katalyst" auf Seite 353

Facebook-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Facebook-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Facebook-Verbindungsoptionen für infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Option	Beschreibung
ConsumerKey	Die Anwendungs-ID, die Sie beim Erstellen der Anwendung in Facebook erhalten. Facebook verwendet den Schlüssel zur Identifizierung der Anwendung.
ConsumerSecret	Das Anwendungsgeheimwort, das Sie beim Erstellen der Anwendung in Facebook erhalten. Facebook verwendet das Geheimwort für das Eigentum am Verbraucherschlüssel.
AccessToken	Zugriffstoken, den das OAuth-Dienstprogramm zurückgibt. Facebook verwendet diesen Token anstelle der Benutzeranmeldedaten für den Zugriff auf geschützte Ressourcen.
AccessSecret	Das Zugriffsgeheimwort ist für eine Facebook-Verbindung nicht erforderlich.
Bereich	Berechtigungen für die Anwendung. Geben Sie die Berechtigungen ein, die Sie zum Konfigurieren von OAuth verwendet haben.

Verwandte Themen:

- “Adabas-Verbindungsoptionen” auf Seite 291
- “DataSift-Verbindungsoptionen” auf Seite 293
- “DB2 für i5/OS-Verbindungsoptionen” auf Seite 294
- “Greenplum-Verbindungsoptionen” auf Seite 299
- “HBase-Verbindungsoptionen” auf Seite 300
- “HDFS-Verbindungsoptionen” auf Seite 302
- “Hadoop Connection Options” auf Seite 304
- “Hive-Verbindungsoptionen” auf Seite 311
- “ DB2 für z/OS-Verbindungsoptionen” auf Seite 316
- “IBM DB2-Verbindungsoptionen” auf Seite 318
- “IMS-Verbindungsoptionen” auf Seite 322
- “JDBC Connection Options” auf Seite 324
- “LinkedIn-Verbindungsoptionen” auf Seite 327
- “Microsoft SQL Server-Verbindungsoptionen” auf Seite 328
- “Netezza-Verbindungsoptionen” auf Seite 332
- “OData-Verbindungsoptionen” auf Seite 334
- “ ODBC-Verbindungsoptionen” auf Seite 335
- “Oracle-Verbindungsoptionen” auf Seite 338
- “Salesforce-Verbindungsoptionen” auf Seite 341

- "SAP-Verbindungsoptionen" auf Seite 343
- "Sequentielle Verbindungs-Optionen" auf Seite 344
- "Verbindungsoptionen des parallelen Teradata-Transporters" auf Seite 346
- "Twitter-Verbindungsoptionen" auf Seite 348
- "Twitter Streaming-Verbindungsoptionen" auf Seite 350
- "VSAM-Verbindungsoptionen" auf Seite 351
- "Verbindungsoptionen von Web Content-Kapow Katalyst" auf Seite 353

Greenplum-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Greenplum-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:
... -o option_name=value option_name=value ...

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Greenplum-Verbindungsoptionen für die infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Option	Beschreibung
UserName	Erforderlich. Benutzername mit Berechtigungen für den Zugriff auf die Greenplum-Datenbank.
Passwort	Erforderlich. Passwort für die Verbindung zur Greenplum-Datenbank.
driverName	Erforderlich. Name des Greenplum-JDBC-Treibers. Beispiel:`com.pivotal.jdbc.GreenplumDriver` Weitere Informationen über den Treiber finden Sie in der Greenplum-Dokumentation.
connectionString	Erforderlich. Greenplum-JDBC-Verbindungs-URL. Beispiel: `jdbc:pivotal:greenplum:// <hostname>:<port>;DatabaseName=<database_name>` Weitere Informationen über die Verbindungs-URL finden Sie in der Greenplum-Dokumentation.
hostName	Erforderlich. Hostname oder IP-Adresse des Greenplum-Servers.
portNumber	Optional. Portnummer des Greenplum-Servers. Wenn Sie 0 eingeben, liest das Dienstprogramm „gpload" aus der Umgebungsvariable $PGPORT. Standardwert ist 5432.
databaseName	Erforderlich. Name der Datenbank, zu der Sie eine Verbindung herstellen möchten.
enableSSL	Erforderlich. Legen Sie diese Option auf TRUE fest, um sichere Kommunikation zwischen dem Dienstprogramm „gpload" und dem Greenplum-Server über SSL einzurichten.
SSLCertificatePath	Erforderlich, wenn Sie SSL aktivieren. Pfad, in dem die SSL-Zertifikate für den Greenplum-Server gespeichert werden.

Verwandte Themen:

- "Adabas-Verbindungsoptionen" auf Seite 291

- “DataSift-Verbindungsoptionen” auf Seite 293
- “DB2 für i5/OS-Verbindungsoptionen” auf Seite 294
- “Facebook-Verbindungsoptionen” auf Seite 297
- “HBase-Verbindungsoptionen” auf Seite 300
- “HDFS-Verbindungsoptionen” auf Seite 302
- “Hadoop Connection Options” auf Seite 304
- “Hive-Verbindungsoptionen” auf Seite 311
- “ DB2 für z/OS-Verbindungsoptionen” auf Seite 316
- “IBM DB2-Verbindungsoptionen” auf Seite 318
- “IMS-Verbindungsoptionen” auf Seite 322
- “JDBC Connection Options” auf Seite 324
- “LinkedIn-Verbindungsoptionen” auf Seite 327
- “Microsoft SQL Server-Verbindungsoptionen” auf Seite 328
- “Netezza-Verbindungsoptionen” auf Seite 332
- “OData-Verbindungsoptionen” auf Seite 334
- “ ODBC-Verbindungsoptionen” auf Seite 335
- “Oracle-Verbindungsoptionen” auf Seite 338
- “Salesforce-Verbindungsoptionen” auf Seite 341
- “SAP-Verbindungsoptionen” auf Seite 343
- “Sequentielle Verbindungs-Optionen” auf Seite 344
- “Verbindungsoptionen des parallelen Teradata-Transporters” auf Seite 346
- “Twitter-Verbindungsoptionen” auf Seite 348
- “Twitter Streaming-Verbindungsoptionen” auf Seite 350
- “VSAM-Verbindungsoptionen” auf Seite 351
- “Verbindungsoptionen von Web Content-Kapow Katalyst” auf Seite 353

HBase-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Hbase-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die HBase-Verbindungsoptionen für die Befehle „infacmd isp CreateConnection“ und „UpdateConnection“ beschrieben:

Eigenschaft	Beschreibung
Name	Der Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung ändern. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: `~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /`
ID	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 4.000 Zeichen enthalten.
Speicherort	Die Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Der Verbindungstyp. Wählen Sie HBase.
ZooKeeper-Host(s)	Name des Computers, auf dem der ZooKeeper-Server gehostet wird. Bei diesem Namen wird zwischen Groß- und Kleinschreibung unterschieden. Wenn der ZooKeeper im replizierten Modus ausgeführt wird, geben Sie eine kommagetrennte Liste der Server in den ZooKeeper-Quorumservern an. Wenn die TCP-Verbindung zum Server unterbrochen wird, stellt der Client eine Verbindung zu einem anderen Server im Quorum her.
ZooKeeper-Port	Portnummer des Computers, auf dem der ZooKeeper-Server gehostet wird.
Kerberos-Verbindung aktivieren	Ermöglicht der Informatica-Domäne die Kommunikation mit dem HBase-Master- oder -Regionsserver, der Kerberos-Authentifizierung verwendet.
HBase-Master-Prinzipal	Dienst-Prinzipalname (SPN) des HBase-Masterservers. Ermöglicht dem ZooKeeper-Server die Kommunikation mit einem HBase-Masterserver, der Kerberos-Authentifizierung verwendet. Geben Sie eine Zeichenfolge in folgendem Format ein: `hbase/<domain.name>@<YOUR-REALM>` Wobei: - Domain.name der Domänenname des Computers ist, auf dem der HBase-Masterserver gehostet wird. - YOUR-REALM der Kerberos-Bereich ist.
HBase-Regionsserver-Prinzipal	Dienst-Prinzipalname (SPN) des HBase-Regionsservers. Ermöglicht dem ZooKeeper-Server die Kommunikation mit einem HBase-Regionsserver, der Kerberos-Authentifizierung verwendet. Geben Sie eine Zeichenfolge in folgendem Format ein: `hbase_rs/<domain.name>@<YOUR-REALM>` Wobei: - Domain.name der Domänenname des Computers ist, auf dem der HBase-Masterserver gehostet wird. - YOUR-REALM der Kerberos-Bereich ist.

Verwandte Themen:

- “Adabas-Verbindungsoptionen” auf Seite 291
- “DataSift-Verbindungsoptionen” auf Seite 293
- “DB2 für i5/OS-Verbindungsoptionen” auf Seite 294
- “Facebook-Verbindungsoptionen” auf Seite 297
- “Greenplum-Verbindungsoptionen” auf Seite 299
- “HDFS-Verbindungsoptionen” auf Seite 302
- “Hadoop Connection Options” auf Seite 304
- “Hive-Verbindungsoptionen” auf Seite 311
- “ DB2 für z/OS-Verbindungsoptionen” auf Seite 316
- “IBM DB2-Verbindungsoptionen” auf Seite 318
- “IMS-Verbindungsoptionen” auf Seite 322
- “JDBC Connection Options” auf Seite 324
- “LinkedIn-Verbindungsoptionen” auf Seite 327
- “Microsoft SQL Server-Verbindungsoptionen” auf Seite 328
- “Netezza-Verbindungsoptionen” auf Seite 332
- “OData-Verbindungsoptionen” auf Seite 334
- “ ODBC-Verbindungsoptionen” auf Seite 335
- “Oracle-Verbindungsoptionen” auf Seite 338
- “Salesforce-Verbindungsoptionen” auf Seite 341
- “SAP-Verbindungsoptionen” auf Seite 343
- “Sequentielle Verbindungs-Optionen” auf Seite 344
- “Verbindungsoptionen des parallelen Teradata-Transporters” auf Seite 346
- “Twitter-Verbindungsoptionen” auf Seite 348
- “Twitter Streaming-Verbindungsoptionen” auf Seite 350
- “VSAM-Verbindungsoptionen” auf Seite 351
- “Verbindungsoptionen von Web Content-Kapow Katalyst” auf Seite 353

HDFS-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer HDFS-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die HDFS-Verbindungsoptionen für infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Option	Beschreibung
userName	Benutzername für den Zugriff auf HDFS.
nameNodeURI	Die URI für den Zugriff auf HDFS. Die URI muss im folgenden Format sein: `hdfs://<namenode>:<port>` wobei - `<namenode>` der Hostname oder IP-Adresse von NameNode ist - `<port>` der Port ist, den NameNode auf Remoteprozeduraufrufe (RPC) abhört.

Verwandte Themen:

- "Adabas-Verbindungsoptionen" auf Seite 291
- "DataSift-Verbindungsoptionen" auf Seite 293
- "DB2 für i5/OS-Verbindungsoptionen" auf Seite 294
- "Facebook-Verbindungsoptionen" auf Seite 297
- "Greenplum-Verbindungsoptionen" auf Seite 299
- "HBase-Verbindungsoptionen" auf Seite 300
- "Hadoop Connection Options" auf Seite 304
- "Hive-Verbindungsoptionen" auf Seite 311
- " DB2 für z/OS-Verbindungsoptionen" auf Seite 316
- "IBM DB2-Verbindungsoptionen" auf Seite 318
- "IMS-Verbindungsoptionen" auf Seite 322
- "JDBC Connection Options" auf Seite 324
- "LinkedIn-Verbindungsoptionen" auf Seite 327
- "Microsoft SQL Server-Verbindungsoptionen" auf Seite 328
- "Netezza-Verbindungsoptionen" auf Seite 332
- "OData-Verbindungsoptionen" auf Seite 334
- " ODBC-Verbindungsoptionen" auf Seite 335
- "Oracle-Verbindungsoptionen" auf Seite 338
- "Salesforce-Verbindungsoptionen" auf Seite 341
- "SAP-Verbindungsoptionen" auf Seite 343
- "Sequentielle Verbindungs-Optionen" auf Seite 344
- "Verbindungsoptionen des parallelen Teradata-Transporters" auf Seite 346
- "Twitter-Verbindungsoptionen" auf Seite 348
- "Twitter Streaming-Verbindungsoptionen" auf Seite 350
- "VSAM-Verbindungsoptionen" auf Seite 351
- "Verbindungsoptionen von Web Content-Kapow Katalyst" auf Seite 353

Hadoop Connection Options

Use connection options to define a Hive connection.

Enter connection options in the following format:

```
... -o option_name='value' option_name='value' ...
```

To enter multiple options, separate them with a space.

The following table describes Hadoop connection options for infacmd isp CreateConnection and UpdateConnection commands that you configure when you want to use the Hadoop connection:

Option	Description
connectionId	String that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or less and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.
connectionType	Required. Type of connection is Hadoop.
name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: `~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /`

RMAddress	The service within Hadoop that submits requests for resources or spawns YARN applications.
	Use the following format:
	`<hostname>:<port>`
	Where
	- <hostname> is the host name or IP address of the Yarn resource manager.
	- <port> is the port on which the Yarn resource manager listens for remote procedure calls (RPC).
	For example, enter: `myhostame:8032`
	You can also get the Resource Manager Address property from yarn-site.xml located in the following directory on the Hadoop cluster: `/etc/hadoop/conf/`
	The Resource Manager Address appears as the following property in yarn-site.xml:
	`<property>`
	`<name>yarn.resourcemanager.address</name>`
	`<value>hostname:port</value>`
	`<description>The address of the applications manager interface in the Resource Manager.</description>`
	`</property>`
	Optionally, if the `yarn.resourcemanager.address` property is not configured in yarn-site.xml, you can find the host name from the `yarn.resourcemanager.hostname` or `yarn.resourcemanager.scheduler.address` properties in yarn-site.xml. You can then configure the Resource Manager Address in the Hadoop connection with the following value: `hostname:8032`

cadiAppYarnQueueName	The YARN scheduler queue name used by the Blaze engine that specifies available resources on a cluster. The name is case sensitive.

Option	Description
cadiExecutionParameterList	Custom properties that are unique to the Blaze engine. You can specify multiple properties. Use the following format: `<property1>=<value>` Where - <property1> is a Blaze engine optimization property. - <value> is the value of the Blaze engine optimization property. To specify multiple properties use `&:` as the property separator. Use custom properties only at the request of Informatica Global Customer Support.
cadiMaxPort	The maximum value for the port number range for the Blaze engine.
cadiMinPort	The minimum value for the port number range for the Blaze engine.
cadiUserName	The operating system profile user name for the Blaze engine.
cadiWorkingDirectory	The HDFS file path of the directory that the Blaze engine uses to store temporary files. Verify that the directory exists. The YARN user, Blaze engine user, and mapping impersonation user must have write permission on this directory.
databaseName	Namespace for tables. Use the name `default` for tables that do not have a specified database name.

defaultFSURI	The URI to access the default Hadoop Distributed File System.
	Use the following connection URI:
	`hdfs://<node name>:<port>`
	Where
	- <node name> is the host name or IP address of the NameNode.
	- <port> is the port on which the NameNode listens for remote procedure calls (RPC).
	For example, enter: `hdfs://myhostname:8020/`
	You can also get the Default File System URI property from core-site.xml located in the following directory on the Hadoop cluster: `/etc/hadoop/conf/`
	Use the value from the `fs.defaultFS` property found in core-site.xml.
	For example, use the following value:
	`<property>`
	`<name>fs.defaultFS</name>`
	`<value>hdfs://localhost:8020</value>`
	`</property>`
	If the Hadoop cluster runs MapR, use the following URI to access the MapR File system: `maprfs:///`.

Option	Description

engineType	The engine that the Hadoop environment uses to run a mapping on the Hadoop cluster. Select a value from the drop down list.
	For example select: `MRv2`
	To set the engine type in the Hadoop connection, you must get the value for the `mapreduce.framework.name` property from mapred-site.xml located in the following directory on the Hadoop cluster: `/etc/hadoop/conf/`
	If the value for `mapreduce.framework.name` is `classic`, select `mrv1` as the engine type in the Hadoop connection.
	If the value for `mapreduce.framework.name` is `yarn`, you can select the `mrv2` or `tez` as the engine type in the Hadoop connection. Do not select Tez if Tez is not configured for the Hadoop cluster.
	You can also set the value for the engine type in hive-site.xml. The engine type appears as the following property in hive-site.xml:
	`<property>`
	`<name>hive.execution.engine</name>`
	`<value>tez</value>`
	`<description>Chooses execution engine. Options are: mr (MapReduce, default) or tez (Hadoop 2 only)</description>`
	`</property>`

environmentSQL	SQL commands to set the Hadoop environment. The Data Integration Service executes the environment SQL at the beginning of each Hive script generated in a Hive execution plan. The following rules and guidelines apply to the usage of environment SQL: - Use the environment SQL to specify Hive queries. - Use the environment SQL to set the classpath for Hive user-defined functions and then use environment SQL or PreSQL to specify the Hive user-defined functions. You cannot use PreSQL in the data object properties to specify the classpath. The path must be the fully qualified path to the JAR files used for user-defined functions. Set the parameter hive.aux.jars.path with all the entries in infapdo.aux.jars.path and the path to the JAR files for user-defined functions. - You can use environment SQL to define Hadoop or Hive parameters that you want to use in the PreSQL commands or in custom queries.
hadoopExecEnvExecutionParameterList	Custom properties that are unique to the Hadoop environment. You can specify multiple properties. Use the following format: `<property1>=<value>` Where - <property1> is a Hadoop environment optimization property. - <value> is the value of the Hadoop environment optimization property. To specify multiple properties use `&:` as the property separator. Use custom properties only at the request of Informatica Global Customer Support.
Hiveserver2Enabled	Optional. Runs the mapping in the HiveServer2 mode. If you enable HiveServer2 execution mode, use the JDBCConnectString option to provide the JDBC URL to access HiveServer2. The default mode of execution is HiveCLI.

Option	Description
Hiveusername	User name of the user that the Data Integration Service impersonates to run mappings on a Hadoop cluster. If the Hadoop cluster uses Kerberos authentication, the principal name for the JDBC connection string and the user name must be the same. **Hinweis:** You must use user impersonation for the Hadoop connection if the Hadoop cluster uses Kerberos authentication. If the Hadoop cluster does not use Kerberos authentication, the user name depends on the behavior of the JDBC driver. If you do not specify a user name, the Hadoop cluster authenticates jobs based on the operating system profile user name of the machine that runs the Data Integration Service.

hiveWarehouseDirectoryOnHDFS	The absolute HDFS file path of the default database for the warehouse that is local to the cluster. For example, the following file path specifies a local warehouse: `/user/hive/warehouse`
	For Cloudera CDH, if the Metastore Execution Mode is remote, then the file path must match the file path specified by the Hive Metastore Service on the Hadoop cluster.
	You can get the value for the Hive Warehouse Directory on HDFS from the `hive.metastore.warehouse.dir` property in hive-site.xml located in the following directory on the Hadoop cluster: `/etc/hadoop/conf/`
	For example, use the following value:
	`<property>`
	`<name>hive.metastore.warehouse.dir</name>`
	`<value>/usr/hive/warehouse </value>`
	`<description>location of the warehouse directory</ description>`
	`</property>`
	For MapR, `hive-site.xml` is located in the following direcetory: `/opt/mapr/hive/<hive version>/conf`.

JDBCConnectString	The JDBC connection URI used to access the data and metadata from the Hadoop server. You can use PowerExchange for Hive to communicate with a HiveServer service or HiveServer2 service. To connect to HiveServer, specify the connection string in the following format: `jdbc:hive2://<hostname>:<port>/<db>` Where - <hostname> is name or IP address of the machine on which HiveServer2 runs. - <port> is the port number on which HiveServer2 listens. - <db> is the database name to which you want to connect. If you do not provide the database name, the Data Integration Service uses the default database details. To connect to HiveServer 2, use the connection string format that Apache Hive implements for that specific Hadoop Distribution. For more information about Apache Hive connection string formats, see the Apache Hive documentation.

Option	Description

jobMonitoringURL	The URL for the MapReduce JobHistory server. You can use the URL for the JobTracker URI if you use MapReduce version 1.
	Use the following format:
	`<hostname>:<port>`
	Where
	- <hostname> is the host name or IP address of the JobHistory server.
	- <port> is the port on which the JobHistory server listens for remote procedure calls (RPC).
	For example, enter: `myhostname:8021`
	You can get the value for the Job Monitoring URL from mapred-site.xml. The Job Monitoring URL appears as the following property in mapred-site.xml:
	`<property>`
	`<name>mapred.job.tracker</name>`
	`<value>myhostname:8021 </value>`
	`<description>The host and port that the MapReduce job tracker runs at.</description>`
	`</property>`

metastoreDatabaseDriver	Driver class name for the JDBC data store. For example, the following class name specifies a MySQL driver:
	`com.mysql.jdbc.Driver`
	You can get the value for the Metastore Database Driver from hive-site.xml. The Metastore Database Driver appears as the following property in hive-site.xml:
	`<property>`
	`  <name>javax.jdo.option.ConnectionDriverName</name>`
	`  <value>com.mysql.jdbc.Driver</value>`
	`</property>`

metastoreDatabasePassword	The password for the metastore user name.
	You can get the value for the Metastore Database Password from hive-site.xml. The Metastore Database Password appears as the following property in hive-site.xml:
	`<property>`
	`  <name>javax.jdo.option.ConnectionPassword</name>`
	`  <value>password</value>`
	`</property>`

Option	Description

metastoreDatabaseURI	The JDBC connection URI used to access the data store in a local metastore setup. Use the following connection URI:
	`jdbc:<datastore type>://<node name>:<port>/<database name>`
	where
	- <node name> is the host name or IP address of the data store.
	- <data store type> is the type of the data store.
	- <port> is the port on which the data store listens for remote procedure calls (RPC).
	- <database name> is the name of the database.
	For example, the following URI specifies a local metastore that uses MySQL as a data store:
	`jdbc:mysql://hostname23:3306/metastore`
	You can get the value for the Metastore Database URI from hive-site.xml. The Metastore Database URI appears as the following property in hive-site.xml:
	`<property>`
	`  <name>javax.jdo.option.ConnectionURL</name>`
	`  <value>jdbc:mysql://MYHOST/metastore</value>`
	`</property>`

metastoreDatabaseUserName	The metastore database user name.
	You can get the value for the Metastore Database User Name from hive-site.xml. The Metastore Database User Name appears as the following property in hive-site.xml:
	`<property>`
	`  <name>javax.jdo.option.ConnectionUserName</name>`
	`  <value>hiveuser</value>`
	`</property>`

metastoreMode	Controls whether to connect to a remote metastore or a local metastore. By default, local is selected. For a local metastore, you must specify the Metastore Database URI, Metastore Database Driver, Username, and Password. For a remote metastore, you must specify only the Remote Metastore URI.
	You can get the value for the Metastore Execution Mode from hive-site.xml. The Metastore Execution Mode appears as the following property in hive-site.xml:
	`<property>`
	`<name>hive.metastore.local</name>`
	`<value>true</true>`
	`</property>`
	Hinweis: The `hive.metastore.local` property is deprecated in hive-site.xml for Hive server versions 0.9 and above. If the `hive.metastore.local` property does not exist but the `hive.metastore.uris` property exists, and you know that the Hive server has started, you can set the connection to a remote metastore.

Option	Description

remoteMetastoreURI	The metastore URI used to access metadata in a remote metastore setup. For a remote metastore, you must specify the Thrift server details.
	Use the following connection URI:
	`thrift://<hostname>:<port>`
	Where
	- <hostname> is name or IP address of the Thrift metastore server.
	- <port> is the port on which the Thrift server is listening.
	For example, enter: `thrift://myhostname:9083/`
	You can get the value for the Remote Metastore URI from hive-site.xml. The Remote Metastore URI appears as the following property in hive-site.xml:
	`<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>`

SparkHDFSStagingDir	The HDFS file path of the directory that the Spark engine uses to store temporary files for running jobs. The YARN user, Spark engine user, and mapping impersonation user must have write permission on this directory.
SparkExecutionParameterList	An optional list of configuration parameters to apply to the Spark engine. You can change the default Spark configuration properties values, such as `spark.executor.memory` or `spark.driver.cores`. Use the following format: `<property1>=<value>` - <property1> is a Spark configuration property. - <value> is the value of the property. For example, you can configure a YARN scheduler queue name that specifies available resources on a cluster: `spark.yarn.queue=TestQ` To enter multiple properties, separate each name-value pair with the following text: `&:`
stgDataCompressionCodecClass	Codec class name that enables data compression and improves performance on temporary staging tables.
stgDataCompressionCodecType	Hadoop compression library for a compression codec class name.

Verwandte Themen:

- "Adabas-Verbindungsoptionen" auf Seite 291
- "DataSift-Verbindungsoptionen" auf Seite 293
- "DB2 für i5/OS-Verbindungsoptionen" auf Seite 294
- "Facebook-Verbindungsoptionen" auf Seite 297
- "Greenplum-Verbindungsoptionen" auf Seite 299
- "HBase-Verbindungsoptionen" auf Seite 300
- "HDFS-Verbindungsoptionen" auf Seite 302
- "Hive-Verbindungsoptionen" auf Seite 311
- " DB2 für z/OS-Verbindungsoptionen" auf Seite 316
- "IBM DB2-Verbindungsoptionen" auf Seite 318

- “IMS-Verbindungsoptionen” auf Seite 322
- “JDBC Connection Options” auf Seite 324
- “LinkedIn-Verbindungsoptionen” auf Seite 327
- “Microsoft SQL Server-Verbindungsoptionen” auf Seite 328
- “Netezza-Verbindungsoptionen” auf Seite 332
- “OData-Verbindungsoptionen” auf Seite 334
- “ ODBC-Verbindungsoptionen” auf Seite 335
- “Oracle-Verbindungsoptionen” auf Seite 338
- “Salesforce-Verbindungsoptionen” auf Seite 341
- “SAP-Verbindungsoptionen” auf Seite 343
- “Sequentielle Verbindungs-Optionen” auf Seite 344
- “Verbindungsoptionen des parallelen Teradata-Transporters” auf Seite 346
- “Twitter-Verbindungsoptionen” auf Seite 348
- “Twitter Streaming-Verbindungsoptionen” auf Seite 350
- “VSAM-Verbindungsoptionen” auf Seite 351
- “Verbindungsoptionen von Web Content-Kapow Katalyst” auf Seite 353

Hive-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Hive-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name='value' option_name='value' ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen.

Die folgende Tabelle beschreibt Hive-Verbindungsoptionen für infacmd isp CreateConnection- und UpdateConnection-Befehle, die Sie konfigurieren, wenn Sie die Hive-Verbindung verwenden möchten:

Option	Beschreibung
connectionType	Erforderlich. Verbindungstyp ist HIVE.
name	Der Datenquellname (Name) der Verbindung. Beim Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden, und er muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung ändern. Der Name darf nicht länger als 128 Zeichen sein und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: `~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /`
relationalSourceAndTarget	Hive-Verbindungsmodus. Stellen Sie diese Option auf "TRUE", wenn Sie die Verbindung für den Zugriff auf Hive-Data Warehouse nutzen möchten. Wenn Sie auf das Hive-Ziel zugreifen möchten, müssen Sie die gleiche oder eine andere Hive-Verbindung aktivieren, um das Mapping auf dem Hadoop-Cluster auszuführen. Wenn Sie relationale Quelle und Ziel aktivieren, müssen Sie Option metadataDatabaseString angeben.

Option	Beschreibung
pushdownMode	Hive-Verbindungsmodus. Stellen Sie diese Option auf "TRUE", wenn Sie die Verbindung verwenden möchten, um Mappings im Hadoop-Cluster auszuführen Wenn Sie die Verbindung für den Pushdwon-Modus aktivieren, müssen Sie die Optionen zum Ausführen der Informatica-Mappings im Hadoop-Cluster angeben.
environmentSQL	SQL-Befehle zum Einrichten der Hadoop-Umgebung. Im nativen Umgebungstyp führt der Data Integration Service die Umgebungs-SQL jedes Mal aus, wenn er eine Verbindung zum Hive-Metastore herstellt. Wenn die Hive-Verbindung zum Ausführen von Mappings im Hadoop-Cluster verwendet wird, führt der Data Integration Service die Umgebungs-SQL zu Beginn jeder Hive-Sitzung aus. Die folgenden Regeln und Richtlinien gelten für die Verwendung von Umgebungs-SQL in beiden Verbindungsmodi: - Verwenden Sie die Umgebungs-SQL, um Hive-Abfragen anzugeben. - Verwenden Sie die Umgebungs-SQL, um den Klassenpfad für benutzerdefinierte Hive-Funktionen einzustellen und verwenden Sie dann entweder Umgebungs-SQL oder PreSQL, um die benutzerdefinierten Hive-Funktionen anzugeben. Sie können PreSQL nicht in den Datenobjekteigenschaften zur Angabe des Klassenpfads verwenden. Der Pfad muss der voll qualifizierte Pfad zu den JAR-Dateien für die benutzerdefinierten Funktionen sein. Stellen Sie die Parameter hive.aux.jars.path mit allen Einträgen in infapdo.aux.jars.path und den Pfad zu den JAR-Dateien für benutzerdefinierte Funktionen ein. - Sie können auch Umgebungs-SQL zum Definieren von Hadoop- oder Hive-Parametern verwenden, die Sie in den PreSQL-Befehlen oder in benutzerspezifischen Abfragen nutzen möchten. Wenn die Hive-Verbindung zum Ausführen von Mappings im Hadoop-Cluster verwendet wird, so wird nur die Umgebungs-SQL der Hive-Verbindung ausgeführt. Die verschiedenen Umgebungs-SQL-Befehle für die Verbindungen von Hive-Quelle und -Ziel werden nicht ausgeführt, selbst wenn Hive-Quellen und -Ziele sich in verschiedenen Clustern befinden.
enableQuotes	Schließt alle für die Datenbank reservierten Wörter in Anführungszeichen ein. Die Standardeinstellung ist "FALSE".

Eigenschaften für den Zugriff auf Hive als Quelle oder Ziel

Die folgende Tabelle beschreibt die erforderlichen Optionen für infacmd isp CreateConnection- und UpdateConnection-Befehle, die Sie konfigurieren, wenn Sie die Hive-Verbindung für den Zugriff auf Daten verwenden möchten:

Eigenschaft	Beschreibung
metadataConnString	Die JDBC-Verbindungs-URI für den Zugriff auf die Metadaten vom Hadoop-Server. Die Verbindungszeichenfolge verwendet das folgende Format: `jdbc:hive://<hostname>:<port>/<db>` wobei - `hostname` der Name oder die IP-Adresse des Rechners ist, auf dem der Hive-Server ausgeführt wird - `port` der Port ist, auf dem der Hive-Server abhört - `db` die Datenbank ist, zu der Sie eine Verbindung herstellen möchten. Wenn Sie die Datenbankdetails nicht zur Verfügung stellen, verwendet der Data Integration Service die standardmäßigen Datenbank-Details.
bypassHiveJDBCServer	JDBC-Treibermodus. Aktivieren Sie diese Option zur Verwendung des eingebetteten JDBC-Treibers (eingebetteter Modus). Zur Verwendung des eingebetteten JDBC-Modus führen Sie folgende Aufgaben durch: - Stellen Sie sicher, dass Hive-Client und Informatica Services auf demselben Rechner installiert sind. - Konfigurieren Sie die Hive-Verbindungseigenschaften zum Ausführen von Mappings im Hadoop-Cluster. Wenn Sie den nicht eingebetteten Modus wählen, müssen Sie die Verbindungszeichenfolge für Datenzugriff konfigurieren. Der eingebettete JDBC-Modus wird dem nicht eingebetteten Modus vorgezogen.
connectString	Die Verbindungszeichenfolge, die zum Zugriff auf Daten aus dem Hadoop-Datenspeicher verwendet wird. Die Verbindungszeichenfolge des nicht eingebetteten JDBC-Modus muss das folgende Format haben: `jdbc:hive://<hostname>:<port>/<db>` wobei - `hostname` der Name oder die IP-Adresse des Rechners ist, auf dem der Hive-Server ausgeführt wird. - `port` der Port ist, auf dem der Hive-Server abhört. Der Standardwert ist 10000. - `db` die Datenbank ist, zu der Sie eine Verbindung herstellen möchten. Wenn Sie die Datenbankdetails nicht zur Verfügung stellen, verwendet der Data Integration Service die standardmäßigen Datenbank-Details.

Eigenschaften zum Ausführen von Mappings im Hadoop-Cluster

Die folgende Tabelle beschreibt die erforderlichen Optionen für infacmd isp CreateConnection- und UpdateConnection-Befehle, die Sie konfigurieren, wenn Sie die Hive-Verbindung zum Ausführen von Informatica-Mappings im Hadoop-Cluster verwenden möchten:

Eigenschaft	Beschreibung
databaseName	Namespace für Tabellen. Verwenden Sie den Namen `default` für Tabellen, bei denen kein angegebener Datenbankname vorhanden ist.
defaultFSURI	Die URI für den Zugriff auf das verteilte Standard-Hadoop-Dateisystem. FS URI muss das folgende Format haben: `hdfs://<node name>:<port>` wobei - `node name` der Hostname oder die IP-Adresse des NameNode ist - `port` der Port ist, den NameNode auf Remoteprozeduraufrufe (RPC) abhört.
jobTrackerURI	Der Dienst innerhalb von Hadoop, der die MapReduce-Aufgaben an bestimmte Knoten im Cluster sendet. JobTracker URI muss das folgende Format haben: `<jobtrackername>:<port>` wobei - `jobtrackername` der Hostname oder die IP-Adresse des JobTracker ist. - `port` der Port ist, von dem aus der JobTracker auf Remoteprozeduraufrufe (RPC) abhört.
hiveWarehouseDirectoryOnHDFS	Der absolute HDFS-Dateipfad der Standarddatenbank für die Warehouse, die lokal für den Cluster ist. Der folgende Dateipfad gibt zum Beispiel eine lokale Warehouse an: `/user/hive/warehouse`
metastoreExecutionMode	Steuert, ob eine Verbindung zu einem Remote-Metastore oder einem lokalen Metastore hergestellt wird. Für einen lokalen Metastore müssen Sie die Metastore-Datenbank-URI, Treiber, Benutzername und Passwort angeben. Für einen ausgelagerten Metastore müssen Sie nur die Remote Metastore URI angeben.

metastoreDatabaseURI	Die JDBC-Verbindungs-URI zum Zugriff auf den Datenspeicher in einer lokalen Metastore-Einrichtung. Die URI muss das folgende Format haben:
	`jdbc:<datastore type>://<node name>:<port>/<database name>`
	wobei
	- `node name` der Hostname oder die IP-Adresse des Datenspeichers ist
	- `data store type` der Typ des Datenspeichers ist
	- `port` der Port ist, von dem aus der Datenspeicher auf Remoteprozeduraufrufe (RPC) abhört
	- `database name` der Name der Datenbank ist
	Die folgende URI gibt zum Beispiel einen lokalen Metastore an, der MySQL als Datenspeicher verwendet:
	`jdbc:mysql://hostname23:3306/metastore`

metastoreDatabaseDriver	Treiberklassenname für den JDBC-Datenspeicher. Der folgende Klassenname gibt zum Beispiel einen MySQL-Treiber an: `com.mysql.jdbc.Driver`
metastoreDatabaseUserName	Der Benutzername der Metastore-Datenbank.

Eigenschaft	Beschreibung
metastoreDatabasePassword	Das Passwort für den Benutzernamen der Datenbank.
remoteMetastoreURI	Die Metastore-URI, die für den Zugriff auf Metadaten in einer Remote-Metastore-Einrichtung verwendet wird. Für einen Remote-Metastore müssen Sie die Thrift-Serverdetails angeben. Die URI muss das folgende Format haben: `thrift://<hostname>:<port>` wobei - `hostname` der Name oder die IP-Adresse des Thrift-Metastore-Servers ist - `port` der Port ist, auf dem der Thrift-Server abhört.

Verwandte Themen:

- "Adabas-Verbindungsoptionen" auf Seite 291
- "DataSift-Verbindungsoptionen" auf Seite 293
- "DB2 für i5/OS-Verbindungsoptionen" auf Seite 294
- "Facebook-Verbindungsoptionen" auf Seite 297
- "Greenplum-Verbindungsoptionen" auf Seite 299
- "HBase-Verbindungsoptionen" auf Seite 300
- "HDFS-Verbindungsoptionen" auf Seite 302
- "Hadoop Connection Options" auf Seite 304
- " DB2 für z/OS-Verbindungsoptionen" auf Seite 316
- "IBM DB2-Verbindungsoptionen" auf Seite 318
- "IMS-Verbindungsoptionen" auf Seite 322
- "JDBC Connection Options" auf Seite 324
- "LinkedIn-Verbindungsoptionen" auf Seite 327
- "Microsoft SQL Server-Verbindungsoptionen" auf Seite 328
- "Netezza-Verbindungsoptionen" auf Seite 332
- "OData-Verbindungsoptionen" auf Seite 334
- " ODBC-Verbindungsoptionen" auf Seite 335
- "Oracle-Verbindungsoptionen" auf Seite 338
- "Salesforce-Verbindungsoptionen" auf Seite 341
- "SAP-Verbindungsoptionen" auf Seite 343
- "Sequentielle Verbindungs-Optionen" auf Seite 344
- "Verbindungsoptionen des parallelen Teradata-Transporters" auf Seite 346
- "Twitter-Verbindungsoptionen" auf Seite 348
- "Twitter Streaming-Verbindungsoptionen" auf Seite 350
- "VSAM-Verbindungsoptionen" auf Seite 351
- "Verbindungsoptionen von Web Content-Kapow Katalyst" auf Seite 353

DB2 für z/OS-Verbindungsoptionen

Verwenden Sie DB2Z-Verbindungsoptionen, um die IBM für DB2 z/OS-Verbindung zu definieren.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die DB2Z-Verbindungsoptionen für infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Option	Beschreibung
DataAccessConnectString	Verbindungsstring für den Zugriff auf Daten in der Datenbank. <database name>
EnvironmentSQL	Optional. SQL-Befehle zum Einrichten der Datenbankumgebung beim Herstellen einer Verbindung zur Datenbank. Der Datenintegrationsdienst führt die SQL-Befehle zur Verbindungsumgebung jedes Mal aus, wenn er eine Verbindung zur Datenbank herstellt. **Hinweis:** Setzen Sie Sonderzeichen in doppelte Anführungszeichen.
CodePage	Erforderlich. Codepage, die zum Lesen aus einer Quell-Datenbank oder zum Schreiben auf eine Target-Datenbank oder -Datei verwendet wird.
ArraySize	Optional. Bestimmt die Anzahl der Datensätze im Speicher-Array für die Threads, wenn der Worker-Threads-Wert größer als 0 ist. Gültige Werte sind 1 bis 100000. Der Standardwert ist 25.
Compression	Optional. Komprimiert die Daten, um die Menge an Daten zu reduzieren, die über das Netzwerk geschrieben werden. Standardwert ist „false“.
CorrelationID	Optional. Beschriftung, die auf DB2-Aufgaben oder -Abfragen angewendet wird, um DB2 für z/OS für die Ressource auszuweisen. Geben Sie bis zu 8 Byte an alphanumerische Zeichen ein.
EncyptionLevel	Optional. Verschlüsselungsebene für RC2 oder DES für Verschlüsselungstypen. Geben Sie einen der folgenden Werte für die Verschlüsselungsebene ein: - 1. Verwenden Sie einen 56-Bit-Kodierungsschlüssel für DES und RC2. - 2. Verwenden Sie einen 168-Bit-Triple-DES-Kodierungsschlüssel für DES oder einen 64-Bit-Kodierungsschlüssel für RC2. - 3. Verwenden Sie einen 168-Bit-Triple-DES-Kodierungsschlüssel für DES oder einen 128-Bit-Kodierungsschlüssel für RC2. Der Standardwert ist 1. **Hinweis:** Wenn Sie für den Verschlüsselungstyp „Keine“ auswählen, ignoriert der Datenintegrationsdienst den Wert für die Verschlüsselungsebene.
EncryptionType	Optional. Typ der Verschlüsselung. Geben Sie einen der folgenden Werte für den Verschlüsselungstyp ein: - Keine - RC2 - DES Der Standardwert ist „Keine“.
InterpretAsRows	Optional. Repräsentiert die Pacing-Größe als Anzahl von Zeilen. Bei FALSE gibt die Pacing-Größe Kilobyte wieder. Standardwert ist „false“.

Option	Beschreibung
Speicherort	Speicherort des PowerExchange Listener-Knotens, der eine Verbindung zur Datenbank herstellen kann. Der Knoten wird in der dbmover.cfg-Konfigurationsdatei von PowerExchange definiert.
OffloadProcessing	Optional. Verschiebt die Stapeldatenverarbeitung von der VSAM-Quelle zum Datenintegrationsdienst-Computer. Geben Sie einen der folgenden Werte ein: - Auto. Der Datenintegrationsdienst bestimmt, ob Offload-Verarbeitung verwendet werden soll. - Ja. Offload-Verarbeitung wird verwendet. - Nein. Offload-Verarbeitung wird nicht verwendet. Der Standardwert ist Auto.
PacingSize	Optional. Menge der Daten, die das Quellsystem an den PowerExchange Listener weitergeben kann. Konfigurieren Sie die Pacing-Größe, wenn eine externe Anwendung, eine Datenbank oder der Datenintegrationsdienst einen Engpass darstellt. Je geringer der Wert ist, desto schneller ist die Leistung. Der Mindestwert ist 0. Geben Sie 0 für maximale Leistung ein. Standardwert ist 0.
RejectFile	Optional. Geben Sie den Namen und den Pfad der Ablehnungsdateien ein. Ablehnungsdateien enthalten Zeilen, die nicht in die Datenbank geschrieben wurden.
WorkerThread	Optional. Anzahl der vom Datenintegrationsdienst verwendeten Threads, um Stapeldaten bei aktivierter Offload-Verarbeitung zu verarbeiten. Um eine optimale Leistung zu erzielen, sollte dieser Wert die Anzahl der verfügbaren Prozessoren auf dem Rechner des Datenintegrationsdienstes nicht überschreiten. Gültige Werte sind 1 bis 64. Der Standardwert ist 0, der Multithreading verhindert.
WriteMode	Geben Sie einen der folgenden Schreibmodi ein: - CONFIRMWRITEON. Sendet Daten zum PowerExchange Listener und wartet auf eine Erfolgs-/Nichterfolgsreaktion, bevor weitere Daten gesendet werden. - CONFIRMWRITEOFF. Sendet Daten zum PowerExchange Listener, ohne eine Erfolgs-/Nichterfolgsreaktion abzuwarten. Verwenden Sie diese Option, wenn die Target-Tabelle bei Auftreten eines Fehlers erneut geladen werden kann. - ASYNCHRONOUSWITHFAULTT. Sendet Daten asynchron zum PowerExchange Listener mit der Möglichkeit der Fehlererkennung. Der Standardwert ist CONFIRMWRITEON.
EnableConnectionPool	Optional. Ermöglicht paralleles Verarbeiten beim Laden von Daten in einer Tabelle im Bulk-Modus. Wird für Oracle verwendet. TRUE oder FALSE. Standardwert ist „true“.
ConnectionPoolSize	Optional. Maximale Anzahl an inaktiven Verbindungsinstanzen, die der Datenintegrationsdienst für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert auf eine höhere Anzahl als die Mindestanzahl an inaktiven Verbindungsinstanzen fest.
ConnectionPoolMaxIdleTime	Optional. Anzahl der Sekunden, die eine die Mindestanzahl an Verbindungsinstanzen überschreitende Verbindung inaktiv bleiben kann, bevor sie vom Verbindungspool abgebrochen wird. Der Verbindungspool ignoriert die Leerlaufzeit, wenn die Mindestanzahl an inaktiven Verbindungsinstanzen nicht überschritten wird.
ConnectionPoolMinConnections	Optional. Die Mindestanzahl an inaktiven Verbindungsinstanzen, die der Pool für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert so fest, dass er der Poolgröße inaktiver Verbindungen gleicht oder kleiner als diese ist. Standardwert ist 0.

Verwandte Themen:

- "Adabas-Verbindungsoptionen" auf Seite 291
- "DataSift-Verbindungsoptionen" auf Seite 293
- "DB2 für i5/OS-Verbindungsoptionen" auf Seite 294
- "Facebook-Verbindungsoptionen" auf Seite 297
- "Greenplum-Verbindungsoptionen" auf Seite 299
- "HBase-Verbindungsoptionen" auf Seite 300
- "HDFS-Verbindungsoptionen" auf Seite 302
- "Hadoop Connection Options" auf Seite 304
- "Hive-Verbindungsoptionen" auf Seite 311
- "IBM DB2-Verbindungsoptionen" auf Seite 318
- "IMS-Verbindungsoptionen" auf Seite 322
- "JDBC Connection Options" auf Seite 324
- "LinkedIn-Verbindungsoptionen" auf Seite 327
- "Microsoft SQL Server-Verbindungsoptionen" auf Seite 328
- "Netezza-Verbindungsoptionen" auf Seite 332
- "OData-Verbindungsoptionen" auf Seite 334
- " ODBC-Verbindungsoptionen" auf Seite 335
- "Oracle-Verbindungsoptionen" auf Seite 338
- "Salesforce-Verbindungsoptionen" auf Seite 341
- "SAP-Verbindungsoptionen" auf Seite 343
- "Sequentielle Verbindungs-Optionen" auf Seite 344
- "Verbindungsoptionen des parallelen Teradata-Transporters" auf Seite 346
- "Twitter-Verbindungsoptionen" auf Seite 348
- "Twitter Streaming-Verbindungsoptionen" auf Seite 350
- "VSAM-Verbindungsoptionen" auf Seite 351
- "Verbindungsoptionen von Web Content-Kapow Katalyst" auf Seite 353

IBM DB2-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer IBM DB2-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die IBM DB2-Verbindungsoptionen für infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Option	Beschreibung
PassThruEnabled	Optional. Aktiviert Pass-Through-Sicherheit für die Verbindung. Wenn Sie Pass-Through-Sicherheit für eine Verbindung aktivieren, verwendet die Domäne nicht die im Verbindungsobjekt definierten Anmeldeinformationen, sondern den Benutzernamen und das Passwort des Clients, um sich an der entsprechenden Datenbank anzumelden.

MetadataAccessConnectString	Erforderlich. JDBC-Verbindungs-URL für den Zugriff auf Metadaten in der Datenbank.
	`jdbc:informatica:db2:// <Hostname>:<Port>;DatabaseName=<Datenbankname>`
	Beim Importieren einer Tabelle aus dem Developer Tool oder dem Analyst Tool werden standardmäßig alle Tabellen unterhalb des standardmäßigen Schemanamens angezeigt. Um Tabellen unterhalb eines bestimmten Schemas anstelle des Standardschemas anzuzeigen, können Sie den Namen des Schemas angeben, aus dem Sie die Tabelle importieren möchten. Schließen Sie den Parameter „ischemaname“ in die URL ein, um den Schemanamen anzugeben. Beispiel: Mit der folgenden Syntax wird eine Tabelle aus einem bestimmten Schema importiert:
	`jdbc:informatica:db2:// <Hostname>:<Port>;DatabaseName=<Datenbankname>;ischemaname=<Schema_Name>`
	Um eine Tabelle in mehreren Schemas zu suchen und zu importieren, können Sie die Namen mehrerer Schemas im Parameter „ischemaname“ festlegen. Beim Namen eines Schemas wird die Groß-/Kleinschreibung beachtet. Trennen Sie Schemanamen durch senkrechte Striche (|) voneinander. Beispiel: Mit der folgenden Syntax können Sie eine Tabelle in drei Schemas suchen und importieren:
	`jdbc:informatica:db2:// <Hostname>:<Port>;DatabaseName=<Datenbankname>;ischemaname=<schema_name1>|<schema_name2>|<schema_name3>`

Option	Beschreibung
AdvancedJDBCSecurityOptions	Optional. Datenbankparameter für Metadata-Zugriff auf eine sichere Datenbank. Informatica behandelt den Wert des Felds „AdvancedJDBCSecurityOptions“ als vertrauliche Daten und verschlüsselt die Parameter-Zeichenfolge. Um eine Verbindung zu einer sicheren Datenbank herzustellen, beziehen Sie die folgenden Parameter mit ein: - EncryptionMethod. Erforderlich. Gibt an, ob Daten bei der Netzwerkübertragung verschlüsselt werden. Dieser Parameter muss auf SSL festgelegt werden. - ValidateServerCertificate. Optional. Gibt an, ob Informatica das Zertifikat validiert, das vom Datenbankserver gesendet wird. Wenn dieser Parameter auf "True" gesetzt wird, validiert Informatica das vom Datenbankserver gesendete Zertifikat. Wenn Sie den HostNameInCertificate-Parameter angeben, validiert Informatica ebenfalls den Hostnamen im Zertifikat. Wenn dieser Parameter auf "false" festgelegt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat nicht. Informatica ignoriert alle Truststore-Informationen, die Sie angeben. - HostNameInCertificate. Optional. Hostname des Computers, auf dem die sichere Datenbank gehostet wird. Wenn Sie einen Hostnamen angeben, validiert Informatica den Hostnamen in der Verbindungszeichenfolge mit dem Hostnamen im SSL-Zertifikat. - TrustStore. Erforderlich. Pfad und Dateiname der Truststore-Datei, die das SSL-Zertifikat für die Datenbank enthält. - TrustStorePassword Erforderlich. Passwort der Truststore-Datei für die sichere Datenbank. **Hinweis:** Eine vollständige Liste der sicheren JDBC-Parameter finden Sie in der DataDirect JDBC-Dokumentation. Informatica hängt die sichere JDBC-Parameter an die Verbindungszeichenfolge an. Wenn Sie die sicheren JDBC-Parameter direkt in den Verbindungsstring mit einbeziehen, geben Sie keine Parameter in das Feld „AdvancedJDBCSecurityOptions“ ein.
DataAccessConnectString	Verbindungszeichenfolge für den Zugriff auf Daten in der Datenbank Geben Sie die Verbindungszeichenfolge im folgenden Format ein: `<Datenbankname>`
CodePage	Erforderlich. Codepage, die zum Lesen aus einer Quell-Datenbank oder zum Schreiben in eine Target-Datenbank verwendet wird.
EnvironmentSQL	Optional. SQL-Befehle zum Einrichten der Datenbankumgebung beim Herstellen einer Verbindung zur Datenbank. Der Datenintegrationsdienst führt die SQL-Befehle zur Verbindungsumgebung jedes Mal aus, wenn er eine Verbindung zur Datenbank herstellt. Beispiel: `ALTER SESSION SET CURRENT_SCHEMA=INFA_USR;` **Hinweis:** Setzen Sie Sonderzeichen in doppelte Anführungszeichen.
TransactionSQL	Optional. SQL-Befehle zum Ausführen vor jeder Transaktion. Der Datenintegrationsdienst führt die Transaktions-SQL am Anfang jeder Transaktion aus. Beispiel: `SET TRANSACTION ISOLATION LEVEL SERIALIZABLE;` **Hinweis:** Setzen Sie Sonderzeichen in doppelte Anführungszeichen.
Tablespace	Optional. Der Tablespace-Name der Datenbank.

Option	Beschreibung
QuoteChar	Optional. Das Zeichen, das als Anführungszeichen in dieser Verbindung verwendet wird. Der Zeichentyp, der zur Kennzeichnung von Sonderzeichen und reservierten SQL-Schlüsselwörtern, wie WHERE, verwendet wird. Der Datenintegrationsdienst schließt mit dem ausgewählten Zeichen Sonderzeichen und reservierte SQL-Schlüsselwörter ein. Der Datenintegrationsdienst verwendet dieses Zeichen auch für die Eigenschaft „QuoteChar“. Standardwert ist 0.
EnableQuotes	Optional. Kann zum Aktivieren von Anführungszeichen für diese Verbindung gewählt werden. Sofern aktiviert, schließt der Datenintegrationsdienst Tabellen-, Ansichts-, Schema-, Synonym- und Spaltennamen in Bezeichnerzeichen ein, wenn SQL für diese Objekte in der Verbindung erzeugt und ausgeführt wird. Zu verwenden, wenn Objekte Namen mit gemischter Groß-/Kleinschreibung oder kleingeschriebene Namen haben. Gültige Werte sind „True“ oder „False“. Standardwert ist „True“.
EnableConnectionPool	Optional. Aktiviert das Verbindungspooling. Wenn Sie Verbindungspooling aktivieren, behält der Verbindungspool inaktive Verbindungsinstanzen im Speicher. Wenn Sie Verbindungspooling deaktivieren, stoppt der Datenintegrationsdienst alle Poolingaktivitäten. Gültige Werte sind „True“ oder „False“. Standardwert ist „True“.
ConnectionPoolSize	Optional. Maximale Anzahl an inaktiven Verbindungsinstanzen, die der Datenintegrationsdienst für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert auf eine höhere Anzahl als die Mindestanzahl an inaktiven Verbindungsinstanzen fest. Standardwert ist 15.
ConnectionPoolMaxIdleTime	Optional. Anzahl der Sekunden, die eine die Mindestanzahl an Verbindungsinstanzen überschreitende Verbindung inaktiv bleiben kann, bevor sie vom Verbindungspool abgebrochen wird. Der Verbindungspool ignoriert die Leerlaufzeit, wenn die Mindestanzahl an inaktiven Verbindungsinstanzen nicht überschritten wird. Standardwert ist 120.
ConnectionPoolMinConnections	Optional. Die Mindestanzahl an inaktiven Verbindungsinstanzen, die der Pool für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert so fest, dass er der Poolgröße inaktiver Verbindungen gleicht oder kleiner als diese ist. Standardwert ist 0.

Verwandte Themen:

- “Adabas-Verbindungsoptionen” auf Seite 291
- “DataSift-Verbindungsoptionen” auf Seite 293
- “DB2 für i5/OS-Verbindungsoptionen” auf Seite 294
- “Facebook-Verbindungsoptionen” auf Seite 297
- “Greenplum-Verbindungsoptionen” auf Seite 299
- “HBase-Verbindungsoptionen” auf Seite 300
- “HDFS-Verbindungsoptionen” auf Seite 302
- “Hadoop Connection Options” auf Seite 304
- “Hive-Verbindungsoptionen” auf Seite 311
- “ DB2 für z/OS-Verbindungsoptionen” auf Seite 316
- “IMS-Verbindungsoptionen” auf Seite 322
- “JDBC Connection Options” auf Seite 324
- “LinkedIn-Verbindungsoptionen” auf Seite 327
- “Microsoft SQL Server-Verbindungsoptionen” auf Seite 328

- “Netezza-Verbindungsoptionen” auf Seite 332
- “OData-Verbindungsoptionen” auf Seite 334
- “ ODBC-Verbindungsoptionen” auf Seite 335
- “Oracle-Verbindungsoptionen” auf Seite 338
- “Salesforce-Verbindungsoptionen” auf Seite 341
- “SAP-Verbindungsoptionen” auf Seite 343
- “Sequentielle Verbindungs-Optionen” auf Seite 344
- “Verbindungsoptionen des parallelen Teradata-Transporters” auf Seite 346
- “Twitter-Verbindungsoptionen” auf Seite 348
- “Twitter Streaming-Verbindungsoptionen” auf Seite 350
- “VSAM-Verbindungsoptionen” auf Seite 351
- “Verbindungsoptionen von Web Content-Kapow Katalyst” auf Seite 353

IMS-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer IMS-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die IMS-Verbindungsoptionen beschrieben:

Option	Beschreibung
CodePage	Erforderlich. Code zum Lesen aus oder Schreiben in die Datenbank. Verwenden Sie den ISO-Codepage-Namen, z. B. ISO-8859-6. Der Codepage-Name berücksichtigt keine Groß- und Kleinschreibung.
ArraySize	Optional. Bestimmt die Anzahl der Datensätze im Speicher-Array für die Threads, wenn der Worker-Threads-Wert größer als 0 ist. Gültige Werte sind 1 bis 100000. Default is 25.
Compression	Optional. Komprimiert die Daten, um die Menge an Daten zu reduzieren, die Informatica-Anwendungen über das Netzwerk schreiben. TRUE oder FALSE. Die Standardeinstellung ist "false".
EncryptionLevel	Optional. Verschlüsselungsebene für RC2 oder DES für Verschlüsselungstypen. Geben Sie einen der folgenden Werte für die Verschlüsselungsebene ein: - 1. Verwenden Sie einen 56-Bit-Kodierungsschlüssel für DES und RC2. - 2. Verwenden Sie einen 168-Bit-Triple-DES-Kodierungsschlüssel für DES oder einen 64-Bit-Kodierungsschlüssel für RC2. - 3. Verwenden Sie einen 168-Bit-Triple-DES-Kodierungsschlüssel für DES oder einen 128-Bit-Kodierungsschlüssel für RC2. Default is 1. **Hinweis:** Wenn Sie für den Verschlüsselungstyp None auswählen, ignoriert der Data Integration Service den Wert für die Verschlüsselungsebene.

Option	Beschreibung
EncryptionType	Optional. Geben Sie einen der folgenden Werte für den Verschlüsselungstyp ein: - Keine - RC2 - DES Die Standardeinstellung ist "None".
InterpretAsRows	Optional. Bei TRUE gibt die Pacing-Größe eine Anzahl von Zeilen wieder. Bei FALSE gibt die Pacing-Größe Kilobyte wieder. Die Standardeinstellung ist "false".
Location	Speicherort des PowerExchange Listener-Knotens, der eine Verbindung zur Datenbank herstellen kann. Der Speicherort wird im ersten Parameter der NODE-Anweisung in der dbmover.cfg-Konfigurationsdatei von PowerExchange definiert.
OffLoadProcessing	Optional. Verschiebt die Stapeldatenverarbeitung vom Quellcomputer zum Data Integration Service-Computer. Geben Sie einen der folgenden Werte ein: - Auto. Der Data Integration Service bestimmt, ob Offload-Verarbeitung verwendet werden soll. - Yes. Offload-Verarbeitung wird verwendet. - No. Offload-Verarbeitung wird nicht verwendet. Der Standardwert ist Auto.
PacingSize	Optional. Verlangsamt die Datenübertragungsrate, um Engpässe zu reduzieren. Je geringer der Wert ist, desto höher ist die Sitzungsleistung. Der Mindestwert ist 0. Geben Sie 0 für optimale Leistung ein. Default is 0.
WorkerThread	Optional. Anzahl der vom Data Integration Service verwendeten Threads, um Stapeldaten bei aktivierter Offload-Verarbeitung zu verarbeiten. Um eine optimale Leistung zu erzielen, sollte dieser Wert die Anzahl der verfügbaren Prozessoren auf dem Data Integration Service-Computer nicht überschreiten. Gültige Werte sind 1 bis 64. Der Standardwert ist 0, der Multithreading verhindert.
WriteMode	Geben Sie einen der folgenden Schreibmodi ein: - CONFIRMWRITEON. Sendet Daten zum PowerExchange Listener und wartet auf eine Erfolgs-/Nichterfolgsreaktion, bevor weitere Daten gesendet werden. - CONFIRMWRITEOFF. Sendet Daten zum PowerExchange Listener, ohne eine Erfolgs-/Nichterfolgsreaktion abzuwarten. Verwenden Sie diese Option, wenn die Target-Tabelle bei Auftreten eines Fehlers erneut geladen werden kann. - ASYNCHRONOUSWITHFAULTT. Sendet Daten asynchron zum PowerExchange Listener mit der Möglichkeit der Fehlererkennung. Die Standardoption ist CONFIRMWRITEON.
EnableConnectionPool	Optional. Ermöglicht das Verbindungspooling. Wenn Sie Verbindungspooling aktivieren, behält der Verbindungspool inaktive Verbindungsinstanzen im Speicher. Wenn Sie Verbindungspooling deaktivieren, stoppt der Data Integration Service alle Poolingaktivitäten. TRUE oder FALSE. Die Standardeinstellung ist "false".
ConnectionPoolSize	Optional. Maximale Anzahl an inaktiven Verbindungsinstanzen, die der Data Integration Service für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert auf eine höhere Anzahl als die Mindestanzahl an inaktiven Verbindungsinstanzen fest. Default is 15.

Option	Beschreibung
ConnectionPoolMaxIdleTime	Optional. Anzahl der Sekunden, die eine die Mindestanzahl an Verbindungsinstanzen überschreitende Verbindung inaktiv bleiben kann, bevor sie vom Verbindungspool abgebrochen wird. Der Verbindungspool ignoriert die Leerlaufzeit, wenn die Mindestanzahl an inaktiven Verbindungsinstanzen nicht überschritten wird. Default is 120.
ConnectionPoolMinConnections	Optional. Die Mindestanzahl an inaktiven Verbindungsinstanzen, die der Pool für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert so fest, dass er der Poolgröße inaktiver Verbindungen gleicht oder kleiner als diese ist. Default is 0.

Verwandte Themen:

- "Adabas-Verbindungsoptionen" auf Seite 291
- "DataSift-Verbindungsoptionen" auf Seite 293
- "DB2 für i5/OS-Verbindungsoptionen" auf Seite 294
- "Facebook-Verbindungsoptionen" auf Seite 297
- "Greenplum-Verbindungsoptionen" auf Seite 299
- "HBase-Verbindungsoptionen" auf Seite 300
- "HDFS-Verbindungsoptionen" auf Seite 302
- "Hadoop Connection Options" auf Seite 304
- "Hive-Verbindungsoptionen" auf Seite 311
- " DB2 für z/OS-Verbindungsoptionen" auf Seite 316
- "IBM DB2-Verbindungsoptionen" auf Seite 318
- "JDBC Connection Options" auf Seite 324
- "LinkedIn-Verbindungsoptionen" auf Seite 327
- "Microsoft SQL Server-Verbindungsoptionen" auf Seite 328
- "Netezza-Verbindungsoptionen" auf Seite 332
- "OData-Verbindungsoptionen" auf Seite 334
- " ODBC-Verbindungsoptionen" auf Seite 335
- "Oracle-Verbindungsoptionen" auf Seite 338
- "Salesforce-Verbindungsoptionen" auf Seite 341
- "SAP-Verbindungsoptionen" auf Seite 343
- "Sequentielle Verbindungs-Optionen" auf Seite 344
- "Verbindungsoptionen des parallelen Teradata-Transporters" auf Seite 346
- "Twitter-Verbindungsoptionen" auf Seite 348
- "Twitter Streaming-Verbindungsoptionen" auf Seite 350
- "VSAM-Verbindungsoptionen" auf Seite 351
- "Verbindungsoptionen von Web Content-Kapow Katalyst" auf Seite 353

JDBC Connection Options

Use connection options to define a JDBC connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

To enter multiple options, separate options with spaces. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes JDBC connection options for infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
JDBCDriverClassName	The Java class that you use to connect to the database. The following list provides the driver class name that you can enter for the applicable database type: - DataDirect JDBC driver class name for Oracle: `com.informatica.jdbc.oracle.OracleDriver` - DataDirect JDBC driver class name for IBM DB2: `com.informatica.jdbc.db2.DB2Driver` - DataDirect JDBC driver class name for Microsoft SQL Server: `com.informatica.jdbc.sqlserver.SQLServerDriver` - DataDirect JDBC driver class name for Sybase ASE: `com.informatica.jdbc.sybase.SybaseDriver` - DataDirect JDBC driver class name for Informix: `com.informatica.jdbc.informix.InformixDriver` - DataDirect JDBC driver class name for MySQL: `com.informatica.jdbc.mysql.MySQLDriver` For more information about which driver class to use with specific databases, see the vendor documentation.
MetadataConnString	The URL that you use to connect to the database. The following list provides the connection string that you can enter for the applicable database type: - DataDirect JDBC driver for Oracle: `jdbc:informatica:oracle:// <hostname>:<port>;SID=<sid>` - DataDirect JDBC driver for IBM DB2: `jdbc:informatica:db2:// <hostname>:<port>;DatabaseName=<database name>` - DataDirect JDBC driver for Microsoft SQL Server: `jdbc:informatica:sqlserver:// <host>:<port>;DatabaseName=<database name>` - DataDirect JDBC driver for Sybase ASE: `jdbc:informatica:sybase:// <host>:<port>;DatabaseName=<database name>` - DataDirect JDBC driver for Informix: `jdbc:informatica:informix:// <host>:<port>;informixServer=<informix server name>;databaseName=<dbName>` - DataDirect JDBC driver for MySQL: `jdbc:informatica:mysql:// <host>:<port>;DatabaseName=<database name>` For more information about the connection string to use for specific databases, see the vendor documentation for the URL syntax.
EnvironmentSQL	Optional. SQL commands to set the database environment when you connect to the database. The Data Integration Service executes the connection environment SQL each time it connects to the database. For example, `ALTER SESSION SET CURRENT_SCHEMA=INFA_USR;` **Hinweis:** Enclose special characters in double quotation marks.

Option	Description
TransactionSQL	Optional. SQL commands to execute before each transaction. The Data Integration Service executes the transaction SQL at the beginning of each transaction. For example, `SET TRANSACTION ISOLATION LEVEL SERIALIZABLE;` **Hinweis:** Enclose special characters in double quotes.
QuoteChar	Optional. The character that you will use for quotes in this connection. The type of character used to identify special characters and reserved SQL keywords, such as WHERE. The Data Integration Service places the selected character around special characters and reserved SQL keywords. The Data Integration Service also uses this character for the QuoteChar property. Default is DOUBLE_QUOTE.
EnableQuotes	Optional. Select to enable quotes or not for this connection. When enabled, the Data Integration Service places identifier characters around table, view, schema, synonym, and column names when generating and executing SQL against these objects in the connection. Use if the objects have mixed-case or lowercase names. Valid values are True or False. Default is True.
hadoopConnector	Required if you want to enable Sqoop connectivity for the data object that uses the JDBC connection. The Data Integration Service runs the mapping in the Hadoop run-time environment through Sqoop. You can configure Sqoop connectivity for relational data objects, customized data objects, and logical data objects that are based on a JDBC-compliant database. Set the value to `SQOOP_146` to enable Sqoop connectivity.
hadoopConnectorArgs	Optional. Enter the arguments that the Sqoop program must use to connect to the database. Enclose the Sqoop arguments within single quotes. For example, `hadoopConnectorArgs='--<Sqoop argument 1> --<Sqoop argument 2>'` If you do not enter Sqoop arguments, the Data Integration Service constructs the Sqoop command based on the JDBC connection properties.

Verwandte Themen:

- "Adabas-Verbindungsoptionen" auf Seite 291
- "DataSift-Verbindungsoptionen" auf Seite 293
- "DB2 für i5/OS-Verbindungsoptionen" auf Seite 294
- "Facebook-Verbindungsoptionen" auf Seite 297
- "Greenplum-Verbindungsoptionen" auf Seite 299
- "HBase-Verbindungsoptionen" auf Seite 300
- "HDFS-Verbindungsoptionen" auf Seite 302
- "Hadoop Connection Options" auf Seite 304
- "Hive-Verbindungsoptionen" auf Seite 311
- " DB2 für z/OS-Verbindungsoptionen" auf Seite 316
- "IBM DB2-Verbindungsoptionen" auf Seite 318

- “IMS-Verbindungsoptionen” auf Seite 322
- “LinkedIn-Verbindungsoptionen” auf Seite 327
- “Microsoft SQL Server-Verbindungsoptionen” auf Seite 328
- “Netezza-Verbindungsoptionen” auf Seite 332
- “OData-Verbindungsoptionen” auf Seite 334
- “ ODBC-Verbindungsoptionen” auf Seite 335
- “Oracle-Verbindungsoptionen” auf Seite 338
- “Salesforce-Verbindungsoptionen” auf Seite 341
- “SAP-Verbindungsoptionen” auf Seite 343
- “Sequentielle Verbindungs-Optionen” auf Seite 344
- “Verbindungsoptionen des parallelen Teradata-Transporters” auf Seite 346
- “Twitter-Verbindungsoptionen” auf Seite 348
- “Twitter Streaming-Verbindungsoptionen” auf Seite 350
- “VSAM-Verbindungsoptionen” auf Seite 351
- “Verbindungsoptionen von Web Content-Kapow Katalyst” auf Seite 353

LinkedIn-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer LinkedIn-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die LinkedIn-Verbindungsoptionen für infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Option	Beschreibung
ConsumerKey	Der API-Schlüssel, den Sie beim Erstellen der Anwendung in LinkedIn erhalten. LinkedIn verwendet den Schlüssel zur Identifizierung der Anwendung.
ConsumerSecret	Der Geheimschlüssel, den Sie beim Erstellen der Anwendung in LinkedIn erhalten. LinkedIn verwendet das Geheimwort für das Eigentum am Verbraucherschlüssel.
AccessToken	Zugriffstoken, den das OAuth-Dienstprogramm zurückgibt. Die LinkedIn-Anwendung verwendet diesen Token anstelle der Benutzeranmeldedaten für den Zugriff auf geschützte Ressourcen.
AccessSecret	Zugriffsgeheimwort, das das OAuth-Dienstprogramm zurückgibt. Das Geheimwort legt das Eigentum eines Token fest.

Verwandte Themen:

- “Adabas-Verbindungsoptionen” auf Seite 291
- “DataSift-Verbindungsoptionen” auf Seite 293

- “DB2 für i5/OS-Verbindungsoptionen” auf Seite 294
- “Facebook-Verbindungsoptionen” auf Seite 297
- “Greenplum-Verbindungsoptionen” auf Seite 299
- “HBase-Verbindungsoptionen” auf Seite 300
- “HDFS-Verbindungsoptionen” auf Seite 302
- “Hadoop Connection Options” auf Seite 304
- “Hive-Verbindungsoptionen” auf Seite 311
- “ DB2 für z/OS-Verbindungsoptionen” auf Seite 316
- “IBM DB2-Verbindungsoptionen” auf Seite 318
- “IMS-Verbindungsoptionen” auf Seite 322
- “JDBC Connection Options” auf Seite 324
- “Microsoft SQL Server-Verbindungsoptionen” auf Seite 328
- “Netezza-Verbindungsoptionen” auf Seite 332
- “OData-Verbindungsoptionen” auf Seite 334
- “ ODBC-Verbindungsoptionen” auf Seite 335
- “Oracle-Verbindungsoptionen” auf Seite 338
- “Salesforce-Verbindungsoptionen” auf Seite 341
- “SAP-Verbindungsoptionen” auf Seite 343
- “Sequentielle Verbindungs-Optionen” auf Seite 344
- “Verbindungsoptionen des parallelen Teradata-Transporters” auf Seite 346
- “Twitter-Verbindungsoptionen” auf Seite 348
- “Twitter Streaming-Verbindungsoptionen” auf Seite 350
- “VSAM-Verbindungsoptionen” auf Seite 351
- “Verbindungsoptionen von Web Content-Kapow Katalyst” auf Seite 353

Microsoft SQL Server-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Microsoft SQL Server-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden Verbindungsoptionen von Microsoft SQL Server für die Befehle „infacmd isp CreateConnection“ und „UpdateConnection“ beschrieben:

Option	Beschreibung
UseTrustedConnection	Optional. Der Integrationsdienst verwendet die Windows-Authentifizierung, um auf die Microsoft SQL Server-Datenbank zuzugreifen. Der Benutzername, mit dem der Integrationsdienst gestartet wird, muss ein gültiger Windows-Benutzer mit Zugriff auf die Microsoft SQL Server-Datenbank sein. „True“ oder „False“. Standardwert ist „False“.
PassThruEnabled	Optional. Aktiviert Pass-Through-Sicherheit für die Verbindung. Wenn Sie Pass-Through-Sicherheit für eine Verbindung aktivieren, verwendet die Domäne nicht die im Verbindungsobjekt definierten Anmeldeinformationen, sondern den Benutzernamen und das Passwort des Clients, um sich an der entsprechenden Datenbank anzumelden.

MetadataAccessConnectString	JDBC-Verbindungs-URL für den Zugriff auf Metadaten in der Datenbank.
	Verwenden Sie die folgende Verbindungs-URL:
	`jdbc:informatica:sqlserver:// <Hostname>:<Port>;DatabaseName=<Datenbankname>`
	Beziehen Sie zum Testen der Verbindung mit NTLM-Authentifizierung die folgenden Parameter in die Verbindungszeichenfolge ein:
	- AuthenticationMethod. Die zu verwendende Version der NTLM-Authentifizierung.
	Hinweis: UNIX unterstützt NTLMv1 und NTLMv2, jedoch nicht NTLM.
	- Domäne. Die Domäne, zu der der SQL Server gehört.
	Das folgende Beispiel zeigt die Verbindungszeichenfolge für einen SQL Server, der NTLMv2-Authentifizierung in einer NT-Domäne namens „Informatica.com“ verwendet:
	`jdbc:informatica:sqlserver:// host01:1433;DatabaseName=SQL1;AuthenticationMethod=ntlm2java;Domain=Informatica.com`
	Wenn Sie eine Verbindung über NTLM-Authentifizierung herstellen, können Sie in den MS SQL Server-Verbindungseigenschaften die Option **Verwenden Sie trusted Verbindung** aktivieren. Wenn Sie eine Verbindung über NTLMv1- oder NTLMv2-Authentifizierung herstellen, müssen Sie den Benutzernamen und das Kennwort in den Verbindungseigenschaften angeben.

Option	Beschreibung
AdvancedJDBCSecurityOptions	Optional. Datenbankparameter für Metadata-Zugriff auf eine sichere Datenbank. Informatica behandelt den Wert des Felds „AdvancedJDBCSecurityOptions“ als vertrauliche Daten und verschlüsselt die Parameter-Zeichenfolge. Um eine Verbindung zu einer sicheren Datenbank herzustellen, beziehen Sie die folgenden Parameter mit ein: - EncryptionMethod. Erforderlich. Gibt an, ob Daten bei der Netzwerkübertragung verschlüsselt werden. Dieser Parameter muss auf SSL festgelegt werden. - ValidateServerCertificate. Optional. Gibt an, ob Informatica das Zertifikat validiert, das vom Datenbankserver gesendet wird. Wenn dieser Parameter auf "True" gesetzt wird, validiert Informatica das vom Datenbankserver gesendete Zertifikat. Wenn Sie den HostNameInCertificate-Parameter angeben, validiert Informatica ebenfalls den Hostnamen im Zertifikat. Wenn dieser Parameter auf "false" festgelegt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat nicht. Informatica ignoriert alle Truststore-Informationen, die Sie angeben. - HostNameInCertificate. Optional. Hostname des Computers, auf dem die sichere Datenbank gehostet wird. Wenn Sie einen Hostnamen angeben, validiert Informatica den Hostnamen in der Verbindungszeichenfolge mit dem Hostnamen im SSL-Zertifikat. - TrustStore. Erforderlich. Pfad und Dateiname der Truststore-Datei, die das SSL-Zertifikat für die Datenbank enthält. - TrustStorePassword Erforderlich. Passwort der Truststore-Datei für die sichere Datenbank. **Hinweis:** Eine vollständige Liste der sicheren JDBC-Parameter finden Sie in der DataDirect JDBC-Dokumentation. Informatica hängt die sichere JDBC-Parameter an die Verbindungszeichenfolge an. Wenn Sie die sicheren JDBC-Parameter direkt in der Verbindungszeichenfolge einschließen, geben Sie keinen Parameter in das Feld AdvancedJDBCSecurityOptions ein.
DataAccessConnectString	Erforderlich. Verbindungszeichenfolge für den Zugriff auf Daten in der Datenbank Geben Sie die Verbindungszeichenfolge im folgenden Format ein: `<Servername>@<Datenbankname>`
DomainName	Optional. Der Name der Domäne, in der Microsoft SQL Server ausgeführt wird.
PacketSize	Optional. Erhöhen Sie die Netzwerkpaketgröße, damit größere Datenpakete das Netzwerk gleichzeitig durchlaufen können.
CodePage	Erforderlich. Code zum Lesen aus oder Schreiben in die Datenbank. Verwenden Sie den ISO-Codepage-Namen, z. B. ISO-8859-6. Der Codepage-Name berücksichtigt keine Groß- und Kleinschreibung.
UseDSN	Erforderlich. Legt fest, ob der Datenintegrationsdienst den Namen der Datenquelle für die Verbindung verwenden muss. Wenn Sie den Optionswert auf „true“ festlegen, ruft der Datenintegrationsdienst den Datenbanknamen und den Servernamen aus dem DSN ab. Wenn Sie den Optionswert auf „true“ festlegen, müssen Sie den Datenbanknamen und den Servernamen eingeben.

Option	Beschreibung
ProviderType	Erforderlich. Der Verbindungsprovider, den Sie für eine Verbindung zur Microsoft SQL-Serverdatenbank nutzen möchten. Sie können einen der folgenden Werte definieren: - 0. Legen Sie den Wert auf 0 fest, wenn Sie den ODBC-Providertyp verwenden möchten. Standardwert ist 0. - 1. Legen Sie den Wert auf 1 fest, wenn Sie den OLEDB-Providertyp verwenden möchten. OLEDB ist ein veralteter Providertyp. Informatica unterstützt den OLEDB-Providertyp in zukünftigen Versionen nicht mehr.
OwnerName	Optional. Der Name des Tabelleneigentümers.
SchemaName	Optional. Der Name des Schemas in der Datenbank. Sie müssen den Schemanamen für das Profiling-Warehouse angeben, wenn der Schemaname anders lautet als der Benutzername für die Datenbank. Sie müssen den Schemanamen für die Datenobjekt-Cache-Datenbank angeben, wenn der Schemaname nicht mit dem Datenbank-Benutzernamen übereinstimmt und Sie benutzerverwaltete Cache-Tabellen konfigurieren.
EnvironmentSQL	Optional. SQL-Befehle zum Einrichten der Datenbankumgebung beim Herstellen einer Verbindung zur Datenbank. Der Datenintegrationsdienst führt die SQL-Befehle zur Verbindungsumgebung jedes Mal aus, wenn er eine Verbindung zur Datenbank herstellt. Beispiel: `ALTER SESSION SET CURRENT_SCHEMA=INFA_USR;` **Hinweis:** Setzen Sie Sonderzeichen in doppelte Anführungszeichen.
TransactionSQL	Optional. SQL-Befehle zum Ausführen vor jeder Transaktion. Der Datenintegrationsdienst führt die Transaktions-SQL am Anfang jeder Transaktion aus. Beispiel: `SET TRANSACTION ISOLATION LEVEL SERIALIZABLE;` **Hinweis:** Setzen Sie Sonderzeichen in doppelte Anführungszeichen.
QuoteChar	Optional. Das Zeichen, das als Anführungszeichen in dieser Verbindung verwendet wird. Der Zeichentyp, der zur Kennzeichnung von Sonderzeichen und reservierten SQL-Schlüsselwörtern, wie WHERE, verwendet wird. Der Datenintegrationsdienst schließt mit dem ausgewählten Zeichen Sonderzeichen und reservierte SQL-Schlüsselwörter ein. Der Datenintegrationsdienst verwendet dieses Zeichen auch für die Eigenschaft „QuoteChar“. Standardwert ist 0.
EnableQuotes	Optional. Wählen Sie diesen Wert, um Anführungszeichen für diese Verbindung zu aktivieren. Sofern aktiviert, schließt der Datenintegrationsdienst Tabellen-, Ansichts-, Schema-, Synonym- und Spaltennamen in Bezeichnerzeichen ein, wenn SQL für diese Objekte in der Verbindung erzeugt und ausgeführt wird. Zu verwenden, wenn Objekte Namen mit gemischter Groß-/Kleinschreibung oder kleingeschriebene Namen haben. Gültige Werte sind „True“ oder „False“. Standardwert ist „True“.
EnableConnectionPool	Optional. Aktiviert das Verbindungspooling. Wenn Sie Verbindungspooling aktivieren, behält der Verbindungspool inaktive Verbindungsinstanzen im Speicher. Wenn Sie Verbindungspooling deaktivieren, stoppt der Datenintegrationsdienst alle Poolingaktivitäten. Gültige Werte sind „True“ oder „False“. Standardwert ist „True“.
ConnectionPoolSize	Optional. Maximale Anzahl an inaktiven Verbindungsinstanzen, die der Datenintegrationsdienst für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert auf eine höhere Anzahl als die Mindestanzahl an inaktiven Verbindungsinstanzen fest. Standardwert ist 15.

Option	Beschreibung
ConnectionPoolMaxIdleTime	Optional. Anzahl der Sekunden, die eine die Mindestanzahl an Verbindungsinstanzen überschreitende Verbindung inaktiv bleiben kann, bevor sie vom Verbindungspool abgebrochen wird. Der Verbindungspool ignoriert die Leerlaufzeit, wenn die Mindestanzahl an inaktiven Verbindungsinstanzen nicht überschritten wird. Standardwert ist 120.
ConnectionPoolMinConnections	Optional. Die Mindestanzahl an inaktiven Verbindungsinstanzen, die der Pool für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert so fest, dass er der Poolgröße inaktiver Verbindungen gleicht oder kleiner als diese ist. Standardwert ist 0.

Verwandte Themen:

- "Adabas-Verbindungsoptionen" auf Seite 291
- "DataSift-Verbindungsoptionen" auf Seite 293
- "DB2 für i5/OS-Verbindungsoptionen" auf Seite 294
- "Facebook-Verbindungsoptionen" auf Seite 297
- "Greenplum-Verbindungsoptionen" auf Seite 299
- "HBase-Verbindungsoptionen" auf Seite 300
- "HDFS-Verbindungsoptionen" auf Seite 302
- "Hadoop Connection Options" auf Seite 304
- "Hive-Verbindungsoptionen" auf Seite 311
- " DB2 für z/OS-Verbindungsoptionen" auf Seite 316
- "IBM DB2-Verbindungsoptionen" auf Seite 318
- "IMS-Verbindungsoptionen" auf Seite 322
- "JDBC Connection Options" auf Seite 324
- "LinkedIn-Verbindungsoptionen" auf Seite 327
- "Netezza-Verbindungsoptionen" auf Seite 332
- "OData-Verbindungsoptionen" auf Seite 334
- " ODBC-Verbindungsoptionen" auf Seite 335
- "Oracle-Verbindungsoptionen" auf Seite 338
- "Salesforce-Verbindungsoptionen" auf Seite 341
- "SAP-Verbindungsoptionen" auf Seite 343
- "Sequentielle Verbindungs-Optionen" auf Seite 344
- "Verbindungsoptionen des parallelen Teradata-Transporters" auf Seite 346
- "Twitter-Verbindungsoptionen" auf Seite 348
- "Twitter Streaming-Verbindungsoptionen" auf Seite 350
- "VSAM-Verbindungsoptionen" auf Seite 351
- "Verbindungsoptionen von Web Content-Kapow Katalyst" auf Seite 353

Netezza-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Netezza-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

... -o option_name=value option_name=value ...

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Netezza-Verbindungsoptionen für die infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Option	Beschreibung
connectionString	Erforderlich. Name der ODBC-Datenquelle, die Sie zum Herstellen einer Verbindung zur Netezza-Datenbank erstellen.
jdbcUrl	Erforderlich. JDBC-URL, die vom Developer Tool beim Herstellen einer Verbindung zur Netezza-Datenbank verwendet werden muss. Verwenden Sie das folgende Format: jdbc:netezza://<hostname>:<port>/<database name>
username	Erforderlich. Benutzername mit den entsprechenden Berechtigungen für den Zugriff auf die Netezza-Datenbank.
password	Erforderlich. Passwort für den Datenbankbenutzernamen.
timeout	Erforderlich. Zeit in Sekunden, die das Developer Tool auf eine Antwort von der Netezza-Datenbank wartet, ehe es die Verbindung schließt.

Verwandte Themen:

- "Adabas-Verbindungsoptionen" auf Seite 291
- "DataSift-Verbindungsoptionen" auf Seite 293
- "DB2 für i5/OS-Verbindungsoptionen" auf Seite 294
- "Facebook-Verbindungsoptionen" auf Seite 297
- "Greenplum-Verbindungsoptionen" auf Seite 299
- "HBase-Verbindungsoptionen" auf Seite 300
- "HDFS-Verbindungsoptionen" auf Seite 302
- "Hadoop Connection Options" auf Seite 304
- "Hive-Verbindungsoptionen" auf Seite 311
- " DB2 für z/OS-Verbindungsoptionen" auf Seite 316
- "IBM DB2-Verbindungsoptionen" auf Seite 318
- "IMS-Verbindungsoptionen" auf Seite 322
- "JDBC Connection Options" auf Seite 324
- "LinkedIn-Verbindungsoptionen" auf Seite 327
- "Microsoft SQL Server-Verbindungsoptionen" auf Seite 328
- "OData-Verbindungsoptionen" auf Seite 334
- " ODBC-Verbindungsoptionen" auf Seite 335
- "Oracle-Verbindungsoptionen" auf Seite 338
- "Salesforce-Verbindungsoptionen" auf Seite 341
- "SAP-Verbindungsoptionen" auf Seite 343
- "Sequentielle Verbindungs-Optionen" auf Seite 344

- “Verbindungsoptionen des parallelen Teradata-Transporters” auf Seite 346
- “Twitter-Verbindungsoptionen” auf Seite 348
- “Twitter Streaming-Verbindungsoptionen” auf Seite 350
- “VSAM-Verbindungsoptionen” auf Seite 351
- “Verbindungsoptionen von Web Content-Kapow Katalyst” auf Seite 353

OData-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer OData-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:
... -o option_name=value option_name=value ...

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die OData-Verbindungsoptionen für die infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Eigenschaft	Beschreibung
URL	Erforderlich. Root-URL des OData-Diensts, die die Daten bereitstellt, die Sie lesen möchten.
securityType	Optional. Sicherheitsprotokoll, das das Developer Tool verwenden muss, um eine sichere Verbindung mit dem OData-Server herzustellen. Geben Sie einen der folgenden Werte ein: - Keiner - SSL - TLS
trustStoreFileName	Erforderlich, wenn Sie einen Sicherheitstyp eingeben. Name der Truststore-Datei, die das öffentliche Zertifikat für den OData-Server enthält.
trustStorePassword	Erforderlich, wenn Sie einen Sicherheitstyp eingeben. Passwort für die Truststore-Datei, die das öffentliche Zertifikat für den OData-Server enthält.
keyStoreFileName	Erforderlich, wenn Sie einen Sicherheitstyp eingeben. Name der Schlüsselspeicherdatei, die den privaten Schlüssel für den OData-Server enthält.
keyStorePassword	Erforderlich, wenn Sie einen Sicherheitstyp eingeben. Passwort für die Schlüsselspeicherdatei, die den privaten Schlüssel für den OData-Server enthält.

Verwandte Themen:

- “Adabas-Verbindungsoptionen” auf Seite 291
- “DataSift-Verbindungsoptionen” auf Seite 293
- “DB2 für i5/OS-Verbindungsoptionen” auf Seite 294
- “Facebook-Verbindungsoptionen” auf Seite 297
- “Greenplum-Verbindungsoptionen” auf Seite 299
- “HBase-Verbindungsoptionen” auf Seite 300

- “HDFS-Verbindungsoptionen” auf Seite 302
- “Hadoop Connection Options” auf Seite 304
- “Hive-Verbindungsoptionen” auf Seite 311
- “ DB2 für z/OS-Verbindungsoptionen” auf Seite 316
- “IBM DB2-Verbindungsoptionen” auf Seite 318
- “IMS-Verbindungsoptionen” auf Seite 322
- “JDBC Connection Options” auf Seite 324
- “LinkedIn-Verbindungsoptionen” auf Seite 327
- “Microsoft SQL Server-Verbindungsoptionen” auf Seite 328
- “Netezza-Verbindungsoptionen” auf Seite 332
- “ ODBC-Verbindungsoptionen” auf Seite 335
- “Oracle-Verbindungsoptionen” auf Seite 338
- “Salesforce-Verbindungsoptionen” auf Seite 341
- “SAP-Verbindungsoptionen” auf Seite 343
- “Sequentielle Verbindungs-Optionen” auf Seite 344
- “Verbindungsoptionen des parallelen Teradata-Transporters” auf Seite 346
- “Twitter-Verbindungsoptionen” auf Seite 348
- “Twitter Streaming-Verbindungsoptionen” auf Seite 350
- “VSAM-Verbindungsoptionen” auf Seite 351
- “Verbindungsoptionen von Web Content-Kapow Katalyst” auf Seite 353

ODBC-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer ODBC-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die ODBC-Verbindungsoptionen für infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Option	Beschreibung
PassThruEnabled	Optional. Aktiviert Pass-Through-Sicherheit für die Verbindung. Wenn Sie Pass-Through-Sicherheit für eine Verbindung aktivieren, verwendet die Domäne nicht die im Verbindungsobjekt definierten Anmeldeinformationen, sondern den Benutzernamen und das Passwort des Clients, um sich an der entsprechenden Datenbank anzumelden.
DataAccessConnectString	Verbindungsstring für den Zugriff auf Daten in der Datenbank. Geben Sie den Verbindungsstring im folgenden Format ein: `<Datenbankname>`

Option	Beschreibung
CodePage	Erforderlich. Codepage, die zum Lesen aus einer Quell-Datenbank oder zum Schreiben auf eine Target-Datenbank oder -Datei verwendet wird.
EnvironmentSQL	Optional. SQL-Befehle zum Einrichten der Datenbankumgebung beim Herstellen einer Verbindung zur Datenbank. Der Datenintegrationsdienst führt die SQL-Befehle zur Verbindungsumgebung jedes Mal aus, wenn er eine Verbindung zur Datenbank herstellt. Beispiel: `ALTER SESSION SET CURRENT_SCHEMA=INFA_USR;` **Hinweis:** Setzen Sie Sonderzeichen in doppelte Anführungszeichen.
TransactionSQL	Optional. SQL-Befehle zum Ausführen vor jeder Transaktion. Der Datenintegrationsdienst führt die Transaktions-SQL am Anfang jeder Transaktion aus. Beispiel: `SET TRANSACTION ISOLATION LEVEL SERIALIZABLE;` **Hinweis:** Setzen Sie Sonderzeichen in doppelte Anführungszeichen.
QuoteChar	Optional. Das Zeichen, das als Anführungszeichen in dieser Verbindung verwendet wird. Der Zeichentyp, der verwendet wird, um Sonderzeichen und reservierte SQL-Schlüsselwörter wie WHERE zu kennzeichnen. Der Datenintegrationsdienst schließt mit dem ausgewählten Zeichen Sonderzeichen und reservierte SQL-Schlüsselwörter ein. Der Datenintegrationsdienst verwendet dieses Zeichen auch für die Eigenschaft „QuoteChar“. Der Standardwert ist 4.
ODBC-Provider	Optional. Der Datenbanktyp, zu dem der Datenintegrationsdienst mit ODBC eine Verbindung herstellt. Geben Sie zur Pushdown-Optimierung den Datenbanktyp an, damit der Datenintegrationsdienst die native Datenbank-SQL generieren kann. Es gibt die folgenden Optionen: - Andere - Sybase - Microsoft_SQL_Server - Teradata - Netezza - Greenplum Standardwert ist „Andere“.
EnableQuotes	Optional. Wählen Sie diesen Wert, um Anführungszeichen für diese Verbindung zu aktivieren. Sofern aktiviert, umgibt der Datenintegrationsdienst Tabellen-, Ansichts-, Schema-, Synonym- und Spaltennamen beim Generieren und Ausführen von SQL für diese Objekte in der Verbindung mit ID-Zeichen. Zu verwenden, wenn Objekte Namen mit gemischter Groß-/Kleinschreibung oder kleingeschriebene Namen haben. Gültige Werte sind „true“ oder „false“. Standardwert ist „false“.
EnableConnectionPool	Optional. Ermöglicht das Verbindungspooling. Wenn Sie Verbindungspooling aktivieren, behält der Verbindungspool inaktive Verbindungsinstanzen im Speicher. Wenn Sie Verbindungspooling deaktivieren, stoppt der Datenintegrationsdienst alle Poolingaktivitäten. Gültige Werte sind „true“ oder „false“. Standardwert ist „true“.
ConnectionPoolSize	Optional. Maximale Anzahl an inaktiven Verbindungsinstanzen, die der Datenintegrationsdienst für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert auf eine höhere Anzahl als die Mindestanzahl an inaktiven Verbindungsinstanzen fest. Standardwert ist 15.

Option	Beschreibung
ConnectionPoolMaxIdleTime	Optional. Anzahl der Sekunden, die eine die Mindestanzahl an Verbindungsinstanzen überschreitende Verbindung inaktiv bleiben kann, bevor sie vom Verbindungspool abgebrochen wird. Der Verbindungspool ignoriert die Leerlaufzeit, wenn die Mindestanzahl an inaktiven Verbindungsinstanzen nicht überschritten wird. Standardwert ist 120.
ConnectionPoolMinConnections	Optional. Die Mindestanzahl an inaktiven Verbindungsinstanzen, die der Pool für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert so fest, dass er der Poolgröße inaktiver Verbindungen gleicht oder kleiner als diese ist. Standardwert ist 0.

Verwandte Themen:

- "Adabas-Verbindungsoptionen" auf Seite 291
- "DataSift-Verbindungsoptionen" auf Seite 293
- "DB2 für i5/OS-Verbindungsoptionen" auf Seite 294
- "Facebook-Verbindungsoptionen" auf Seite 297
- "Greenplum-Verbindungsoptionen" auf Seite 299
- "HBase-Verbindungsoptionen" auf Seite 300
- "HDFS-Verbindungsoptionen" auf Seite 302
- "Hadoop Connection Options" auf Seite 304
- "Hive-Verbindungsoptionen" auf Seite 311
- " DB2 für z/OS-Verbindungsoptionen" auf Seite 316
- "IBM DB2-Verbindungsoptionen" auf Seite 318
- "IMS-Verbindungsoptionen" auf Seite 322
- "JDBC Connection Options" auf Seite 324
- "LinkedIn-Verbindungsoptionen" auf Seite 327
- "Microsoft SQL Server-Verbindungsoptionen" auf Seite 328
- "Netezza-Verbindungsoptionen" auf Seite 332
- "OData-Verbindungsoptionen" auf Seite 334
- "Oracle-Verbindungsoptionen" auf Seite 338
- "Salesforce-Verbindungsoptionen" auf Seite 341
- "SAP-Verbindungsoptionen" auf Seite 343
- "Sequentielle Verbindungs-Optionen" auf Seite 344
- "Verbindungsoptionen des parallelen Teradata-Transporters" auf Seite 346
- "Twitter-Verbindungsoptionen" auf Seite 348
- "Twitter Streaming-Verbindungsoptionen" auf Seite 350
- "VSAM-Verbindungsoptionen" auf Seite 351
- "Verbindungsoptionen von Web Content-Kapow Katalyst" auf Seite 353

Oracle-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Oracle-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Oracle-Verbindungsoptionen für infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Option	Beschreibung
PassThruEnabled	Optional. Aktiviert Pass-Through-Sicherheit für die Verbindung. Wenn Sie Pass-Through-Sicherheit für eine Verbindung aktivieren, verwendet die Domäne nicht die im Verbindungsobjekt definierten Anmeldeinformationen, sondern den Benutzernamen und das Passwort des Clients, um sich an der entsprechenden Datenbank anzumelden.
MetadataAccessConnectString	JDBC-Verbindungs-URL für den Zugriff auf Metadaten in der Datenbank jdbc:informatica:oracle://<host_name>:<port>;SID=<database name>

Option	Beschreibung
AdvancedJDBCSecurityOptions	Optional. Datenbankparameter für Metadata-Zugriff auf eine sichere Datenbank. Informatica behandelt den Wert des Felds „AdvancedJDBCSecurityOptions“ als vertrauliche Daten und verschlüsselt die Parameter-Zeichenfolge. Um eine Verbindung zu einer sicheren Datenbank herzustellen, beziehen Sie die folgenden Parameter mit ein: - EncryptionMethod. Erforderlich. Gibt an, ob Daten bei der Netzwerkübertragung verschlüsselt werden. Dieser Parameter muss auf SSL festgelegt werden. - ValidateServerCertificate. Optional. Gibt an, ob Informatica das Zertifikat validiert, das vom Datenbankserver gesendet wird. Wenn dieser Parameter auf „true“ gesetzt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat. Wenn Sie den HostNameInCertificate-Parameter angeben, validiert Informatica ebenfalls den Hostnamen im Zertifikat. Wenn dieser Parameter auf "false" festgelegt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat nicht. Informatica ignoriert alle Truststore-Informationen, die Sie angeben. - HostNameInCertificate. Optional. Hostname des Computers, auf dem die sichere Datenbank gehostet wird. Wenn Sie einen Hostnamen angeben, validiert Informatica den Hostnamen in der Verbindungszeichenfolge mit dem Hostnamen im SSL-Zertifikat. - TrustStore. Erforderlich. Pfad und Dateiname der Truststore-Datei, die das SSL-Zertifikat für die Datenbank enthält. - TrustStorePassword Erforderlich. Passwort der Truststore-Datei für die sichere Datenbank. - KeyStore. Erforderlich. Pfad und Dateiname der Schlüsselspeicherdatei. - KeyStorePassword. Passwort der Schlüsselspeicherdatei für die sichere Datenbank. **Hinweis:** Eine vollständige Liste der sicheren JDBC-Parameter finden Sie in der DataDirect JDBC-Dokumentation. Informatica hängt die sichere JDBC-Parameter an die Verbindungszeichenfolge an. Wenn Sie die sicheren JDBC-Parameter direkt in der Verbindungszeichenfolge einschließen, geben Sie keinen Parameter in das Feld AdvancedJDBCSecurityOptions ein.
DataAccessConnectString	Verbindungszeichenfolge für den Zugriff auf Daten in der Datenbank Geben Sie die Verbindungszeichenfolge im folgenden Format aus dem TNSNAMES-Eintrag ein: `<Datenbankname>`
CodePage	Erforderlich. Codepage, die zum Lesen aus einer Quelldatenbank oder zum Schreiben in eine Zieldatenbank oder -Datei verwendet wird.
EnvironmentSQL	Optional. SQL-Befehle zum Einrichten der Datenbankumgebung beim Herstellen einer Verbindung zur Datenbank. Der Datenintegrationsdienst führt die SQL-Befehle zur Verbindungsumgebung jedes Mal aus, wenn er eine Verbindung zur Datenbank herstellt. Beispiel: `ALTER SESSION SET CURRENT_SCHEMA=INFA_USR;` **Hinweis:** Setzen Sie Sonderzeichen in doppelte Anführungszeichen.

Option	Beschreibung
TransactionSQL	Optional. SQL-Befehle zum Ausführen vor jeder Transaktion. Der Datenintegrationsdienst führt die Transaktions-SQL am Anfang jeder Transaktion aus. Beispiel: `SET TRANSACTION ISOLATION LEVEL SERIALIZABLE;` **Hinweis:** Setzen Sie Sonderzeichen in doppelte Anführungszeichen.
EnableParallelMode	Optional. Ermöglicht Parallelverarbeitung beim Laden von Daten in eine Tabelle im Massenmodus. Wird für Oracle verwendet. „True“ oder „False“. Standardwert ist „False“.
QuoteChar	Optional. Das Zeichen, das als Anführungszeichen in dieser Verbindung verwendet wird. Der Zeichentyp, der zur Kennzeichnung von Sonderzeichen und reservierten SQL-Schlüsselwörtern, wie WHERE, verwendet wird. Der Datenintegrationsdienst schließt mit dem ausgewählten Zeichen Sonderzeichen und reservierte SQL-Schlüsselwörter ein. Der Datenintegrationsdienst verwendet dieses Zeichen auch für die Eigenschaft „QuoteChar“. Standardwert ist 0.
EnableQuotes	Optional. Wählen Sie diesen Wert, um Anführungszeichen für diese Verbindung zu aktivieren. Sofern aktiviert, schließt der Datenintegrationsdienst Tabellen-, Ansichts-, Schema-, Synonym- und Spaltennamen in Bezeichnerzeichen ein, wenn SQL für diese Objekte in der Verbindung erzeugt und ausgeführt wird. Zu verwenden, wenn Objekte Namen mit gemischter Groß-/Kleinschreibung oder kleingeschriebene Namen haben. Gültige Werte sind „True“ oder „False“. Standardwert ist „True“.
EnableConnectionPool	Optional. Aktiviert das Verbindungspooling. Wenn Sie Verbindungspooling aktivieren, behält der Verbindungspool inaktive Verbindungsinstanzen im Speicher. Wenn Sie Verbindungspooling deaktivieren, stoppt der Datenintegrationsdienst alle Poolingaktivitäten. Gültige Werte sind „True“ oder „False“. Standardwert ist „True“.
ConnectionPoolSize	Optional. Maximale Anzahl an inaktiven Verbindungsinstanzen, die der Datenintegrationsdienst für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert auf eine höhere Anzahl als die Mindestanzahl an inaktiven Verbindungsinstanzen fest. Standardwert ist 15.
ConnectionPoolMaxIdleTime	Optional. Anzahl der Sekunden, die eine die Mindestanzahl an Verbindungsinstanzen überschreitende Verbindung inaktiv bleiben kann, bevor sie vom Verbindungspool abgebrochen wird. Der Verbindungspool ignoriert die Leerlaufzeit, wenn die Mindestanzahl an inaktiven Verbindungsinstanzen nicht überschritten wird. Standardwert ist 120.
ConnectionPoolMinConnections	Optional. Die Mindestanzahl an inaktiven Verbindungsinstanzen, die der Pool für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert so fest, dass er der Poolgröße inaktiver Verbindungen gleicht oder kleiner als diese ist. Standardwert ist 0.

Verwandte Themen:

- “Adabas-Verbindungsoptionen” auf Seite 291
- “DataSift-Verbindungsoptionen” auf Seite 293
- “DB2 für i5/OS-Verbindungsoptionen” auf Seite 294
- “Facebook-Verbindungsoptionen” auf Seite 297

- “Greenplum-Verbindungsoptionen” auf Seite 299
- “HBase-Verbindungsoptionen” auf Seite 300
- “HDFS-Verbindungsoptionen” auf Seite 302
- “Hadoop Connection Options” auf Seite 304
- “Hive-Verbindungsoptionen” auf Seite 311
- “ DB2 für z/OS-Verbindungsoptionen” auf Seite 316
- “IBM DB2-Verbindungsoptionen” auf Seite 318
- “IMS-Verbindungsoptionen” auf Seite 322
- “JDBC Connection Options” auf Seite 324
- “LinkedIn-Verbindungsoptionen” auf Seite 327
- “Microsoft SQL Server-Verbindungsoptionen” auf Seite 328
- “Netezza-Verbindungsoptionen” auf Seite 332
- “OData-Verbindungsoptionen” auf Seite 334
- “ ODBC-Verbindungsoptionen” auf Seite 335
- “Salesforce-Verbindungsoptionen” auf Seite 341
- “SAP-Verbindungsoptionen” auf Seite 343
- “Sequentielle Verbindungs-Optionen” auf Seite 344
- “Verbindungsoptionen des parallelen Teradata-Transporters” auf Seite 346
- “Twitter-Verbindungsoptionen” auf Seite 348
- “Twitter Streaming-Verbindungsoptionen” auf Seite 350
- “VSAM-Verbindungsoptionen” auf Seite 351
- “Verbindungsoptionen von Web Content-Kapow Katalyst” auf Seite 353

Salesforce-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Salesforce-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:
... -o option_name=value option_name=value ...

Beispiel:

```
infacmd createConnection -dn DomainName -un Domain_UserName -pd Domain_Pwd -cn conname -
cid conname -ct SFDC -o userName=salesforceUserName password=salesforcePWD
serviceURL=https://login.salesforce.com/services/Soap/u/26.0
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Salesforce-Verbindungsoptionen für infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Option	Beschreibung
userName	Salesforce-Benutzername
Passwort	Passwort für den Salesforce-Benutzernamen Beim Passwort wird die Groß- und Kleinschreibung beachtet. Um auf Salesforce von außerhalb des vertrauenswürdigen Netzwerks Ihres Unternehmens zuzugreifen, müssen Sie einen Sicherheitstoken an Ihr Passwort anhängen, um sich bei der API oder einem Desktop-Client anzumelden. Um Ihren Sicherheitstoken zu erhalten oder zurückzusetzen, melden Sie sich bei Salesforce an und klicken auf **Setup (Einrichten)** > **My Personal Information (Meine persönlichen Daten)** > **Reset My Security Token (Meinen Sicherheitstoken zurücksetzen)**.
serviceURL	Dies ist die URL des Salesforce-Diensts, auf den Sie zugreifen möchten. In einer Test- oder Entwicklungsumgebung möchten Sie möglicherweise auf die Salesforce Sandbox-Testumgebung zugreifen. Weitere Informationen Salesforce-Sandbox finden Sie in der Salesforce-Dokumentation.

Verwandte Themen:

- "Adabas-Verbindungsoptionen" auf Seite 291
- "DataSift-Verbindungsoptionen" auf Seite 293
- "DB2 für i5/OS-Verbindungsoptionen" auf Seite 294
- "Facebook-Verbindungsoptionen" auf Seite 297
- "Greenplum-Verbindungsoptionen" auf Seite 299
- "HBase-Verbindungsoptionen" auf Seite 300
- "HDFS-Verbindungsoptionen" auf Seite 302
- "Hadoop Connection Options" auf Seite 304
- "Hive-Verbindungsoptionen" auf Seite 311
- " DB2 für z/OS-Verbindungsoptionen" auf Seite 316
- "IBM DB2-Verbindungsoptionen" auf Seite 318
- "IMS-Verbindungsoptionen" auf Seite 322
- "JDBC Connection Options" auf Seite 324
- "LinkedIn-Verbindungsoptionen" auf Seite 327
- "Microsoft SQL Server-Verbindungsoptionen" auf Seite 328
- "Netezza-Verbindungsoptionen" auf Seite 332
- "OData-Verbindungsoptionen" auf Seite 334
- " ODBC-Verbindungsoptionen" auf Seite 335
- "Oracle-Verbindungsoptionen" auf Seite 338
- "SAP-Verbindungsoptionen" auf Seite 343
- "Sequentielle Verbindungs-Optionen" auf Seite 344
- "Verbindungsoptionen des parallelen Teradata-Transporters" auf Seite 346
- "Twitter-Verbindungsoptionen" auf Seite 348
- "Twitter Streaming-Verbindungsoptionen" auf Seite 350

- “VSAM-Verbindungsoptionen” auf Seite 351
- “Verbindungsoptionen von Web Content-Kapow Katalyst” auf Seite 353

SAP-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer SAP-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die SAP-Verbindungsoptionen für infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Option	Beschreibung
UserName	Erforderlich. SAP-Systembenutzername.
Passwort	Erforderlich. Passwort für den Benutzernamen.
HostName	Erforderlich. Hostname der SAP-Anwendung.
ClientNumber	Erforderlich. SAP-Clientnummer.
SystemNumber	Erforderlich. SAP-Systemnummer.
Sprache	Optional. SAP-Anmeldesprache.

Verwandte Themen:

- “Adabas-Verbindungsoptionen” auf Seite 291
- “DataSift-Verbindungsoptionen” auf Seite 293
- “DB2 für i5/OS-Verbindungsoptionen” auf Seite 294
- “Facebook-Verbindungsoptionen” auf Seite 297
- “Greenplum-Verbindungsoptionen” auf Seite 299
- “HBase-Verbindungsoptionen” auf Seite 300
- “HDFS-Verbindungsoptionen” auf Seite 302
- “Hadoop Connection Options” auf Seite 304
- “Hive-Verbindungsoptionen” auf Seite 311
- “ DB2 für z/OS-Verbindungsoptionen” auf Seite 316
- “IBM DB2-Verbindungsoptionen” auf Seite 318
- “IMS-Verbindungsoptionen” auf Seite 322
- “JDBC Connection Options” auf Seite 324
- “LinkedIn-Verbindungsoptionen” auf Seite 327
- “Microsoft SQL Server-Verbindungsoptionen” auf Seite 328
- “Netezza-Verbindungsoptionen” auf Seite 332
- “OData-Verbindungsoptionen” auf Seite 334

- " ODBC-Verbindungsoptionen" auf Seite 335
- "Oracle-Verbindungsoptionen" auf Seite 338
- "Salesforce-Verbindungsoptionen" auf Seite 341
- "Sequentielle Verbindungs-Optionen" auf Seite 344
- "Verbindungsoptionen des parallelen Teradata-Transporters" auf Seite 346
- "Twitter-Verbindungsoptionen" auf Seite 348
- "Twitter Streaming-Verbindungsoptionen" auf Seite 350
- "VSAM-Verbindungsoptionen" auf Seite 351
- "Verbindungsoptionen von Web Content-Kapow Katalyst" auf Seite 353

Sequentielle Verbindungs-Optionen

Verwenden Sie SEQ-Verbindungsoptionen zum Definieren einer Verbindung zu einem sequentiellen z/OS-Datensatz.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die SEQ-Verbindungsoptionen für infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Option	Beschreibung
CodePage	Erforderlich. Code zum Lesen aus oder Schreiben in die sequentielle Datei. Verwenden Sie den ISO-Codepage-Namen, z. B. ISO-8859-6. Der Codepage-Name berücksichtigt keine Groß- und Kleinschreibung.
ArraySize	Optional. Bestimmt die Anzahl der Datensätze im Speicher-Array für die Threads, wenn der Worker-Threads-Wert größer als 0 ist. Gültige Werte sind 1 bis 100000. Default is 25.
Compression	Optional. Komprimiert die Daten, um die Menge an Daten zu reduzieren, die Informatica-Anwendungen über das Netzwerk schreiben. TRUE oder FALSE. Die Standardeinstellung ist "false".
EncryptionLevel	Optional. Verschlüsselungsebene für RC2 oder DES für Verschlüsselungstypen. Geben Sie einen der folgenden Werte für die Verschlüsselungsebene ein: - 1. Verwenden Sie einen 56-Bit-Kodierungsschlüssel für DES und RC2. - 2. Verwenden Sie einen 168-Bit-Triple-DES-Kodierungsschlüssel für DES oder einen 64-Bit-Kodierungsschlüssel für RC2. - 3. Verwenden Sie einen 168-Bit-Triple-DES-Kodierungsschlüssel für DES oder einen 128-Bit-Kodierungsschlüssel für RC2. Default is 1. **Hinweis:** Wenn Sie für den Verschlüsselungstyp None auswählen, ignoriert der Data Integration Service den Wert für die Verschlüsselungsebene.
EncryptionType	Optional. Geben Sie einen der folgenden Werte für den Verschlüsselungstyp ein: - Keine - RC2 - DES Die Standardeinstellung ist "None".

Option	Beschreibung
InterpretAsRows	Optional. Bei TRUE gibt die Pacing-Größe eine Anzahl von Zeilen wieder. Bei FALSE gibt die Pacing-Größe Kilobyte wieder. Die Standardeinstellung ist "false".
Location	Speicherort des PowerExchange Listener-Knotens, der eine Verbindung zur Datenquelle herstellen kann. Der Speicherort wird im ersten Parameter der NODE-Anweisung in der dbmover.cfg-Konfigurationsdatei von PowerExchange definiert.
OffLoadProcessing	Optional. Verschiebt die Stapeldatenverarbeitung vom Datenquellcomputer zum Data Integration Service-Computer. Geben Sie einen der folgenden Werte ein: - Auto. Der Data Integration Service bestimmt, ob Offload-Verarbeitung verwendet werden soll. - Yes. Offload-Verarbeitung wird verwendet. - No. Offload-Verarbeitung wird nicht verwendet. Der Standardwert ist Auto.
PacingSize	Optional. Verlangsamt die Datenübertragungsrate, um Engpässe zu reduzieren. Je geringer der Wert ist, desto höher ist die Sitzungsleistung. Der Mindestwert ist 0. Geben Sie 0 für optimale Leistung ein. Default is 0.
WorkerThread	Optional. Anzahl der vom Data Integration Service verwendeten Threads, um Stapeldaten bei aktivierter Offload-Verarbeitung zu verarbeiten. Um eine optimale Leistung zu erzielen, sollte dieser Wert die Anzahl der verfügbaren Prozessoren auf dem Data Integration Service-Computer nicht überschreiten. Gültige Werte sind 1 bis 64. Der Standardwert ist 0, der Multithreading verhindert.
WriteMode	Geben Sie einen der folgenden Schreibmodi ein: - CONFIRMWRITEON. Sendet Daten zum Data Integration Service und wartet auf eine Erfolgs-/Nichterfolgsreaktion, bevor weitere Daten gesendet werden. - CONFIRMWRITEOFF. Sendet Daten zum Data Integration Service, ohne eine Erfolgs-/Nichterfolgsreaktion abzuwarten. Verwenden Sie diese Option, wenn die Target-Tabelle bei Auftreten eines Fehlers erneut geladen werden kann. - ASYNCHRONOUSWITHFAULTT. Sendet Daten asynchron zum Data Integration Service mit der Möglichkeit der Fehlererkennung. Die Standardoption ist CONFIRMWRITEON.
EnableConnectionPool	Optional. Ermöglicht das Verbindungspooling. Wenn Sie Verbindungspooling aktivieren, behält der Verbindungspool inaktive Verbindungsinstanzen im Speicher. Wenn Sie Verbindungspooling deaktivieren, stoppt der Data Integration Service alle Poolingaktivitäten. TRUE oder FALSE. Die Standardeinstellung ist "false".
ConnectionPoolSize	Optional. Maximale Anzahl an inaktiven Verbindungsinstanzen, die der Data Integration Service für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert auf eine höhere Anzahl als die Mindestanzahl an inaktiven Verbindungsinstanzen fest. Default is 15.
ConnectionPoolMaxIdle Time	Optional. Anzahl der Sekunden, die eine die Mindestanzahl an Verbindungsinstanzen überschreitende Verbindung inaktiv bleiben kann, bevor sie vom Verbindungspool abgebrochen wird. Der Verbindungspool ignoriert die Leerlaufzeit, wenn die Mindestanzahl an inaktiven Verbindungsinstanzen nicht überschritten wird. Default is 120.
ConnectionPoolMinCon nections	Optional. Die Mindestanzahl an inaktiven Verbindungsinstanzen, die der Pool für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert so fest, dass er der Poolgröße inaktiver Verbindungen gleicht oder kleiner als diese ist. Default is 0.

Verwandte Themen:

- “Adabas-Verbindungsoptionen” auf Seite 291
- “DataSift-Verbindungsoptionen” auf Seite 293
- “DB2 für i5/OS-Verbindungsoptionen” auf Seite 294
- “Facebook-Verbindungsoptionen” auf Seite 297
- “Greenplum-Verbindungsoptionen” auf Seite 299
- “HBase-Verbindungsoptionen” auf Seite 300
- “HDFS-Verbindungsoptionen” auf Seite 302
- “Hadoop Connection Options” auf Seite 304
- “Hive-Verbindungsoptionen” auf Seite 311
- “ DB2 für z/OS-Verbindungsoptionen” auf Seite 316
- “IBM DB2-Verbindungsoptionen” auf Seite 318
- “IMS-Verbindungsoptionen” auf Seite 322
- “JDBC Connection Options” auf Seite 324
- “LinkedIn-Verbindungsoptionen” auf Seite 327
- “Microsoft SQL Server-Verbindungsoptionen” auf Seite 328
- “Netezza-Verbindungsoptionen” auf Seite 332
- “OData-Verbindungsoptionen” auf Seite 334
- “ ODBC-Verbindungsoptionen” auf Seite 335
- “Oracle-Verbindungsoptionen” auf Seite 338
- “Salesforce-Verbindungsoptionen” auf Seite 341
- “SAP-Verbindungsoptionen” auf Seite 343
- “Verbindungsoptionen des parallelen Teradata-Transporters” auf Seite 346
- “Twitter-Verbindungsoptionen” auf Seite 348
- “Twitter Streaming-Verbindungsoptionen” auf Seite 350
- “VSAM-Verbindungsoptionen” auf Seite 351
- “Verbindungsoptionen von Web Content-Kapow Katalyst” auf Seite 353

Verbindungsoptionen des parallelen Teradata-Transporters

Verwenden Sie Verbindungsoptionen zur Definition einer Teradata-PT-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name='value' option_name='value' ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

Die folgende Tabelle beschreibt die Optionen der Teradata-PT-Verbindung für infacmd isp CreateConnection- und UpdateConnection-Befehle:

Option	Beschreibung
UserName	Erforderlich. Benutzername der Teradata-Datenbank mit den entsprechenden Schreibberechtigung zum Zugriff auf die Datenbank.
Passwort	Erforderlich. Passwort für den Benutzernamen der Teradata-Datenbank.
DriverName	Erforderlich. Name des Teradata-JDBC-Treibers.
ConnectionString	Erforderlich. JDBC-URL zum Abrufen von Metadaten.
TDPID	Erforderlich. Name oder IP-Adresse des Teradata-Datenbankcomputers.
databaseName	Erforderlich. Teradata-Datenbankname. Wenn Sie keinen Datenbanknamen eingeben, verwendet die Teradata-PT-API den Standardanmeldungsnamen der Datenbank.
DataCodePage	Optional. Codepage, die mit der Datenbank verbunden ist. Beim Ausführen eines Mappings, das ein Teradata-Target lädt, muss die Codepage der Teradata-PT-Verbindung mit der Codepage des Teradata-Target übereinstimmen. Standardwert ist UTF-8.
Beharrlichkeit	Optional. Anzahl der Stunden, in denen die Teradata-PT-API weiterhin versucht, sich anzumelden, wenn die maximale Anzahl von Operationen in der Teradata-Datenbank ausgeführt wird. Muss ein positiver, ganzzahliger Wert sein, der nicht Null ist. Standardwert ist 4.
MaxSessions	Optional. Maximale Anzahl der Sitzungen, die die Teradata-PT-API mit der Teradata-Datenbank herstellt. Muss ein positiver, ganzzahliger Wert sein, der nicht Null ist. Standardwert ist 4.
MinSessions	Optional. Mindestanzahl von Teradata-PT-API-Sitzungen, die erforderlich ist, damit der Teradata-PT-API-Job fortfährt. Muss ein positiver, ganzzahliger Wert zwischen 1 und dem maximalen Wert für Sitzungen sein. Standardwert ist 1.
Ruhezustand	Optional. Anzahl der Minuten, in denen die Teradata-PT-API anhält, bevor sie wieder versucht, sich anzumelden, wenn die maximale Anzahl von Operationen in der Teradata-Datenbank ausgeführt wird. Muss ein positiver, ganzzahliger Wert sein, der nicht Null ist. Standardwert ist 6.
useMetadataJdbcUrl	Optional. Legen Sie diese Option auf TRUE fest, um anzugeben, dass der TDCH (Teradata Connector for Hadoop) die JDBC-URL verwenden muss, die in der Verbindungszeichenfolge angegeben wurde. Legen Sie diese Option auf FALSE fest, um eine andere JDBC-URL anzugeben, die vom TDCH bei der Ausführung der Zuordnung verwendet werden muss.

Option	Beschreibung
tdchJdbcUrl	Erforderlich. JDBC-URL, die TDCH beim Ausführen der Zuordnung verwenden muss.
dataEncryption	Erforderlich. Aktiviert vollständige Sicherheitsverschlüsselung von SQL-Abfragen, Antworten und Daten unter Windows. Fügen Sie zur Aktivierung von Verschlüsselung unter UNIX den Befehl UseDataEncryption=Yes zum DNS in der Datei „odbc.ini“ hinzu.

Verwandte Themen:

- “Adabas-Verbindungsoptionen” auf Seite 291
- “DataSift-Verbindungsoptionen” auf Seite 293
- “DB2 für i5/OS-Verbindungsoptionen” auf Seite 294
- “Facebook-Verbindungsoptionen” auf Seite 297
- “Greenplum-Verbindungsoptionen” auf Seite 299
- “HBase-Verbindungsoptionen” auf Seite 300
- “HDFS-Verbindungsoptionen” auf Seite 302
- “Hadoop Connection Options” auf Seite 304
- “Hive-Verbindungsoptionen” auf Seite 311
- “ DB2 für z/OS-Verbindungsoptionen” auf Seite 316
- “IBM DB2-Verbindungsoptionen” auf Seite 318
- “IMS-Verbindungsoptionen” auf Seite 322
- “JDBC Connection Options” auf Seite 324
- “LinkedIn-Verbindungsoptionen” auf Seite 327
- “Microsoft SQL Server-Verbindungsoptionen” auf Seite 328
- “Netezza-Verbindungsoptionen” auf Seite 332
- “OData-Verbindungsoptionen” auf Seite 334
- “ ODBC-Verbindungsoptionen” auf Seite 335
- “Oracle-Verbindungsoptionen” auf Seite 338
- “Salesforce-Verbindungsoptionen” auf Seite 341
- “SAP-Verbindungsoptionen” auf Seite 343
- “Sequentielle Verbindungs-Optionen” auf Seite 344
- “Twitter-Verbindungsoptionen” auf Seite 348
- “Twitter Streaming-Verbindungsoptionen” auf Seite 350
- “VSAM-Verbindungsoptionen” auf Seite 351
- “Verbindungsoptionen von Web Content-Kapow Katalyst” auf Seite 353

Twitter-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Twitter-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Twitter-Verbindungsoptionen für infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Option	Beschreibung
ConsumerKey	Der Verbraucherschlüssel, den Sie beim Erstellen der Anwendung in Twitter erhalten. Twitter verwendet die Schlüssel zur Identifizierung der Anwendung.
ConsumerSecret	Das Verbrauchergeheimwort, das Sie beim Erstellen einer Twitter-Anwendung erhalten. Twitter verwendet das Geheimwort für das Eigentum am Verbraucherschlüssel.
AccessToken	Zugriffstoken, den das OAuth-Dienstprogramm zurückgibt. Twitter verwendet diesen Token anstelle der Benutzeranmeldedaten für den Zugriff auf geschützte Ressourcen.
AccessSecret	Zugriffsgeheimwort, das das OAuth-Dienstprogramm zurückgibt. Das Geheimwort legt das Eigentum eines Token fest.

Verwandte Themen:

- “Adabas-Verbindungsoptionen” auf Seite 291
- “DataSift-Verbindungsoptionen” auf Seite 293
- “DB2 für i5/OS-Verbindungsoptionen” auf Seite 294
- “Facebook-Verbindungsoptionen” auf Seite 297
- “Greenplum-Verbindungsoptionen” auf Seite 299
- “HBase-Verbindungsoptionen” auf Seite 300
- “HDFS-Verbindungsoptionen” auf Seite 302
- “Hadoop Connection Options” auf Seite 304
- “Hive-Verbindungsoptionen” auf Seite 311
- “ DB2 für z/OS-Verbindungsoptionen” auf Seite 316
- “IBM DB2-Verbindungsoptionen” auf Seite 318
- “IMS-Verbindungsoptionen” auf Seite 322
- “JDBC Connection Options” auf Seite 324
- “LinkedIn-Verbindungsoptionen” auf Seite 327
- “Microsoft SQL Server-Verbindungsoptionen” auf Seite 328
- “Netezza-Verbindungsoptionen” auf Seite 332
- “OData-Verbindungsoptionen” auf Seite 334
- “ ODBC-Verbindungsoptionen” auf Seite 335
- “Oracle-Verbindungsoptionen” auf Seite 338
- “Salesforce-Verbindungsoptionen” auf Seite 341
- “SAP-Verbindungsoptionen” auf Seite 343

- “Sequentielle Verbindungs-Optionen” auf Seite 344
- “Verbindungsoptionen des parallelen Teradata-Transporters” auf Seite 346
- “Twitter Streaming-Verbindungsoptionen” auf Seite 350
- “VSAM-Verbindungsoptionen” auf Seite 351
- “Verbindungsoptionen von Web Content-Kapow Katalyst” auf Seite 353

Twitter Streaming-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer Twitter Streaming-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Twitter Streaming-Verbindungsoptionen für infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Option	Beschreibung
HoseType	Streaming-API-Methoden. Sie können die folgenden Methoden angeben: - Filter. Die Twitter `statuses/filter`-Methode gibt öffentliche Statusangaben zurück, die mit den Suchkriterien übereinstimmen. - Beispiel. Die Twitter `statuses/sample`-Methode gibt eine zufällige Stichprobe aus allen öffentlichen Statusangaben zurück.
UserName	Name des Twitter-Benutzerbildschirms
Passwort	Twitter-Passwort.

Verwandte Themen:

- “Adabas-Verbindungsoptionen” auf Seite 291
- “DataSift-Verbindungsoptionen” auf Seite 293
- “DB2 für i5/OS-Verbindungsoptionen” auf Seite 294
- “Facebook-Verbindungsoptionen” auf Seite 297
- “Greenplum-Verbindungsoptionen” auf Seite 299
- “HBase-Verbindungsoptionen” auf Seite 300
- “HDFS-Verbindungsoptionen” auf Seite 302
- “Hadoop Connection Options” auf Seite 304
- “Hive-Verbindungsoptionen” auf Seite 311
- “ DB2 für z/OS-Verbindungsoptionen” auf Seite 316
- “IBM DB2-Verbindungsoptionen” auf Seite 318
- “IMS-Verbindungsoptionen” auf Seite 322
- “JDBC Connection Options” auf Seite 324
- “LinkedIn-Verbindungsoptionen” auf Seite 327
- “Microsoft SQL Server-Verbindungsoptionen” auf Seite 328

- “Netezza-Verbindungsoptionen” auf Seite 332
- “OData-Verbindungsoptionen” auf Seite 334
- “ ODBC-Verbindungsoptionen” auf Seite 335
- “Oracle-Verbindungsoptionen” auf Seite 338
- “Salesforce-Verbindungsoptionen” auf Seite 341
- “SAP-Verbindungsoptionen” auf Seite 343
- “Sequentielle Verbindungs-Optionen” auf Seite 344
- “Verbindungsoptionen des parallelen Teradata-Transporters” auf Seite 346
- “Twitter-Verbindungsoptionen” auf Seite 348
- “VSAM-Verbindungsoptionen” auf Seite 351
- “Verbindungsoptionen von Web Content-Kapow Katalyst” auf Seite 353

VSAM-Verbindungsoptionen

Verwenden Sie Verbindungsoptionen zum Definieren einer VSAM-Verbindung.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die VSAM-Verbindungsoptionen für infacmd isp CreateConnection- und UpdateConnection-Befehle beschrieben:

Option	Beschreibung
CodePage	Erforderlich. Code zum Lesen aus oder Schreiben in die VSAM-Datei. Verwenden Sie den ISO-Codepage-Namen, z. B. ISO-8859-6. Der Codepage-Name berücksichtigt keine Groß- und Kleinschreibung.
ArraySize	Optional. Bestimmt die Anzahl der Datensätze im Speicher-Array für die Threads, wenn der Worker-Threads-Wert größer als 0 ist. Gültige Werte sind 1 bis 100000. Default is 25.
Compression	Optional. Komprimiert die Daten, um die Menge an Daten zu reduzieren, die Informatica-Anwendungen über das Netzwerk schreiben. TRUE oder FALSE. Die Standardeinstellung ist "false".
EncryptionLevel	Optional. Verschlüsselungsebene für RC2 oder DES für Verschlüsselungstypen. Geben Sie einen der folgenden Werte für die Verschlüsselungsebene ein: - 1. Verwenden Sie einen 56-Bit-Kodierungsschlüssel für DES und RC2. - 2. Verwenden Sie einen 168-Bit-Triple-DES-Kodierungsschlüssel für DES oder einen 64-Bit-Kodierungsschlüssel für RC2. - 3. Verwenden Sie einen 168-Bit-Triple-DES-Kodierungsschlüssel für DES oder einen 128-Bit-Kodierungsschlüssel für RC2. Default is 1. **Hinweis:** Wenn Sie für den Verschlüsselungstyp None auswählen, ignoriert der Data Integration Service den Wert für die Verschlüsselungsebene.

Option	Beschreibung
EncryptionType	Optional. Geben Sie einen der folgenden Werte für den Verschlüsselungstyp ein: - Keine - RC2 - DES Die Standardeinstellung ist "None".
InterpretAsRows	Optional. Bei TRUE gibt die Pacing-Größe eine Anzahl von Zeilen wieder. Bei FALSE gibt die Pacing-Größe Kilobyte wieder. Die Standardeinstellung ist "false".
Location	Speicherort des PowerExchange Listener-Knotens, der eine Verbindung zu VSAM herstellen kann. Der Knoten wird in der dbmover.cfg-Konfigurationsdatei von PowerExchange definiert.
OffLoadProcessing	Optional. Verschiebt die Stapeldatenverarbeitung von der VSAM-Quelle zum Data Integration Service-Computer. Geben Sie einen der folgenden Werte ein: - Auto. Der Data Integration Service bestimmt, ob Offload-Verarbeitung verwendet werden soll. - Yes. Offload-Verarbeitung wird verwendet. - No. Offload-Verarbeitung wird nicht verwendet. Der Standardwert ist Auto.
PacingSize	Optional. Verlangsamt die Datenübertragungsrate, um Engpässe zu reduzieren. Je geringer der Wert ist, desto höher ist die Sitzungsleistung. Der Mindestwert ist 0. Geben Sie 0 für optimale Leistung ein. Default is 0.
WorkerThread	Optional. Anzahl der vom Data Integration Service verwendeten Threads, um Stapeldaten bei aktivierter Offload-Verarbeitung zu verarbeiten. Um eine optimale Leistung zu erzielen, sollte dieser Wert die Anzahl der verfügbaren Prozessoren auf dem Data Integration Service-Computer nicht überschreiten. Gültige Werte sind 1 bis 64. Der Standardwert ist 0, der Multithreading verhindert.
WriteMode	Geben Sie einen der folgenden Schreibmodi ein: - CONFIRMWRITEON. Sendet Daten zum Data Integration Service und wartet auf eine Erfolgs-/Nichterfolgsreaktion, bevor weitere Daten gesendet werden. - CONFIRMWRITEOFF. Sendet Daten zum Data Integration Service, ohne eine Erfolgs-/Nichterfolgsreaktion abzuwarten. Verwenden Sie diese Option, wenn die Target-Tabelle bei Auftreten eines Fehlers erneut geladen werden kann. - ASYNCHRONOUSWITHFAULTT. Sendet Daten asynchron zum Data Integration Service mit der Möglichkeit der Fehlererkennung. Die Standardoption ist CONFIRMWRITEON.
EnableConnectionPool	Optional. Ermöglicht das Verbindungspooling. Wenn Sie Verbindungspooling aktivieren, behält der Verbindungspool inaktive Verbindungsinstanzen im Speicher. Wenn Sie Verbindungspooling deaktivieren, stoppt der Data Integration Service alle Poolingaktivitäten. TRUE oder FALSE. Die Standardeinstellung ist "false".
ConnectionPoolSize	Optional. Maximale Anzahl an inaktiven Verbindungsinstanzen, die der Data Integration Service für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert auf eine höhere Anzahl als die Mindestanzahl an inaktiven Verbindungsinstanzen fest. Default is 15.

Option	Beschreibung
ConnectionPoolMaxIdleTime	Optional. Anzahl der Sekunden, die eine die Mindestanzahl an Verbindungsinstanzen überschreitende Verbindung inaktiv bleiben kann, bevor sie vom Verbindungspool abgebrochen wird. Der Verbindungspool ignoriert die Leerlaufzeit, wenn die Mindestanzahl an inaktiven Verbindungsinstanzen nicht überschritten wird. Default is 120.
ConnectionPoolMinConnections	Optional. Die Mindestanzahl an inaktiven Verbindungsinstanzen, die der Pool für eine Datenbankverbindung aufrechterhält. Legen Sie diesen Wert so fest, dass er der Poolgröße inaktiver Verbindungen gleicht oder kleiner als diese ist. Default is 0.

Verwandte Themen:

- "Adabas-Verbindungsoptionen" auf Seite 291
- "DataSift-Verbindungsoptionen" auf Seite 293
- "DB2 für i5/OS-Verbindungsoptionen" auf Seite 294
- "Facebook-Verbindungsoptionen" auf Seite 297
- "Greenplum-Verbindungsoptionen" auf Seite 299
- "HBase-Verbindungsoptionen" auf Seite 300
- "HDFS-Verbindungsoptionen" auf Seite 302
- "Hadoop Connection Options" auf Seite 304
- "Hive-Verbindungsoptionen" auf Seite 311
- " DB2 für z/OS-Verbindungsoptionen" auf Seite 316
- "IBM DB2-Verbindungsoptionen" auf Seite 318
- "IMS-Verbindungsoptionen" auf Seite 322
- "JDBC Connection Options" auf Seite 324
- "LinkedIn-Verbindungsoptionen" auf Seite 327
- "Microsoft SQL Server-Verbindungsoptionen" auf Seite 328
- "Netezza-Verbindungsoptionen" auf Seite 332
- "OData-Verbindungsoptionen" auf Seite 334
- " ODBC-Verbindungsoptionen" auf Seite 335
- "Oracle-Verbindungsoptionen" auf Seite 338
- "Salesforce-Verbindungsoptionen" auf Seite 341
- "SAP-Verbindungsoptionen" auf Seite 343
- "Sequentielle Verbindungs-Optionen" auf Seite 344
- "Verbindungsoptionen des parallelen Teradata-Transporters" auf Seite 346
- "Twitter-Verbindungsoptionen" auf Seite 348
- "Twitter Streaming-Verbindungsoptionen" auf Seite 350
- "Verbindungsoptionen von Web Content-Kapow Katalyst" auf Seite 353

Verbindungsoptionen von Web Content-Kapow Katalyst

Verwenden Sie die Verbindungsoptionen, um eine Web Content-Kapow Katalyst-Verbindung zu definieren.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

Die folgende Tabelle beschreibt die Verbindungsoptionen von Web Content-Kapow Katalyst für infacmd isp CreateConnection- und UpdateConnection-Befehle:

Option	Beschreibung
ManagementConsoleURL	URL der lokalen Management-Konsole, wo der Robot hochgeladen wird. Die URL muss mit http oder https beginnen. Zum Beispiel http://localhost:50080.
RQLServicePort	Die Portnummer, auf der der Socket-Dienst den RQL-Dienst abhört. Geben Sie einen Wert zwischen 1 und 65535 ein. Der Standardwert ist 50000.
Benutzername	Benutzername ist erforderlich, um auf die lokale Management-Konsole zuzugreifen.
Passwort	Passwort für den Zugriff auf die lokale Management-Konsole.

Verwandte Themen:

- “Adabas-Verbindungsoptionen” auf Seite 291
- “DataSift-Verbindungsoptionen” auf Seite 293
- “DB2 für i5/OS-Verbindungsoptionen” auf Seite 294
- “Facebook-Verbindungsoptionen” auf Seite 297
- “Greenplum-Verbindungsoptionen” auf Seite 299
- “HBase-Verbindungsoptionen” auf Seite 300
- “HDFS-Verbindungsoptionen” auf Seite 302
- “Hadoop Connection Options” auf Seite 304
- “Hive-Verbindungsoptionen” auf Seite 311
- “ DB2 für z/OS-Verbindungsoptionen” auf Seite 316
- “IBM DB2-Verbindungsoptionen” auf Seite 318
- “IMS-Verbindungsoptionen” auf Seite 322
- “JDBC Connection Options” auf Seite 324
- “LinkedIn-Verbindungsoptionen” auf Seite 327
- “Microsoft SQL Server-Verbindungsoptionen” auf Seite 328
- “Netezza-Verbindungsoptionen” auf Seite 332
- “OData-Verbindungsoptionen” auf Seite 334
- “ ODBC-Verbindungsoptionen” auf Seite 335
- “Oracle-Verbindungsoptionen” auf Seite 338
- “Salesforce-Verbindungsoptionen” auf Seite 341
- “SAP-Verbindungsoptionen” auf Seite 343
- “Sequentielle Verbindungs-Optionen” auf Seite 344

- "Verbindungsoptionen des parallelen Teradata-Transporters" auf Seite 346
- "Twitter-Verbindungsoptionen" auf Seite 348
- "Twitter Streaming-Verbindungsoptionen" auf Seite 350
- "VSAM-Verbindungsoptionen" auf Seite 351

CreateFolder

Erstellt einen Ordner in der Domäne. Wenn Sie einen Ordner erstellen, erstellt infacmd den Ordner in der Domäne oder einen von Ihnen angegeben Ordner.

Sie können mit Ordnern Objekte organisieren und die Sicherheit verwalten. Ordner können Knoten, Dienste, Gitter, Lizenzen und andere Ordner enthalten.

Der Befehl „infacmd isp CreateFolder" verwendet die folgende Syntax:

```
CreateFolder

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-FolderName|-fn> folder_name

<-FolderPath|-fp> full_folder_path

[<-FolderDescription|-fd> description_of_folder]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp CreateFolder" beschrieben:

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

Option	Argument	Beschreibung
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-FolderName -fn	folder_name	Erforderlich. Name des Ordners. Ordnernamen müssen innerhalb eines Ordners bzw. der Domäne eindeutig sein. Sie dürfen maximal 79 Zeichen und keine Leerzeichen enthalten.
-FolderPath -fp	full_folder_path	Erforderlich. Vollständiger Pfad (ohne Domänenname) für die Erstellung des Ordners. Folgendes Format ist erforderlich: `/parent_folder/child_folder`
-FolderDescription -fd	description_of_folder	Optional. Beschreibung des Ordners. Wenn die Ordnerbeschreibung Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie sie in Anführungszeichen.

CreateGrid

Erstellt ein Gitter in der Domäne weist dem Gitter Knoten zu. Erstellen Sie ein Gitter, um Jobs an Dienstprozesse zu verteilen, die auf Knoten im Gitter ausgeführt werden.

Der Befehl „infacmd isp CreateGrid“ verwendet die folgende Syntax:

```
CreateGrid

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-GridName|-gn> grid_name

<-NodeList|-nl> node1 node2 ...

[<-FolderPath|-fp> full_folder_path]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp CreateGrid“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-GridName -gn	grid_name	Erforderlich. Name des Gitters.
-NodeList -nl	node1 node2 ...	Erforderlich. Name des Knotens, den Sie dem Gitter zuweisen möchten.
-FolderPath -fp	full_folder_path	Optional. Vollständiger Pfad (ohne Domänenname) des Ordners, in dem Sie das Gitter erstellen möchten. Folgendes Format ist erforderlich: */parent_folder/child_folder* Standardwert ist „/“ (die Domäne).

CreateGroup

Erstellt eine Gruppe in der nativen Sicherheitsdomäne. Sie können Rollen und Berechtigungen zu einer Gruppe in der nativen oder in einer LDAP-Sicherheitsdomäne zuweisen. Die einer Gruppe zugewiesenen Rollen und Berechtigungen legen die Aufgaben fest, die die Benutzer in der Gruppe innerhalb der Domäne durchführen können.

Der Befehl „infacmd isp CreateGroup“ verwendet die folgende Syntax:

```
CreateGroup

<-DomainName|-dn> domain_name
```

```
<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-GroupName|-gn> group_name

[<-GroupDescription|-ds> group_description]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp CreateGroup“ beschrieben:

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

Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-GroupName -gn	group_name	Erforderlich. Name der Gruppe. Der Gruppenname unterliegt nicht der Groß-/Kleinschreibung und kann 1 bis 80 Zeichen umfassen. Er darf weder Tabulatoren, Zeilenendzeichen noch folgende Sonderzeichen enthalten: `, + " \ < > ; / * % ?` Der Name kann ein ASCII-Leerzeichen enthalten, jedoch nicht als erstes oder letztes Zeichen. Alle anderen Leerzeichen sind nicht zulässig.
-GroupDescription -ds	group_description	Optional. Beschreibung der Gruppe. Um eine Beschreibung einzugeben, die Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie sie in Anführungszeichen. Die Beschreibung darf die folgenden Sonderzeichen nicht enthalten: `< > "`

CreateIntegrationService

Erstellt einen PowerCenter-Integrationsdienst in einer Domäne.

Der PowerCenter-Integrationsdienst wird standardmäßig aktiviert, wenn Sie ihn erstellen.

Der Befehl „infacmd isp CreateIntegrationService“ verwendet die folgende Syntax:

```
CreateIntegrationService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

[<-FolderPath|-fp> full_folder_path]

<<-NodeName|-nn> node_name|<-GridName|-gn> grid_name>
```

```
[<-BackupNodes|-bn> node1 node2 ...]

<-RepositoryService|-rs> repository_service_name

[<-RepositoryUser|-ru> repository_user]

[<-RepositoryPassword|-rp> repository_password]

[<-RepositoryUserSecurityDomain|-rsdn> repository_user_security_domain]

[<-ServiceDisable|-sd>]

[<-ServiceOptions|-so> option_name=value ...]

[<-ServiceProcessOptions|-po> option_name=value ...]

[<-EnvironmentVariables|-ev> name=value ...]

[<-LicenseName|-ln> license_name]
```

Hinweis: Für infacmd isp CreateIntegrationService dürfen die Optionen -ru, -rp und -rsdn in der Kerberos-Authentifizierung nicht verwendet werden. Wenn Sie diese Optionen im Kerberos-Modus verwenden, schlägt der Befehl fehl.

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp CreateIntegrationService“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, gilt der während der Installation festgelegte Benutzerbereich als Standardeinstellung.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des PowerCenter-Integrationsdiensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositorys kompatibel sein. Der Name darf maximal 79 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten: `/ * ? < > " |`
-FolderPath -fp	full_folder_path	Optional. Vollständiger Pfad (ohne Domänenname) des Ordners, in dem Sie den Integrationsdienst erstellen möchten. Folgendes Format ist erforderlich: *`/parent_folder/child_folder`* Standardwert ist „/“ (die Domäne).
-NodeName -nn	node_name	Erforderlich, wenn Sie den Gitternamen nicht angeben. Name des Knotens, auf dem der PowerCenter-Integrationsdienst-Prozess ausgeführt werden soll. Wenn die PowerCenter-Umgebung für hohe Verfügbarkeit konfiguriert ist, gibt diese Option den Namen des primären Knotens an. Starten Sie den Integrationsdienst neu, damit die Änderungen wirksam werden.

Option	Argument	Beschreibung
-GridName -gn	grid_name	Erforderlich, wenn Sie den Knotennamen nicht angeben. Name des Gitters, in dem der PowerCenter-Integrationsdienst-Prozess ausgeführt werden soll. Starten Sie den PowerCenter-Integrationsdienst neu, um die Änderungen zu übernehmen.
-BackupNodes -bn	node1 node2 ...	Optional. Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist. Sie können Sicherungsknoten konfigurieren, wenn Sie hohe Verfügbarkeit haben.
-RepositoryService -rs	repository_service_name	Erforderlich. Name des PowerCenter-Repository-Diensts, von dem der PowerCenter-Integrationsdienst abhängt. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen. Starten Sie den PowerCenter-Integrationsdienst neu, um die Änderungen zu übernehmen.
-RepositoryUser -ru	repository_user	Erforderlich für native und LDAP-Authentifizierung. Benutzername zum Herstellen einer Verbindung zum PowerCenter-Repository. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen. Starten Sie den PowerCenter-Integrationsdienst neu, um die Änderungen zu übernehmen.
-RepositoryPassword -rp	repository_password	Erforderlich für native und LDAP-Authentifizierung. Benutzerpasswort. Sie können ein Passwort mit der Option -rp oder der Umgebungsvariable INFA_REPOSITORY_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -rp festgelegte Passwort Vorrang. Starten Sie den PowerCenter-Integrationsdienst neu, um die Änderungen zu übernehmen.
-RepositoryUserSecurityDomain -rsdn	repository_user_security_domain	Erforderlich für LDAP. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der PowerCenter-Repository-Benutzer gehört. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn Sie diese Option nicht angeben, setzt der Befehl die Sicherheitsdomäne des Repository-Benutzers auf nativ.
-ServiceDisable -sd	-	Optional. Erstellt einen deaktivierten Dienst. Sie müssen den Dienst aktivieren, bevor Sie ihn ausführen können.
-ServiceOptions -so	option_name=value	Optional. Diensteigenschaften, mit denen definiert wird, wie der PowerCenter-Integrationsdienst ausgeführt wird.

Option	Argument	Beschreibung
-ServiceProcessOptions -po	option_name=value	Optional. Dienstprozesseigenschaften für den PowerCenter-Integrationsdienst. In einer Umgebung mit Gittern oder mehreren Knoten wendet infacmd diese Eigenschaften auf den primären Knoten, das Gitter und den Backup-Knoten an.
-EnvironmentVariables -ev	name=value	Optional. Geben Sie Umgebungsvariablen als PowerCenter-Integrationsdienst-Prozessoptionen an. Möglicherweise möchten Sie zusätzliche Variablen aufnehmen, die für Ihre PowerCenter-Umgebung eindeutig sind. Starten Sie den Knoten neu, damit die Änderungen wirksam werden.
-LicenseName -ln	license_name	Erforderlich, wenn Sie einen aktivierten Dienst erstellen. Name der Lizenz, die Sie dem PowerCenter-Integrationsdienst zuweisen möchten. Starten Sie den PowerCenter-Integrationsdienst neu, um die Änderungen zu übernehmen.

Integrationsdienst-Optionen

Geben Sie Integrationsdienst-Optionen im folgenden Format ein:

```
infacmd CreateIntegrationService ... -so option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die IIntegrationsdienst-Optionen beschrieben:

Option	Beschreibung
$PMFailureEmailUser	Optional. E-Mail-Adresse des Benutzers, um E-Mail bei fehlerhaftem Abschluss einer Sitzung zu erhalten. Um mehrere Adressen unter Windows einzugeben, verwenden Sie eine Verteilungsliste. Um mehrere Adressen unter UNIX einzugeben, trennen Sie sie durch ein Komma.
$PMSessionErrorThreshold	Optional. Anzahl der nicht schwerwiegenden Fehler, die der Integrationsdienst vor dem Abbruch der Sitzung zulässt. Der Standardwert lautet „0“ (nicht schwerwiegende Fehler führen nicht zum Anhalten der Sitzung).
$PMSessionLogCount	Optional. Anzahl der Sitzungsprotokolle, die der Integrationsdienst für die Sitzung archiviert. Der Mindestwert lautet „0“. 0 ist voreingestellt.
$PMSuccessEmailUser	Optional. E-Mail-Adresse des Benutzers, um E-Mail bei erfolgreichem Abschluss der Sitzung zu empfangen. Um mehrere Adressen unter Windows einzugeben, verwenden Sie eine Verteilungsliste. Um mehrere Adressen unter UNIX einzugeben, trennen Sie sie durch ein Komma.

Option	Beschreibung
$PMWorkflowLogCount	Optional. Anzahl der Arbeitsablaufprotokolle, die der Integrationsdienst für den Arbeitsablauf archiviert. Der Mindestwert lautet „0“. 0 ist voreingestellt.
AggregateTreatNullAsZero	Optional. Behandelt Nullen als NULL in den Aggregatorumwandlungen. Der Standardwert lautet „Nein“.
AggregateTreatRowAsInsert	Optional. Führt Aggregat-Berechnungen vor dem Markieren von Datensätzen zum Einfügen, Aktualisieren, Löschen oder Ablehnen in Update-Strategie-Ausdrücken durch. Der Standardwert lautet „Nein“.

ClientStore	Optional. Geben Sie den Wert für ClientStore mit folgender Syntax ein:
	`<path>/<filename>`
	Beispiel:
	`./Certs/client.keystore`

CreateIndicatorFiles	Optional. Erstellt Indikatordateien beim Ausführen eines Arbeitsablaufs mit einem Einfachdateiziel. Der Standardwert lautet „Nein“.
DataMovementMode	Optional. Modus, mit dem festgelegt wird, wie der Integrationsdienst Zeichendaten verarbeitet: - ASCII - Unicode Der Standardwert ist „ASCII“.
DateDisplayFormat	Optional. Datumsformat, das der Integrationsdienst in Protokolleinträgen verwendet. Der Standardwert lautet „DY MON DD HH 24:MI:SS YYYY“.
DateHandling40Compatibility	Optional. Verarbeitet Daten wie in PowerCenter 1.0/PowerMart 4.0. Der Standardwert lautet „Nein“.
DeadlockSleep	Optional. Anzahl der Sekunden, bevor der Integrationsdienst nach einem Datenbank-Deadlock erneut versucht, in die Zieldatenbank zu schreiben. Der Mindestwert lautet „0“. Der maximale Wert lautet „2.147.483.647“. Der Standardwert lautet „0“ (sofort versuchen, in das Ziel zu schreiben).
ErrorSeverityLevel	Optional. Niedrigste Stufe der Fehlerprotokollierung für Integrationsdienstprotokolle: - Fatal - Fehler - Warnung - Info - Trace - Debug Der Standardwert lautet „Info“.

Option	Beschreibung
ExportSessionLogLibName	Optional. Name der externen Bibliotheksdatei zum Schreiben der Sitzungsprotokollmeldungen.
FlushGMDWrite	Erforderlich, wenn Sie Sitzungswiederherstellung aktivieren. Bewirkt das Flushen der Sitzungswiederherstellungsdaten für die Wiederherstellungsdatei aus dem Betriebssystempuffer auf Diskette. Geben Sie einen der folgenden Levels an: - Auto. Flusht Wiederherstellungsdaten für alle Echtzeitsitzungen mit einer JMS- oder WebSphere MQ-Quelle und einem nicht relationalen Target. - Yes. Flusht Wiederherstellungsdaten für alle Sitzungen. - No. Flusht keine Wiederherstellungsdaten. Wählen Sie diese Option aus, wenn Sie über hochverfügbare externe Systeme verfügen oder wenn Sie die Leistung optimieren müssen. Der Standardwert ist Auto.
HttpProxyDomäne	Optional. Domäne für die Authentifizierung
HttpProxyPasswort	Erforderlich, wenn der Proxyserver Authentifizierung erfordert. Passwort für den authentifizierten Benutzer
HttpProxyPort	Optional. Portnummer des HTTP-Proxy-Servers
HttpProxyServer	Optional. Name des HTTP-Proxy-Servers
HttpProxyBenutzer	Erforderlich, wenn der Proxyserver Authentifizierung erfordert. Authentifizierter Benutzername für den HTTP-Proxy-Server
IgnoreResourceRequirements	Optional. Ignoriert Ressourcenanforderungen für Aufgaben bei der Verteilung von Aufgaben an die Knoten in einem Gitter. Der Standardwert lautet „Ja“.
JCEProvider	Optional. JCEProvider-Klassennamen zum Unterstützen der NTLM-Authentifizierung. Beispiel: `com.unix.crypto.provider.UnixJCE.`
JoinerSourceOrder6xCompatibility	Optional. Verarbeitet Master- und Detail-Pipelines nacheinander wie in PowerCenter-Versionen vor Version 7.0. Der Standardwert lautet „Nein“.
LoadManagerAllowDebugging	Optional. Erlaubt Ihnen, den Integrationsdienst zum Ausführen von Debugger-Sitzungen über den Designer zu verwenden. Der Standardwert lautet „Ja“.
LogsInUTF8	Optional. Schreibt alle Protokolle mit dem UTF-8-Zeichensatz. Der Standardwert lautet „Ja“ (Unicode) oder „Nein“ (ASCII).
MSExchangeProfile	Optional. Vom Dienststartkonto zum Senden einer E-Mail nach der Sitzung verwendetes Microsoft Exchange-Profil.

Option	Beschreibung
MaxLookupSPDBConnections	Optional. Maximale Anzahl an Verbindungen für eine Lookup-Datenbank oder eine Datenbank für gespeicherte Prozeduren beim Starten einer Sitzung. Der Mindestwert lautet „0“. 0 ist voreingestellt.
MaxMSSQLConnections	Optional. Maximale Anzahl an Verbindungen zu einer Microsoft SQL Server-Datenbank beim Starten einer Sitzung Der Mindestwert lautet „100“. Der maximale Wert lautet „2.147.483.647“. Standardwert ist 100.
MaxResilienceTimeout	Optional. Maximaler Zeitraum in Sekunden, in dem der Dienst die Ressourcen zwecks Belastbarkeit beibehält. Der Standardwert lautet „180“.
MaxSybaseConnections	Optional. Maximale Anzahl an Verbindungen zu einer Sybase-Datenbank beim Starten einer Sitzung. Der Mindestwert lautet „100“. Der maximale Wert lautet „2.147.483.647“. Standardwert ist 100.
NumOfDeadlockRetries	Optional. Anzahl der Versuche, die der Integrationsdienst nach einem Datenbank-Deadlock unternimmt, erneut in eine Zieldatenbank zu schreiben. Der Mindestwert lautet „10“. Der maximale Wert lautet „1.000.000.000“. Standardwert ist 10.
OperatingMode	Optional. Betriebsmodus für den Integrationsdienst: - Normal - Sicher Der Standardwert lautet „Normal“.
OperatingModeOnFailover	Optional. Betriebsmodus den Integrationsdienst beim Failover des Dienstprozesses: - Normal - Sicher Der Standardwert lautet „Normal“.
OutputMetaDataForFF	Optional. Schreibt den Spaltenheader in die Einfachdateiziele. Der Standardwert lautet „Nein“.
PersistRuntimeStatsToRepo	Optional. Ebene der im Repository gespeicherten Laufzeitinformationen. Geben Sie einen der folgenden Levels an: - None. Integration Service speichert keine Sitzungs- oder Arbeitsablaufinformationen zur Laufzeit im Repository. - Normal. Integration Service speichert Arbeitsablaufdetails, Aufgabendetails, Sitzungsstatistiken sowie die Quell- und Target-Statistiken im Repository. - Verbose. Integration Service speichert Arbeitsablaufdetails, Aufgabendetails, Sitzungsstatistiken, Quell- und Target-Statistiken, Partitionsdetails und Leistungsdetails im Repository. Der Standardwert lautet „Normal“.
Pmserver3XCompatibility	Optional. Verarbeitet Aggregatorumwandlungen wie der PowerMart-Server in PowerMart 3.5. Der Standardwert lautet „Nein“.

Option	Beschreibung
RunImpactedSessions	Optional. Führt Sitzungen aus, die von den Abhängigkeits-Aktualisierungen beeinflusst sind. Der Standardwert lautet „Nein“.
ServiceResilienceTimeout	Optional. Zeitraum in Sekunden, in dem der Dienst versucht, eine Verbindung zu einem anderen Dienst herzustellen oder erneut herzustellen. Der Standardwert lautet „180“.
StoreHAPersistenceInDB	Optional. Speichert Informationen zum Prozessstatus in Persistenzdatenbanktabellen der zugehörigen PowerCenter-Repository-Datenbank. Der Standardwert lautet „Nein“.
TimestampWorkflowLogMessages	Optional. Hängt einen Zeitstempel für die in das Arbeitsablaufprotokoll geschriebenen Nachrichten an. Der Standardwert lautet „Nein“.
TreatCharAsCharOnRead	Optional. Behält nachgestellte Leerzeichen beim Lesen von SAP- oder PeopleSoft CHAR-Daten bei. Der Standardwert lautet „Ja“.
TreatDBPartitionAsPassThrough	Optional. Verwendet Pass-Through-Partitionierung für Nicht-DB2-Ziele, wenn es sich um den Partitionstyp „Datenbankpartitionierung“ handelt. Der Standardwert lautet „Nein“.
TreatNullInComparisonOperatorsAs	Optional. Legt fest, wie der Integrationsdienst Nullwerte in Vergleichsoperationen bewertet: - Null - Low - High Der Standardwert lautet „Null“.

TrustStore	Optional. Geben Sie den Wert für TrustStore mit der folgenden Syntax ein:
	`<path>/<filename>`
	Beispiel:
	`./Certs/trust.keystore`

UseOperatingSystemProfiles	Optional. Ermöglicht die Verwendung von Betriebssystemprofilen. Verwenden Sie diese Option, wenn der Integrationsdienst unter UNIX ausgeführt wird.
ValidateDataCodePages	Optional. Erzwingt Kompatibilität der Daten-Codepage. Der Standardwert lautet „Ja“.
WriterWaitTimeOut	Optional. Im zielbasierten Übergabemodus der Zeitraum in Sekunden, in dem sich der Schreibvorgang im Leerlauf befindet, bevor er eine Übergabe ausgibt. Der Mindestwert lautet „60“. Der maximale Wert lautet „2.147.483.647“. Der Standardwert lautet „60“.
XMLWarnDupRows	Optional. Schreibt Warnungen über duplizierte Zeilen und duplizierte Zeilen für XML-Ziele in das Sitzungsprotokoll. Der Standardwert lautet „Ja“.

Integration Service-Prozessoptionen

Geben Sie Dienstprozessoptionen im folgenden Format ein:

```
infacmd CreateIntegrationService ... -po option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Integration Service-Prozessoptionen beschrieben:

Option	Beschreibung
$PMBadFileDir	Optional. Standardverzeichnis für Ablehnungsdateien. Es darf die folgenden Sonderzeichen nicht enthalten: * ? < > " | , Die Standardeinstellung ist $PMRootDir/BadFiles.
$PMCacheDir	Optional. Standardverzeichnis für Index- und Datencache-Dateien. Es darf die folgenden Sonderzeichen nicht enthalten: * ? < > " | , Die Standardeinstellung ist $PMRootDir/Cache.
$PMExtProcDir	Optional. Standardverzeichnis für externe Prozeduren. Es darf die folgenden Sonderzeichen nicht enthalten: * ? < > " | , Die Standardeinstellung ist $PMRootDir/ExtProc.
$PMLookupFileDir	Optional. Standardverzeichnis für Lookup-Dateien. Es darf die folgenden Sonderzeichen nicht enthalten: * ? < > " | , Die Standardeinstellung ist $PMRootDir/LkpFiles.
$PMRootDir	Optional. Root-Verzeichnis, auf das vom Knoten aus zugegriffen werden kann. Es darf die folgenden Sonderzeichen nicht enthalten: * ? < > " | , Die Standardeinstellung ist C:\Informatica\PowerCenter8.6\server\infa_shared.
$PMSessionLogDir	Optional. Standardverzeichnis für Sitzungsprotokolle. Es darf die folgenden Sonderzeichen nicht enthalten: * ? < > " | , Die Standardeinstellung ist $PMRootDir/SessLogs.
$PMSourceFileDir	Optional. Standardverzeichnis für Quelldateien. Es darf die folgenden Sonderzeichen nicht enthalten: * ? < > " | , Die Standardeinstellung ist $PMRootDir/SrcFiles.
$PMStorageDir	Optional. Standardverzeichnis für Laufzeitdateien. Es darf die folgenden Sonderzeichen nicht enthalten: * ? < > " | , Die Standardeinstellung ist $PMRootDir/Storage.

Option	Beschreibung
$PMTargetFileDir	Optional. Standardverzeichnis für Target-Dateien. Es darf die folgenden Sonderzeichen nicht enthalten: * ? < > " | , Die Standardeinstellung ist $PMRootDir/TgtFiles.
$PMTempDir	Optional. Standardverzeichnis für temporäre Dateien. Es darf die folgenden Sonderzeichen nicht enthalten: * ? < > " | , Die Standardeinstellung ist $PMRootDir/Temp.
$PMWorkflowLogDir	Optional. Standardverzeichnis für Arbeitsablaufprotokolle. Es darf die folgenden Sonderzeichen nicht enthalten: * ? < > " | , Die Standardeinstellung ist $PMRootDir/WorkflowLogs.
Codepage_ID	Erforderlich. ID-Nummer der Codepage für den Integration Service-Prozess.
JVMClassPath	Optional. Java SDK-Klassenpfad.
JVMMaxMemory	Optional. Der Maximalspeicher, den das Java SDK während einer PowerCenter-Sitzung verwendet. Der Standardwert beträgt 64 MB.
JVMMinMemory	Optional. Der Mindestspeicher, den das Java SDK während einer PowerCenter-Sitzung verwendet. Der Standardwert beträgt 32 MB.

CreateMMService

Erstellt einen Metadata Manager-Dienst in der Domäne. Der Metadata Manager-Dienst wird standardmäßig deaktiviert, wenn Sie ihn erstellen. Führen Sie infacmd EnableService aus, um den Metadata Manager-Dienst zu aktivieren.

Der Befehl „infacmd isp CreateMMService“ verwendet die folgende Syntax:

```
CreateMMService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-NodeName|-nn> node_name

<-ServiceOptions|-so> option_name=value ...>

[<-LicenseName|-ln> license_name]
```

```
[<-FolderPath|-fp> full_folder_path]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp CreateMMService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des Metadata Manager-Diensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf nicht länger als 79 Zeichen sein und keine Leerzeichen, Wagenrückläufe, Tabulatoren oder die folgenden Zeichen enthalten: `/ * ? < > " |`
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem die Metadata Manager-Anwendung ausgeführt werden soll.
-ServiceOptions -so	option_name=value	Optional. Diensteigenschaften, mit denen definiert wird, wie der Metadata Manager-Dienst ausgeführt wird.
-LicenseName -ln	license_name	Erforderlich. Name der Lizenz, die Sie dem Metadata Manager-Dienst zuweisen möchten.
-FolderPath -fp	full_folder_path	Optional. Vollständiger Pfad (ohne Domänenname) des Ordners, in dem Sie den Metadata Manager-Dienst erstellen möchten. Folgendes Format ist erforderlich: */parent_folder/child_folder* Standardwert ist „/“ (die Domäne).

Metadata Manager-Dienst-Optionen

Geben Sie Metadata Manager-Dienst-Optionen im folgenden Format ein:

```
infacmd isp CreateMMService ... -so option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Metadata Manager-Dienst-Optionen beschrieben:

Option	Beschreibung
AgentPort	Erforderlich. Portnummer für den Metadata Manager Agent. Der Agent verwendet diesen Port zum Kommunizieren mit Metadaten-Quell-Repositorys. Standard ist 10251.
CodePage	Erforderlich. Codepage-Beschreibung für das Metadata Manager-Repository. Um eine Codepage einzugeben, die ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

Option	Beschreibung
ConnectString	Erforderlich. Nativer Verbindungsstring für die Metadata Manager-Repository-Datenbank.
DBUser	Erforderlich. Benutzerkonto für die Metadata Manager-Repository-Datenbank.
DBPassword	Erforderlich. Passwort für den Metadata Manager-Repository-Datenbankbenutzer. Benutzerpasswort. Sie können ein Passwort mit der Option -so oder der Umgebungsvariable INFA_DEFAULT_DATABASE_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -so festgelegte Passwort Vorrang.
DatabaseHostname	Erforderlich. Hostname für die Metadata Manager-Repository-Datenbank.
DatabaseName	Erforderlich. Vollständiger Dienstname oder SID für Oracle-Datenbanken. Dienstname für IBM DB2-Datenbanken. Datenbankname für eine Microsoft SQL Server-Datenbank.
DatabasePort	Erforderlich. Portnummer für die Metadata Manager-Repository-Datenbank.
DatabaseType	Erforderlich. Typ der Datenbank für das Metadata Manager-Repository.
ErrorSeverityLevel	Optional. Level der in das Metadata Manager-Dienstprotokoll geschriebenen Fehlermeldungen Die Standardeinstellung ist ERROR.
FileLocation	Erforderlich. Speicherort der von der Metadata Manager-Anwendung verwendeten Dateien.
JdbcOptions	Optional. Weitere JDBC-Optionen. Sie können diese Eigenschaft verwenden, um die folgenden Informationen anzugeben: - Speicherort des Sicherungsservers - Oracle ASO (Advanced Security Option)-Parameter - Microsoft SQL Server-Authentifizierungsparameter - Zusätzliche JDBC-Parameter bei Aktivierung der sicheren Kommunikation für die Metadata Manager-Repository-Datenbank Weitere Informationen zu diesen Parametern finden Sie im *Handbuch für Informatica-Anwendungsdienste*.
MaxConcurrentRequests	Optional. Maximale Anzahl von Anfragen für die Verarbeitung verfügbarer Threads, die die maximale Anzahl der Clients-Anfragen bestimmt, die der Metadata Manager gleichzeitig bearbeiten kann. Standardwert ist 100.
MaxHeapSize	Optional. Dem JVM (Java Virtual Manager), auf dem Metadata Manager ausgeführt wird, zugeordnete RAM-Größe (in MB). Standard ist 512.
MaxQueueLength	Optional. Maximale Warteschlangenlänge für eingehende Verbindungsanfragen, wenn alle möglichen Anfragen verarbeitende Threads von der Metadata Manager-Anwendung genutzt werden Standardwert ist 500.
MaximumActiveConnections	Optional. Anzahl der für die Metadata Manager-Repository-Datenbank verfügbaren aktiven Verbindungen. Die Metadata Manager-Anwendung unterhält einen Verbindungpool für die Verbindung zur Repository-Datenbank. Standard ist 20.
MaximumWaitTime	Optional. Max. Zeitraum (in Sekunden), für den der Metadata Manager die Datenbank-Verbindungsanfragen im Verbindungspool speichert Standardwert ist „180“.

Option	Beschreibung
MetadataTreeMaxFolderChilds	Optional. Anzahl der untergeordneten Objekte, die im Metadata Manager-Metadatenkatalog für alle übergeordneten Objekte angezeigt werden Standardwert ist 100.
ODBCConnectionMode	Vom Integrationsdienst verwendeter Verbindungsmodus, um eine Verbindung zu Metadatenquellen und dem Metadata Manager-Repository beim Laden von Ressourcen herzustellen. Der Wert kann TRUE oder FALSE sein. Sie müssen diese Eigenschaft auf „true“ festlegen, wenn der Integrationsdienst auf einem UNIX-Computer ausgeführt wird und Sie Metadaten aus einer Microsoft SQL Server-Datenbank laden möchten oder wenn Sie eine Microsoft SQL Server-Datenbank für das Metadata Manager-Repository verwenden.
OracleConnType	Erforderlich, wenn Sie Oracle als DatabaseType auswählen. Oracle-Verbindungstyp. Sie können eine der folgenden Optionen eingeben: - OracleSID - OracleServiceName
PortNumber	Erforderlich. Portnummer, auf der die Metadata Manager-Anwendung ausgeführt wird. Standard ist 10250.
StagePoolSize	Optional. Maximale Anzahl der Ressourcen, die vom Metadata Manager gleichzeitig geladen werden Standard ist 3.
TablespaceName	Tablespace-Name für das Metadata Manager-Repository unter IBM DB2.
TimeoutInterval	Optional. Zeitraum in Minuten, in dem der Metadata Manager eine fehlgeschlagene Ressourcenlast in der Ladewarteschlange speichert. Standard ist 30.
URLScheme	Erforderlich. Gibt das Sicherheitsprotokoll an, das Sie für die Metadata Manager-Anwendung konfigurieren: HTTP oder HTTPS.
keystoreFile	Erforderlich, wenn Sie HTTPS verwenden. Schlüsselspeicherdatei, in der die Schlüssel und Zertifikate enthalten sind, die bei Verwendung des SSL-Sicherheitsprotokolls mit der Metadata Manager-Anwendung erforderlich sind.

CreateOSProfile

Erstellt ein Betriebssystemprofil in der Domäne. Bevor Sie Arbeitsabläufe ausführen, die Betriebssystemprofile verwenden, müssen Sie den PowerCenter-Integrationsdienst zur Verwendung von Betriebssystemprofilen konfigurieren.

Der Befehl „infacmd isp CreateOSProfile“ verwendet die folgende Syntax:

```
CreateOSProfile

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
```

```
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-OSProfileName|-on> OSProfile_name
<-SystemName|-sn> system_username
[<-IntegrationServiceProcessOptions|-po> option_name=value ...
[<-EnvironmentVariables|-ev> name=value ...]
[<-DISProcessVariables|-diso> option_name=value ...]
[<-DISEnvironmentVariables|-dise> name=value ...]
[<-HadoopImpersonationProperties|-hipr> hadoop_impersonation_properties]
[<-HadoopImpersonationUser|-hu> hadoop_impersonation_user]
[<-UseLoggedInUserAsProxy|-ip> use_logged_in_user_as_proxy]
[<-ProductExtensionName|-pe> product_extension_name]
[<-ProductOptions|-o> optionGroupName.optionName=Value ...]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp CreateOSProfile“ beschrieben:

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

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-OSProfileName -on	OSProfile_name	Erforderlich. Name des Betriebssystemprofils. Der Name des Betriebssystemprofils kann bis zu 80 Zeichen enthalten. Er darf weder Leerzeichen noch die folgenden Sonderzeichen enthalten: `% * + \ / ? ; < >`
-SystemName -sn	system_username	Erforderlich. Name eines Betriebssystembenutzers, der auf den Computern vorhanden ist, auf denen der Integrationsdienst ausgeführt wird. Der Integrationsdienst führt Arbeitsabläufe mit dem Systemzugriff desjenigen Systembenutzers aus, der für das Betriebssystemprofil definiert wurde.
-IntegrationServiceProcessOptions -po	option_name=value	Optional. Dienstprozesseigenschaften, mit denen definiert wird, wie der PowerCenter-Integrationsdienst ausgeführt wird.
-EnvironmentVariables -ev	name=value	Optional. Name und Wert von Umgebungsvariablen, die vom PowerCenter-Integrationsdienst zur Laufzeit verwendet werden.
-DISProcessVariables -diso	option_name=value	Optional. Dienstprozesseigenschaften, mit denen definiert wird, wie der Datenintegrationsdienst ausgeführt wird.
-DISEnvironmentVariables -dise	name=value	Optional. Name und Wert von Umgebungsvariablen, die vom Datenintegrationsdienst zur Laufzeit verwendet werden.
-HadoopImpersonationProperties -hipr	hadoop_impersonation_properties	Optional. Gibt an, ob der Datenintegrationsdienst den Hadoop-Identitätswechselbenutzer zum Ausführen von Mappings, Arbeitsabläufen und Profiling-Aufträgen in einer Hadoop-Umgebung verwendet. Gültige Werte sind „True“ oder „False“.

Option	Argument	Beschreibung
-HadoopImpersonationUser -hu	hadoop_impersonation_user	Optional. Geben Sie einen Benutzernamen für den Datenintegrationsdienst zum Identitätswechsel an, wenn er einen Auftrag in einer Hadoop-Umgebung ausführt.
-UseLoggedInUserAsProxy -ip	use_logged_in_user_as_proxy	Optional. Gibt an, ob der angemeldete Benutzer als Hadoop-Identitätswechselbenutzer verwendet werden soll. Gültige Werte sind „True“ oder „False“.
-ProductExtensionName -pe	product_extension_name	Optional. Für zukünftige Verwendung reserviert.
-ProductOptions -o	optionGroupName.optionName=Value	Optional. Für zukünftige Verwendung reserviert.

Datenintegrationsdienst-Prozessoptionen für Betriebssystemprofile

Geben Sie die Prozessoptionen des Datenintegrationsdiensts in folgendem Format ein:

```
infacmd CreateOSProfile ... -diso option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Prozessoptionen des Datenintegrationsdiensts beschrieben:

Option	Beschreibung
$DISRootDir	Root-Verzeichnis, auf das vom Knoten aus zugegriffen werden kann. Dies ist das Root-Verzeichnis für andere Dienstprozessvariablen. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " | , [ ]
$DISTempDir	Verzeichnis für temporäre Dateien, die während der Ausführung von Jobs erstellt werden. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " | , [ ] Standardwert ist <Root-Verzeichnis>/disTemp.
$DISCacheDir	Verzeichnis für Index- und Daten-Cache-Dateien für Umwandlungen. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " | , [ ] Standardwert ist <Root-Verzeichnis>/cache.

Option	Beschreibung
$DISSourceDir	Verzeichnis für Einfachdateien der Quelle, die in einem Mapping verwendet werden. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " | , [ ] Standardwert ist <Root-Verzeichnis>/source.
$DISTargetDir	Verzeichnis für Einfachdateien des Ziels, die in einem Mapping verwendet werden. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " | , [ ] Standardwert ist <Root-Verzeichnis>/target.
$DISRejectedFilesDir	Verzeichnis für Ablehnungsdateien. Ablehnungsdateien enthalten Zeilen, die beim Ausführen eines Mappings zurückgewiesen wurden. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " | , [ ] Standardwert ist <Root-Verzeichnis>/reject.
$DISLogDir	Verzeichnis für Protokolle. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " | , [ ] Standardwert ist <Root-Verzeichnis>/disLogs.

PowerCenter-Integrationsdienst-Prozessoptionen für Betriebssystemprofile

Geben Sie die Prozessoptionen des PowerCenter-Integrationsdiensts in folgendem Format ein:

```
infacmd CreateOSProfile ... -po option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Prozessoptionen des PowerCenter-Integrationsdiensts beschrieben:

Option	Beschreibung
$PMBadFileDir	Optional. Verzeichnis für Ablehnungsdateien. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " | , Standardwert ist $PMRootDir/BadFiles.
$PMCacheDir	Optional. Verzeichnis für Index- und Datencache-Dateien. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " | , Standardwert ist $PMRootDir/Cache.
$PMExtProcDir	Optional. Verzeichnis für externe Prozeduren. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " | , Standardwert ist $PMRootDir/ExtProc.

Option	Beschreibung
$PMLookupFileDir	Optional. Verzeichnis für Lookup-Dateien. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " | , Standardwert ist $PMRootDir/LkpFiles.
$PMRootDir	Optional. Root-Verzeichnis, auf das vom Knoten aus zugegriffen werden kann. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " | , Standardwert ist C:\Informatica\PowerCenter\server\infa_shared.
$PMSessionLogDir	Optional. Verzeichnis für Sitzungsprotokolle. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " | , Standardwert ist $PMRootDir/SessLogs.
$PMSourceFileDir	Optional. Verzeichnis für Quelldateien. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " | , Standardwert ist $PMRootDir/SrcFiles.
$PMStorageDir	Optional. Verzeichnis für Laufzeitdateien. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " | , Standardwert ist $PMRootDir/Storage.
$PMTargetFileDir	Optional. Verzeichnis für Zieldateien. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " | , Standardwert ist $PMRootDir/TgtFiles.
$PMTempDir	Optional. Verzeichnis für temporäre Dateien. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " | , Standardwert ist $PMRootDir/Temp.

CreateRepositoryService

Erstellt einen PowerCenter-Repository-Dienst in einer Domäne.

Der PowerCenter-Repository-Dienst wird standardmäßig bei seiner Erstellung aktiviert.

Ein PowerCenter-Repository-Dienst verwaltet ein Repository. Er führt alle Metadatentransaktionen zwischen dem Repository und Repository-Clients aus.

Der Befehl „infacmd isp CreateRepositoryService“ verwendet die folgende Syntax:

```
CreateRepositoryService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name
```

```
<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-NodeName|-nn> node_name

[<-BackupNodes|-bn> node1 node2 ...]

[<-ServiceDisable|-sd>]

<-ServiceOptions|-so> option_name=value ...

[<-LicenseName|-ln> license_name]

[<-FolderPath|-fp> full_folder_path]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp CreateRepositoryService“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des PowerCenter-Repository-Diensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositorys kompatibel sein. Der Name darf maximal 79 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten: `\ / : * ? < > " |`
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der PowerCenter-Repository-Dienstprozess ausgeführt werden soll. Wenn die PowerCenter-Umgebung für hohe Verfügbarkeit konfiguriert ist, gibt diese Option den Namen des primären Knotens an.
-BackupNodes -bn	node1 node2 ...	Optional. Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist. Sie können Sicherungsknoten konfigurieren, wenn Sie hohe Verfügbarkeit haben.
-ServiceDisable -sd	-	Optional. Erstellt einen deaktivierten Dienst. Sie müssen den Dienst aktivieren, bevor Sie ihn ausführen können.
-ServiceOptions -so	option_name=value	Erforderlich. Diensteigenschaften, mit denen definiert wird, wie der PowerCenter-Repository-Dienst ausgeführt wird.

Option	Argument	Beschreibung
-LicenseName -ln	license_name	Erforderlich, wenn Sie einen aktivierten Dienst erstellen. Name der Lizenz, die Sie dem PowerCenter-Repository-Dienst zuweisen möchten.
-FolderPath -fp	full_folder_path	Optional. Vollständiger Pfad (ohne Domänenname) des Ordners, in dem Sie den PowerCenter-Repository-Dienst erstellen möchten. Folgendes Format ist erforderlich: */parent_folder/child_folder* Standardwert ist „/“ (die Domäne).

Repository-Dienst-Optionen (-so)

Geben Sie Repository-Dienst-Optionen im folgenden Format ein:

```
infacmd CreateRepositoryService ... -so option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Repository-Dienst-Optionen beschrieben:

Option	Beschreibung
AllowWritesWithRACaching	Optional. Verwendet PowerCenter Client-Tools zum Ändern von Metadaten im Repository, wenn „RepAgent cachen“ aktiviert ist. Standardwert ist „Ja“.
CheckinCommentsRequired	Optional. Beim Einchecken von Repository-Objekten müssen Benutzer Kommentare hinzufügen. Standardwert ist „Ja“. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
CodePage	Erforderlich. Codepage-Beschreibung für die Datenbank. Zur Eingabe einer Codepage, die ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
ConnectString	Erforderlich. Die während der Einrichtung des PowerCenter-Repository-Diensts angegebene Datenbankverbindungszeichenfolge. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
DBPassword	Erforderlich. Repository-Datenbankpasswort für den Datenbankbenutzer. Sie können ein Passwort mit der Option -so oder der Umgebungsvariable INFA_DEFAULT_DATABASE_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -so festgelegte Passwort Vorrang. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
DBPoolExpiryThreshold	Optional. Die Mindestanzahl an inaktiven Datenbankverbindungen, die im PowerCenter-Repository-Dienst zulässig sind. Beispiel: Wenn 20 inaktive Verbindungen vorhanden sind und Sie diesen Schwellenwert auf 5 festlegen, schließt der PowerCenter-Repository-Dienst höchstens 15 Verbindungen. Die Mindestanzahl beträgt 3. Standardwert ist 5.

Option	Beschreibung
DBPoolExpiryTimeout	Optional. Der Zeitraum in Sekunden, in dem der PowerCenter-Repository-Dienst nach inaktiven Datenbankverbindungen sucht. Ist eine Verbindung für einen Zeitraum inaktiv, der diesen Wert überschreitet, kann der PowerCenter-Repository-Dienst die Verbindung schließen. Der Mindestwert beträgt 300. Der Höchstwert beträgt 2.592.000 (30 Tage). Standardwert ist 3.600 (1 Stunde).
DBUser	Erforderlich. Konto für die Datenbank, die das Repository enthält. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
DatabaseArrayOperationSize	Optional. Anzahl der Zeilen, die bei jedem Array-Datenbankvorgang abgerufen werden, beispielsweise Einfügen oder Abrufen. Standardwert ist 100. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
DatabaseConnectionTimeout	Optional. Zeitraum in Sekunden, in dem der PowerCenter-Repository-Dienst versucht, eine Verbindung zum Datenbankverwaltungssystem herzustellen. Standardwert ist 180.
DatabasePoolSize	Optional. Maximale Anzahl der Verbindungen zur Repository-Datenbank, die der PowerCenter-Repository-Dienst herstellen kann. Der Mindestwert beträgt 20. Standardwert ist 500.
DatabaseType	Erforderlich. Typ der Datenbank, die die Repository-Metadaten speichert. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
EnableRepAgentCaching	Optional. Aktiviert die Funktion „Repository Agent Caching“. Standardwert ist „Ja“.
ErrorSeverityLevel	Optional. Mindestebene der Fehlermeldungen, die in das PowerCenter-Repository-Dienstprotokoll geschrieben werden: - Fatal - Fehler Warnung - Info - Trace - Debug Der Standardwert lautet „Info“.
HeartBeatInterval	Optional. Zeitraum, in dem der PowerCenter-Repository-Dienst seine Verbindungen zu den Clients in diesem Dienst überprüft. Standardwert ist 60 Sekunden.
MaxResilienceTimeout	Optional. Maximaler Zeitraum in Sekunden, in dem der Dienst die Ressourcen zwecks Belastbarkeit beibehält. Standardwert ist 180.
MaximumConnections	Optional. Maximale Anzahl der Verbindungen, die das Repository von den Repository-Clients akzeptiert. Standardwert ist 200.
MaximumLocks	Optional. Maximale Anzahl an Sperren, die das Repository für Metadatenobjekte verwendet. Standardwert ist 50.000.
OperatingMode	Optional. Modus, in dem der PowerCenter-Repository-Dienst ausgeführt wird: - Normal - Exklusiv Standardwert ist „Normal“. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.

Option	Beschreibung
OptimizeDatabaseSchema	Optional. Optimiert das Repository-Datenbankschema beim Erstellen von Repository-Inhalten oder Sichern und Wiederherstellen eines IBM DB2- oder Microsoft SQL Server-Repositorys. Bei Aktivierung versucht der PowerCenter-Repository-Dienst Repository-Tabellen zu erstellen, die Varchar-Spalten mit einer Genauigkeit von 2000 anstelle von CLOB-Spalten enthalten. Verwenden Sie Varchar-Spalten, um die Leistung des Repositorys zu steigern. Bei Verwendung von Varchar-Spalten verringern Sie die Festplatteneingabe und -ausgabe und die Datenbank kann die Spalten zwischenspeichern. Um diese Option zu verwenden, überprüfen Sie die Anforderungen an die Seitengröße für die folgenden Repository-Datenbanken: - IBM DB2. Datenbank-Seitengröße 4 KB oder größer. Mindestens einen temporären Tablespace mit einer Seitengröße von mindestens 16 KB. - Microsoft SQL Server. Datenbank-Seitengröße 8 KB oder größer. Standardwert ist „Deaktiviert“.
PreserveMXData	Optional. Behält MX-Daten für frühere Versionen von Zuordnungen bei. Standardwert ist „Deaktiviert“.
RACacheCapacity	Optional. Anzahl der Objekte, die der Cache bei aktiviertem Repository Agent Caching enthalten kann. Standardwert ist 10.000.
SecurityAuditTrail	Optional. Verfolgt Änderungen, die an Benutzern, Gruppen und Berechtigungen vorgenommen wurden. Standardwert ist „Nein“.
ServiceResilienceTimeout	Optional. Zeitraum in Sekunden, in dem der Dienst versucht, eine Verbindung zu einem anderen Dienst herzustellen oder erneut herzustellen. Standardwert ist 180. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
TableOwnerName	Optional. Name des Eigentümers der Repository-Tabellen für ein IBM DB2-Repository.
TablespaceName	Optional. Tablespace-Name für IBM DB2-Repositorys. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
TrustedConnection	Optional. Verwendet Windows-Authentifizierung, um auf die Microsoft SQL Server-Datenbank zuzugreifen. Standardwert ist „Nein“. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.

CreateRole

Erstellt eine benutzerdefinierte Rolle in der Domäne. Anschließend können Sie der Rolle Berechtigungen für die Domäne oder für einen Anwendungsdiensttyp zuweisen. Sie können keine systemdefinierten Rollen erstellen.

Der Befehl „infacmd isp CreateRole“ verwendet die folgende Syntax:

```
CreateRole

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

[<-SecurityDomain|-sdn> securitydomain]
```

```
<-Password|-pd> password

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-RoleName|-rn> role_name

[<-RoleDescription|-rd> role_description]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp CreateRole“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-RoleName -rn	role_name	Erforderlich. Name der Rolle. Der Rollenname unterliegt nicht der Groß-/Kleinschreibung und kann 1 bis 80 Zeichen umfassen. Er darf weder Tabulatoren, Zeilenendzeichen noch folgende Sonderzeichen enthalten: `, + " \ < > ; / * % ?` Der Name kann ein ASCII-Leerzeichen enthalten, jedoch nicht als erstes oder letztes Zeichen. Alle anderen Leerzeichen sind nicht zulässig.
-RoleDescription -rd	role_description	Optional. Rollenbeschreibung. Die Beschreibung kann maximal 1.000 Zeichen umfassen und darf weder Tabulatoren, Zeilenendzeichen noch folgende Sonderzeichen enthalten: `< > "` Um eine Beschreibung einzugeben, die Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie sie in Anführungszeichen.

CreateSAPBWService

Erstellt einen SAP BW-Dienst in der Domäne. Der SAP BW-Dienst wird standardmäßig aktiviert, wenn Sie ihn erstellen.

Der Befehl „infacmd isp CreateSAPBWService“ verwendet die folgende Syntax:

```
CreateSAPBWService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-NodeName|-nn> node_name

<-IntegrationService|-is> integration_service_name

<-RepositoryUser|-ru> user

<-RepositoryPassword|-rp> password
```

```
[<-ServiceOptions|-so> option_name=value ...]

[<-ServiceProcessOptions|-po> option_name=value ...]

[<-ServiceDisable|-sd>]

[<-LicenseName|-ln> license_name]

[<-FolderPath|-fp> full_folder_path]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp CreateSAPBWService“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des SAP BW-Diensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositorys kompatibel sein. Der Name darf maximal 79 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten: `/ * ? < > " |`
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der SAP BW-Dienst-Prozess ausgeführt werden soll. Wenn die PowerCenter-Umgebung für hohe Verfügbarkeit konfiguriert ist, gibt diese Option den Namen des primären Knotens an.
-IntegrationService -is	integration_service_name	Erforderlich. Name des Integrationsdiensts, zu dem der SAP BW-Dienst eine Verbindung herstellt. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

Option	Argument	Beschreibung
-RepositoryUser -ru	user	Erforderlich. Benutzername zum Herstellen einer Verbindung zum Repository. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RepositoryPassword -rp	Passwort	Erforderlich, wenn die sichere Kommunikation nicht für die Domäne aktiviert ist. Optional, wenn die sichere Kommunikation für die Domäne aktiviert ist. Benutzerpasswort. Sie können ein Passwort mit der Option -rp oder der Umgebungsvariable INFA_REPOSITORY_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -rp festgelegte Passwort Vorrang.
-ServiceOptions -so	option_name=value	Optional. Diensteigenschaften, mit denen definiert wird, wie der SAP BW-Dienst ausgeführt wird.
-ServiceProcessOptions -po	option_name=value	Optional. Dienstprozesseigenschaften für den SAP BW-Dienst.
-ServiceDisable -sd	-	Optional. Erstellt einen deaktivierten Dienst. Sie müssen den Dienst aktivieren, bevor Sie ihn ausführen können.
-LicenseName -ln	license_name	Erforderlich, wenn Sie einen aktivierten Dienst erstellen. Name der Lizenz, die Sie dem SAP BW-Dienst zuweisen möchten.
-FolderPath -fp	full_folder_path	Optional. Vollständiger Pfad (ohne Domänenname) des Ordners, in dem Sie den SAP BW-Dienst erstellen möchten. Folgendes Format ist erforderlich: */parent_folder/child_folder* Standardwert ist „/“ (die Domäne).

SAP BW Service-Optionen

Geben Sie SAP BW Service-Optionen im folgenden Format ein:

```
infacmd CreateSAPBWService ... -so option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die SAP BW Service-Optionen beschrieben:

Option	Beschreibung
BWSystemConxString	Optional. In der Datei `sapnwrfc.ini` definierter DEST-Eintrag für eine Verbindung zu einem RFC-Serverprogramm. Bearbeiten Sie diese Eigenschaft, wenn Sie in der Datei `sapnwrfc.ini` einen anderen DEST-Eintrag für den SAP BW-Dienst erstellt haben.
RetryPeriod	Optional. Anzahl der Sekunden, die der SAP BW Service wartet, bevor er eine Verbindung zum BW-System herstellt, wenn ein vorheriger Verbindungsversuch fehlgeschlagen ist. Standardwert ist „5“.

SAP BW Service-Prozessoption

Geben Sie die Dienstprozessoptionen im folgenden Format ein:

```
infacmd CreateSAPBWService ... -po option_name=value
```

Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle wird die SAP BW Service-Option beschrieben:

Option	Beschreibung
ParamFileDir	Optional. Temporäres Verzeichnis für Parameterdateien. Standardverzeichnis ist /Infa_Home/server/infa_shared/BWParam.

CreateUser

Erstellt ein Benutzerkonto in der nativen Sicherheitsdomäne. Anschließend können Sie Rollen und Berechtigungen zu einem Benutzerkonto zuweisen. Die einem Benutzer zugewiesenen Rollen und Berechtigungen legen die Aufgaben fest, die der Benutzer innerhalb der Domäne durchführen kann.

Der Befehl „infacmd isp CreateUser“ verwendet die folgende Syntax:

```
CreateUser

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NewUserName|-nu> new_user_name

<-NewUserPassword|-np> new_user_password

[<-NewUserFullName|-nf> new_user_full_name]

[<-NewUserDescription|-ds> new_user_description]
```

```
[<-NewUserEMailAddress|-em> new_user_email_address]

[<-NewUserPhoneNumber|-pn> new_user_phone_number]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp CreateUser“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NewUserName -nu	new_user_name	Erforderlich. Anmeldename für das Benutzerkonto. Der Anmeldename für ein Benutzerkonto muss innerhalb der Sicherheitsdomäne, zu der er gehört, eindeutig sein. Der Anmeldename unterliegt nicht der Groß-/Kleinschreibung und kann 1 bis 80 Zeichen umfassen. Er darf weder Tabulatoren, Zeilenendzeichen noch folgende Sonderzeichen enthalten: `, + " \ < > ; / * & % ?` Der Name kann ein ASCII-Leerzeichen enthalten, jedoch nicht als erstes oder letztes Zeichen. Alle anderen Leerzeichen sind nicht zulässig.
-NewUserPassword -np	new_user_password	Erforderlich. Passwort für das Benutzerkonto. Sie können ein Passwort mit der Option -np oder der Umgebungsvariable INFA_PASSWORD festlegen. Wenn Sie ein Passwort mit diesen beiden Methoden festlegen, hat das mit der Option -np festgelegte Passwort Vorrang. Das Passwort unterliegt der Groß-/Kleinschreibung und kann 1 bis 80 Zeichen umfassen.
-NewUserFullName -nf	new_user_full_name	Optional. Vollständiger Name für das Benutzerkonto. Um einen Namen einzugeben, der Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen. Der vollständige Name darf folgende Sonderzeichen nicht enthalten: `< > "`
-NewUserDescription -ds	new_user_description	Optional. Beschreibung des Benutzerkontos. Um eine Beschreibung einzugeben, die Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie sie in Anführungszeichen. Die Beschreibung darf die folgenden Sonderzeichen nicht enthalten: `< > "`

Option	Argument	Beschreibung
-NewUserEMailAddress -em	new_user_email_address	Optional. E-Mail-Adresse des Benutzers. Um eine Adresse einzugeben, die Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie sie in Anführungszeichen. Die E-Mail-Adresse darf keines der folgenden Sonderzeichen enthalten: `< > "` Geben Sie die E-Mail-Adresse im Format `UserName@Domain` ein.
-NewUserPhoneNumber -pn	new_user_phone_number	Optional. Telefonnummer des Benutzers. Um eine Telefonnummer einzugeben, die Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie sie in Anführungszeichen. Die Telefonnummer darf keines der folgenden Sonderzeichen enthalten: `< > "`

CreateWSHubService

Erstellt einen Webdienst-Hub in der Domäne. Der Webdienst-Hub wird standardmäßig aktiviert, wenn Sie ihn erstellen.

Der Befehl „infacmd isp CreateWSHubService“ verwendet die folgende Syntax:

```
CreateWSHubService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

[<-FolderPath|-fp> full_folder_path]

<-NodeName|-nn> node_name

<-RepositoryService|-rs> repository_service_name

<-RepositoryUser|-ru> repository_user

<-RepositoryPassword|-rp> repository_password

[<-RepositoryUserSecurityDomain|-rsdn> repository_user_security_domain]

[<-ServiceDisable|-sd>]

[<-ServiceOptions|-so> option_name=value ...
```

```
<-LicenseName|-ln> license_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp CreateWSHubService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Domäne.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Name des Webdienst-Hubs, den Sie erstellen möchten. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositorys kompatibel sein. Der Name darf maximal 79 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten: `/ * ? < > " |`
-FolderPath -fp	full_folder_path	Optional. Vollständiger Pfad (ohne Domänenname) des Ordners, in dem Sie den Webdienst-Hub erstellen möchten. Folgendes Format ist erforderlich: */parent_folder/child_folder* Standardwert ist „/“ (die Domäne).
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Webdienst-Hub-Prozess ausgeführt werden soll.
-RepositoryService -rs	repository_service_ name	Erforderlich. Name des Repository-Diensts, von dem der Webdienst-Hub abhängig ist. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RepositoryUser -ru	repository_user	Erforderlich. Benutzername zum Herstellen einer Verbindung zum Repository. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RepositoryPassword -rp	repository_password	Erforderlich. Benutzerpasswort. Sie können ein Passwort mit der Option -rp oder der Umgebungsvariable INFA_REPOSITORY_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-rp“ festgelegte Passwort Vorrang.
- RepositoryUserSecurity Domain -rsdn	repository_user_securi ty_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung oder Kerberos-Authentifizierung verwendet. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der PowerCenter-Repository-Benutzer gehört. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ServiceDisable -sd	-	Optional. Erstellt einen deaktivierten Dienst. Sie müssen den Dienst aktivieren, bevor Sie ihn ausführen können.

Option	Argument	Beschreibung
-ServiceOptions -so	option_name=value ...	Optional. Diensteigenschaften, mit denen definiert wird, wie der Webdienst-Hub ausgeführt wird.
-LicenseName -ln	license_name	Erforderlich. Name der Lizenz, die Sie dem Webdienst-Hub zuweisen möchten.

Web Services Hub-Optionen

Geben Sie Web Services Hub-Optionen im folgenden Format ein:

```
infacmd CreateWSHubService ... -so option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden Web Services Hub-Optionen beschrieben:

Option	Beschreibung
DTMTimeout	Optional. Zeit in Sekunden, in der *infacmd* ersucht, eine Verbindung zu DTM herzustellen bzw. erneut herzustellen. Default is 60.
ErrorSeverityLevel	Optional. Mindestlevel der Fehlerprotokollierung für die Web Services Hub-Protokolle: - Schwerwiegend - Fehler - Warnung - Info - Trace - Debug Die Standardeinstellung lautet "Info".
HubHostName	Optional. Name des Computers, auf dem der Web Services Hub gehostet wird. Der Standardwert ist "localhost". Um die Änderungen zu übernehmen, starten Sie den Web Services Hub neu.
HubPortNumber(http)	Optional. Portnummer, auf der der Web Services Hub in Tomcat ausgeführt wird. Default is 7333. Um die Änderungen zu übernehmen, starten Sie den Web Services Hub neu.
HubPortNumber (https)	Portnummer, auf der der Web Services Hub in Tomcat ausgeführt wird. Erforderlich, wenn Sie den Web Services Hub unter HTTPS ausführen möchten. Default is 7343.
InternalHostName	Optional. Hostname, mit dem der Web Services Hub Verbindungen vom Integration Service abhört. Der Standardwert ist "localhost". Um die Änderungen zu übernehmen, starten Sie den Web Services Hub neu.
InternalPortNumber	Optional. Portnummer, mit der der Web Services Hub Verbindungen vom Integration Service abhört. Default is 15555. Um die Änderungen zu übernehmen, starten Sie den Web Services Hub neu.

Option	Beschreibung
MaxConcurrentRequests	Optional. Maximale Anzahl an verfügbaren Verarbeitungs-Threads, mit der die maximale Anzahl an gleichzeitigen Anfragen, die verarbeitet werden können, angegeben wird. Default is 100.
MaxLMConnections	Optional. Maximale Anzahl an Verbindungen zum Integration Service, die für den Web Services Hub gleichzeitig offen sein können. Default is 20.
MaxQueueLength	Optional. Maximale Warteschlangenlänge für eingehende Verbindungsanfragen, wenn alle möglichen Threads für die Verarbeitung von Anfragen verwendet werden. Default is 5000.
SessionExpiryPeriod	Optional. Anzahl an Sekunden, die eine Sitzung ungenutzt bleiben kann, bevor ihre Sitzungs-ID ungültig wird. Die Standardeinstellung lautet 3600 Sekunden.
URLScheme	Optional. Das von Ihnen konfigurierte Sicherheitsprotokoll für den Web Services Hub: HTTP oder HTTPS. Standardwert ist HTTP. Um die Änderungen zu übernehmen, starten Sie den Web Services Hub neu.
WSH_ENCODING	Optional. Zeichenkodierung für den Web Services Hub. Standardmäßig wird UTF-16LE verwendet. Um die Änderungen zu übernehmen, starten Sie den Web Services Hub neu.
KeystoreFile	Optional. Schlüsselspeicherdatei, in der die Schlüssel und Zertifikate enthalten sind, die für die Verwendung des SSL-Sicherheitsprotokolls mit dem Web Services Hub erforderlich sind.

DeleteNamespace

Löscht eine LDAP-Sicherheitsdomäne und die Benutzer und Gruppen in der Sicherheitsdomäne. Löscht die LDAP-Sicherheitsdomäne, wenn die Informatica-Domäne LDAP oder die Kerberos-Authentifizierung verwendet.

Der Befehl „infacmd isp DeleteNamespace“ verwendet die folgende Syntax:

```
DeleteNamespace
 <-DomainName|-dn> domain_name
 <-UserName|-un> user_name
 <-Password|-pd> password
 [<-SecurityDomain|-sdn> security_domain]
 [<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
 [<-ResilienceTimeout|-re> timeout_period_in_seconds]
 <-NameSpace|-ns> namespace
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp DeleteNamespace“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Name der Sicherheitsdomäne, die Sie erstellen möchten und zu dem Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Sie können einen Wert für -sdn angeben oder den Standardwert basierend auf dem Authentifizierungsmodus verwenden: - Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Standardwert ist „Native“. Zum Arbeiten mit der LDAP-Authentifizierung müssen Sie den Wert für -sdn angeben. - Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Standardwert ist „Native“ für native Authentifizierung. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn Sie die Umgebungsvariable nicht angeben, wird der Standardwert von 180 Sekunden verwendet.
-NameSpace -ns	namespace	Erforderlich. Name der LDAP- oder Kerberos-Sicherheitsdomäne. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf weder Leerzeichen noch folgende Sonderzeichen enthalten: , + / < > @ ; \ % ? Der Name darf nicht länger als 128 Zeichen sein. Der Name kann ein ASCII-Leerzeichen enthalten, jedoch nicht als erstes oder letztes Zeichen. Sie können keine anderen Leerzeichen verwenden.

DisableNodeResource

Deaktiviert eine Informatica-Ressource. Informatica-Ressourcen beinhalten Datei-Verzeichnisressourcen, benutzerspezifische Ressourcen und Verbindungsressourcen. Deaktivieren Sie die Ressourcen, die nicht verfügbar sind, um zu verhindern, dass der Load Balancer eine Aufgabe an einen Knoten sendet, der nicht über die erforderlichen Ressourcen verfügt.

Sie können Dateiverzeichnisressourcen, benutzerspezifische Ressourcen und Verbindungsressourcen deaktivieren.

Wenn ein PowerCenter-Integrationsdienst in einem Gitter ausgeführt wird, kann der Load Balancer Ressourcen verwenden, um Sitzungs-, Befehls- und vordefinierte Event-Wait-Aufgaben zu verteilen. Wenn der PowerCenter-Integrationsdienst für die Überprüfung von Ressourcen konfiguriert ist, verteilt der Load Balancer Aufgaben an Knoten mit verfügbaren Ressourcen.

Standardmäßig werden alle Verbindungsressourcen auf einem Knoten aktiviert.

Der Befehl „infacmd isp DisableNodeResource“ verwendet die folgende Syntax:

```
DisableNodeResource

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name

[<-ResourceCategory|-rc> resource_category ("PCIS", "DIS")]

<-ResourceType|-rt> resource_type ("Custom", "File Directory", "Connection")
```

```
<-ResourceName|-rn> resource_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp DisableNodeResource“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem die Ressource definiert ist.
-ResourceCategory -rc	resource_category	Optional. Kategorie der Ressource. Gültige Kategorien umfassen: - PCIS. Ressource für den PowerCenter-Integrationsdienst. - DIS. Für zukünftige Verwendung reserviert. Standardwert ist PCIS.
-ResourceType -rt	resource_type	Erforderlich. Typ der Ressource. Gültige Typen umfassen: - Benutzerdefiniert - Dateiverzeichnis - Verbindung
-ResourceName -rn	resource_name	Erforderlich. Vollständiger Name der Ressource. Um die Namen aller für einen Knoten verfügbaren Ressourcen aufzulisten, führen Sie den infacmd isp ListNodeResources-Befehl aus.

DisableService

Deaktiviert den Anwendungsdienst, der dem Dienstnamen entspricht. Wenn Sie einen Dienst deaktivieren, werden alle Dienstprozesse gestoppt.

Deaktiviert jeden Typ von Anwendungsdienst, einschließlich Systemdienste.

Der Befehl „infacmd isp DisableService“ verwendet die folgende Syntax:

```
DisableService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-Mode|-mo> disable_mode
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp DisableService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Diensts, den Sie deaktivieren möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-Mode -mo	disable_mode	Erforderlich. Definiert, wie der Dienst deaktiviert wird: - Abschließen. Deaktiviert den Dienst, nachdem alle Dienstprozesse gestoppt sind. - Stoppen. Stoppt, falls der Dienst ein PowerCenter-Integrationsdienst ist, alle ausgeführten Arbeitsabläufe und deaktiviert dann den PowerCenter-Integrationsdienst. Handelt es sich bei dem Dienst um einen Analyst-Dienst, werden alle Jobs angehalten und der Dienst wird anschließend deaktiviert. - Abbrechen. Stoppt alle Prozesse sofort und deaktiviert dann den Dienst.

Hinweis: Bei Angabe von „Stopp“ als Deaktivierungsmodus für einen Listenerdienst wartet der Befehl bis zu 30 Sekunden, bis die untergeordneten Listener-Aufgaben abgeschlossen werden. Danach werden der Dienst und der Listenerdienst-Prozess heruntergefahren.

DisableServiceProcess

Deaktiviert den Dienstprozess auf einem angegebenen Knoten.

Sie können einen Dienstprozess auf einem angegebenen Knoten deaktivieren, wenn der Knoten verwaltet werden muss.

Der Befehl „infacmd isp DisableServiceProcess“ verwendet die folgende Syntax:

```
DisableServiceProcess

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-NodeName|-nn> node_name

<-Mode|-mo> disable_mode
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp DisableServiceProcess“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des mit dem Prozess verbundenen Diensts, den Sie deaktivieren möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Dienstprozess ausgeführt wird.
-Mode -mo	disable_mode	Erforderlich. Definiert, wie der Dienstprozess deaktiviert wird: - Vollständig. Ermöglicht, dass der Dienstprozess vor der Deaktivierung die aktuellen Aufgaben abschließt. - Stoppen. Handelt es sich bei dem Prozess um einen Integrationsdienst-Prozess, werden alle laufenden Arbeitsabläufe gestoppt und der Integrationsdienst-Prozess wird deaktiviert. - Abbrechen. Deaktiviert den Dienstprozess, bevor die aktuellen Aufgaben abgeschlossen werden.

DisableUser

Deaktiviert ein Benutzerkonto in der Domäne. Wenn ein Benutzer nicht vorübergehend auf die Domäne zugreifen soll, können Sie das Benutzerkonto deaktivieren.

Wenn Sie ein Benutzerkonto deaktivieren, kann der Benutzer sich nicht an den PowerCenter Anwendungen anmelden.

Der Befehl „infacmd isp DisableUser“ verwendet die folgende Syntax:

```
DisableUser

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ExistingUserName|-eu> existing_user_Name

[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp DisableUser“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
ExistingUserName -eu	existing_user_name	Erforderlich. Benutzerkonto, das Sie deaktivieren möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der zu deaktivierende Benutzer gehört. Standardwert ist „Native“.

EditUser

Bearbeitet die allgemeinen Eigenschaften für ein Benutzerkonto in der nativen Sicherheitsdomäne.

Sie können die Eigenschaften von Benutzerkonten in den LDAP-Sicherheitsdomänen nicht ändern.

Sie können den Anmeldenamen eines nativen Benutzers nicht ändern.

Der Befehl „infacmd isp EditUser“ verwendet die folgende Syntax:

```
EditUser

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ExistingUserName|-eu> existing_user_Name

[<-ExistingUserFullName|-ef> Existing_user_full_name]

[<-ExistingUserDescription|-ds> Existing_user_description]

[<-ExistingUserEMailAddress|-em> Existing_user_email_address]

[<-ExistingUserPhoneNumber|-pn> Existing_user_phone_number]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp EditUser“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ExistingUserName -eu	existing_user_name	Erforderlich. Benutzerkonto, das Sie bearbeiten möchten.
-ExistingUserFullName -sf	existing_user_full_name	Optional. Geänderter vollständiger Name für das Benutzerkonto. Um einen Namen einzugeben, der Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen. Der vollständige Name darf folgende Sonderzeichen nicht enthalten: < > "
-ExistingUserDescription -ds	existing_user_description	Optional. Geänderte Beschreibung für das Benutzerkonto. Um eine Beschreibung einzugeben, die Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie sie in Anführungszeichen. Die Beschreibung darf die folgenden Sonderzeichen nicht enthalten: < > "
-ExistingUserEMailAddress -em	existing_user_email_address	Optional. Geänderte E-Mail-Adresse für den Benutzer. Um eine Adresse einzugeben, die Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie sie in Anführungszeichen. Die E-Mail-Adresse darf keines der folgenden Sonderzeichen enthalten: < > "
-ExistingUserPhoneNumber -pn	existing_user_phone_number	Optional. Geänderte Telefonnummer für den Benutzer. Um eine Telefonnummer einzugeben, die Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie sie in Anführungszeichen. Die Telefonnummer darf die folgenden Sonderzeichen nicht enthalten: < > "

EnableNodeResource

Aktiviert eine Informatica-Ressource. Informatica-Ressourcen beinhalten Datei- oder Verzeichnisressourcen, benutzerspezifische Ressourcen und Verbindungsressourcen. Wenn Sie eine Ressource auf einem Knoten aktivieren, kann der Load Balancer Aufgaben verteilen, die die Ressource für diesen Knoten benötigen.

Wenn ein PowerCenter-Integrationsdienst in einem Gitter ausgeführt wird, kann der Load Balancer Ressourcen verwenden, um Sitzungs-, Befehls- und vordefinierte Event-Wait-Aufgaben zu verteilen. Wenn der PowerCenter-Integrationsdienst für die Überprüfung von Ressourcen konfiguriert ist, verteilt der Load Balancer Aufgaben an Knoten, auf denen Ressourcen hinzugefügt und aktiviert werden.

Der Befehl „infacmd isp EnableNodeResource“ verwendet die folgende Syntax:

```
EnableNodeResource

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name

[<-ResourceCategory|-rc> resource_category ("PCIS", "DIS")]

<-ResourceType|-rt> resource_type ("Custom", "File Directory", "Connection")

<-ResourceName|-rn> resource_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp EnableNodeResource“ beschrieben:

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

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem die Ressource definiert ist.
-ResourceCategory -rc	resource_category	Optional. Kategorie der Ressource. Gültige Kategorien umfassen: - PCIS. Ressource für den PowerCenter-Integrationsdienst. - DIS. Für zukünftige Verwendung reserviert. Standardwert ist PCIS.
-ResourceType -rt	resource_type	Erforderlich. Typ der Ressource. Gültige Typen umfassen: - Benutzerdefiniert - Dateiverzeichnis - Verbindung
-ResourceName -rn	resource_name	Erforderlich. Vollständiger Name der Ressource. Um die Namen aller für einen Knoten verfügbaren Ressourcen aufzulisten, führen Sie den ListNodeResources-Befehl aus.

EnableService

Aktiviert den Anwendungsdienst, der dem Dienstnamen entspricht.

Aktiviert jeden Typ von Anwendungsdienst, einschließlich Systemdienste. Sie können auch den Informatica Administrator aktivieren.

Der Befehl „infacmd isp EnableService“ verwendet die folgende Syntax:

```
EnableService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp EnableService“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des Diensts, den Sie aktivieren möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen. Geben Sie zum Starten des Administrator Tools `_adminconsole` ein.

EnableServiceProcess

Aktiviert den Dienstprozess auf einem angegebenen Knoten.

Der Befehl „infacmd isp EnableServiceProcess“ verwendet die folgende Syntax:

```
EnableServiceProcess

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name
```

```
<-NodeName|-nn> node_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp EnableServiceProcess“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des mit dem Prozess verbundenen Diensts, den Sie aktivieren möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem Sie einen Dienstprozess aktivieren möchten.

EnableUser

Aktiviert ein Benutzerkonto in der Domäne.

Der Befehl „infacmd isp EnableUser“ verwendet die folgende Syntax:

```
EnableUser

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ExistingUserName|-eu> existing_user_Name

[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp EnableUser“ beschrieben:

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

Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
ExistingUserName -eu	existing_user_name	Erforderlich. Benutzerkonto, das Sie aktivieren möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der zu aktivierende Benutzer gehört. Standardwert ist „Native“.

ExportDomainObjects

Exportiert native Benutzer, native Gruppen, Rollen und Verbindungen aus der Informatica-Domäne in eine XML-Datei.

Wenn Sie nicht alle Objekte in der Domäne exportieren möchten, verwenden Sie eine infacmd-Exportsteuerdatei zum Filtern der Objekte, die Sie exportieren möchten.

Verwenden Sie die Befehle „ExportDomainObjects“ und „ImportDomainObjects“, um Objekte zwischen zwei unterschiedlichen Domänen derselben Version zu migrieren. Verwenden Sie zum Exportieren nativer Benutzer und Gruppen aus Domänen unterschiedlicher Versionen den infacmd isp ExportUsersAndGroups-Befehl.

Beim Exportieren einer Gruppe werden alle Untergruppen und Benutzer in der Gruppe exportiert.

Sie können den Administrator-Benutzer, die Administratorgruppe, die Benutzer in der Administratorgruppe, die Gruppe „Jeder“ oder die LDAP-Benutzer oder -Gruppen nicht exportieren. Um LDAP-Benutzer und -Gruppen in einer Informatica-Domäne zu replizieren, exportieren Sie die LDAP-Benutzer und -Gruppen direkt aus dem LDAP-Verzeichnisdienst.

Wenn der Befehl mit einem Java-Speicherfehler fehlschlägt, erhöhen Sie den verfügbaren Speicher für „infacmd“. Um den Systemspeicher zu erhöhen, legen Sie den Wert „-Xmx“ in der Umgebungsvariable ICMD_JAVA_OPTS fest.

Der Befehl „infacmd isp ExportDomainObjects“ verwendet die folgende Syntax:

```
ExportDomainObjects
```

```
<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ExportFile|-fp> export_file_name

[<-ExportControlFile|-cp> export_control_file_name]

[<-RetainPassword|-rp> retain_password]

[<-Force|-f>]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ExportDomainObjects“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ExportFile -fp	export_file_name	Erforderlich. Pfad und Dateiname der Exportdatei. Wenn Sie den Dateipfad nicht angeben, erstellt infacmd die Datei in dem Verzeichnis, in dem infacmd ausgeführt wird.
-ExportControlFile -cp	export_control_file	Optional. Name und Pfad der Exportsteuerdatei, die die exportierten Objekte filtert.
-RetainPassword -rp	retain_password	Optional. Legen Sie die Option auf TRUE fest, um verschlüsselte Passwörter für Benutzer und Verbindungen in der exportierten Datei beizubehalten. Wird die Option auf FALSE festgelegt, werden Benutzer- und Verbindungspasswörter als leere Zeichenfolgen exportiert. Standardwert ist „false“.
-Force -f	-	Optional. Überschreibt die Exportdatei, wenn eine Datei mit demselben Namen bereits vorhanden ist. Wenn Sie diese Option auslassen, werden Sie aufgefordert, das Überschreiben der Datei zu bestätigen.

ExportUsersAndGroups

Exportiert native Benutzer und Gruppen in eine XML-Datei.

Wenn der Befehl mit einem Java-Speicherfehler fehlschlägt, erhöhen Sie den verfügbaren Speicher für „infacmd“. Um den Systemspeicher zu erhöhen, legen Sie den Wert „-Xmx“ in der Umgebungsvariable ICMD_JAVA_OPTS fest.

Der Befehl „infacmd isp ExportUsersAndGroups“ verwendet die folgende Syntax:

```
ExportUsersAndGroups

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ExportFile|-ef> export_file_name

[<-Force|-f>]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ExportUsersAndGroups“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ExportFile -ef	export_file_name	Erforderlich. Name und Dateipfad, in den die Exportdatei geschrieben werden soll. Wenn Sie den Dateipfad nicht angeben, erstellt infacmd die Backup-Datei in dem Verzeichnis, in dem infacmd ausgeführt wird.
-Force -f	-	Optional. Überschreibt die Exportdatei, wenn eine Datei mit demselben Namen bereits vorhanden ist. Wenn Sie diese Option auslassen, werden Sie aufgefordert, das Löschen der Datei zu bestätigen.

Verwandte Themen:

- “ImportUsersAndGroups” auf Seite 457

generateHadoopConnectionFromHiveConnection

Generiert eine Hadoop-Verbindung aus einer Hive-Verbindung, die aktiviert wurde, um die Mapping-Logik in den Hadoop-Cluster zu verschieben. Die generierte Hadoop-Verbindung erbt die Berechtigungen der Hive-Verbindung.

Der Befehl „infacmd generateHadoopConnectionFromHiveConnection“ verwendet die folgende Syntax:

```
generateHadoopConnectionFromHiveConnection

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-ConnectionPrefix|-p> connection_prefix, default value is AutoGen_. Not used if the
target connection name is provided.]

[<-SourceConnectionName|-scn> hive_connection_name. If you do not enter the Hive
connection name, the command generates a Hadoop connection from all Hive connections
enabled for pushdown.]

[<-TargetConnectionName|-tcn> hadoop_connection_name. Used if the Hive connection name
is provided.]

[<-ConflictResolution|-cr> The conflict resolution strategy for a connection generation
task performed previously on the source connection(s). Valid options are skip, replace,
or rename.]
```

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

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

Option	Argument	Beschreibung
SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
ConnectionPrefix -p	connection_prefix	Präfix für die generierte Hadoop-Verbindung. Standardwert ist „AutoGen_“. Wird nicht verwendet, wenn der Verbindungsname für das Ziel angegeben ist. Wenn der Verbindungsname für das Ziel nicht angegeben ist, erbt die generierte Hadoop-Verbindung den Namen der Hive-Verbindung, und die Zeichenfolge mit Unterscheidung zwischen Groß-/Kleinschreibung wird von „Hive“ zu „Hadoop“ geändert.
SourceConnectionName -scn	hive_connection_name	Verbindungsname für die Hive-Quelle. Wenn Sie den Namen der Hive-Verbindung nicht eingeben, generiert der Befehl eine Hadoop-Verbindung aus jeder Hive-Verbindung, für die Pushdown aktiviert ist. Wenn Sie den Verbindungsnamen für die Quelle angeben, ohne den Verbindungsnamen für das Ziel anzugeben, wählt der Befehl einen Namen für die Hadoop-Verbindung aus.

Option	Argument	Beschreibung
TargetConnectionName -tcn	hadoop_connection_name	Verbindungsname für das Hive-Ziel. Wird verwendet, wenn der Hive-Verbindungsname angegeben ist. Wenn Sie den Verbindungsnamen für das Ziel eingeben, aber dieser bereits vorhanden ist, schlägt der Befehl mit der Meldung fehl, dass die Verbindung bereits vorhanden ist.
ConflictResolution -cr	n/v	Die Konfliktlösungsstrategie für eine Aufgabe zur Verbindungsgenerierung wurde zuvor auf der Quellverbindung ausgeführt. Ein Konflikt tritt auf, wenn eine früher generierte Hadoop-Verbindung des Zieltyps gefunden wird. Sie können die folgenden Optionen angeben: - Ersetzen. Die früher generierte Hadoop-Verbindung wird ersetzt. - Umbenennen. Generieren Sie eine andere Hadoop-Verbindung aus der Hive-Verbindung, für die Pushdown aktiviert ist. Um einen Namenskonflikt zu vermeiden, wird `index` an den Namen der Hadoop-Verbindung angehängt. - Überspringen. Standardauflösungstyp. Wenn eine Hadoop-Verbindung bereits aus der entsprechenden Hive-Verbindung mit aktiviertem Pushdown generiert wurde, wird die Hadoop-Verbindung nicht erneut generiert.

GetFolderInfo

Ruft Ordnerinformationen ab. Ordnerinformationen enthalten den Pfad, den Namen und die Beschreibung des Ordners.

Um den infacmd isp GetFolderInfo-Befehl auszuführen, müssen Sie über Berechtigungen für den Ordner verfügen.

Der Befehl „infacmd isp GetFolderInfo“ verwendet die folgende Syntax:

```
GetFolderInfo

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-FolderPath|-fp> full_folder_path
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp GetFolderInfo“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-FolderPath -fp	full_folder_path	Erforderlich. Vollständiger Pfad (ohne Domänenname) des Ordners. Folgendes Format ist obligatorisch: */parent_folder/child_folder*

GetLastError

Ruft die neuesten Fehlermeldungen für einen Anwendungsdienst ab, der auf einem Knoten ausgeführt wird.

Die Fehlermeldungen sind Protokollereignisse, die eine Schweregradstufe von *error* oder *fatal* haben. Dieser Befehl gibt keine Fehler zurück, die vor dem letzten Start von Informatica-Diensten aufgetreten sind.

Sie können Fehlermeldungen in eine Datei speichern oder auf dem Bildschirm anzeigen.

Der Befehl „infacmd isp GetLastError“ verwendet die folgende Syntax:

```
GetLastError

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-NodeName|-nn> node_name

[<-Format|-fm> format_TEXT_XML]

[<-MaxEvents|-me> maximum_number_of_error_events]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp GetLastError“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Optional. Name des Diensts, für den Sie Fehlermeldungen abrufen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Dienst ausgeführt wird.
-Format -fm	format	Optional. Format für Fehlermeldungen. Gültige Typen umfassen: - Text - XML Wenn Sie kein Format angeben, zeigt infacmd die Nachrichten im Textformat mit einer Zeilenlänge von 80 Zeichen an.
-MaxEvents -me	maximum_number_of_error_events	Optional. Maximale Anzahl abzurufender Fehlermeldungen. Der Standardwert ist 1. Der Höchstwert lautet „20“.

GetLog

Ruft Log-Ereignisse ab. Sie können Protokollereignisse für eine Domäne oder einen Dienst erhalten. Sie können Log-Ereignisse in eine Datei schreiben oder auf dem Bildschirm anzeigen.

Um Protokollereignisse für eine Domäne abzurufen, müssen Sie über Berechtigungen für die Domäne verfügen. Um Protokollereignisse für einen Dienst abzurufen, müssen Sie über Berechtigungen für den Dienst verfügen.

Der Befehl „infacmd isp GetLog“ verwendet die folgende Syntax:

```
GetLog

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-StartDate|-sd> start_date_time]

[<-EndDate|-ed> end_date_time]

[<-ReverseOrder|-ro>]

[<-Format|-fm> format_TEXT_XML_BIN]

[<-OutputFile|-lo> output_file_name]

[<-ServiceType|-st> service_type AS|BW|CMS|DIS|IS|MM|MRS|RPS|RS|WS|ES|SCH|RMS|DOMAIN|
SEARCH|]

[<-ServiceName|-sn> service_name]
```

```
[<-Severity|-svt> FATAL_ERROR_WARNING_INFO_TRACE_DEBUG]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp GetLog“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-StartDate -sd	start_date_time	Optional. Gibt die Protokollereignisse beginnend mit dem aktuellen Datum und der aktuellen Uhrzeit zurück. Geben Sie Datum und Uhrzeit in einem der folgenden Formate ein: - MM/dd/yyyy_hh:mm:ssa_Z - MM/dd/yyyy_hh:mma_Z - MM/dd/yyyy_hh:mm:ssa - MM/dd/yyyy_hh:mma - jjjj-MM-tt_HH:mm:ss_Z - jjjj-MM-tt_HH:mm_Z - jjjj-MM-tt_HH:mm:ss - jjjj-MM-tt_HH:mm - MM/dd/yyyy hh:mm:ssa Z - MM/dd/yyyy hh:mma Z - MM/dd/yyyy hh:mm:ssa - MM/dd/yyyy hh:mma - jjjj-MM-tt HH:mm:ss_Z - jjjj-MM-tt HH:mm_Z - jjjj-MM-tt HH:mm:ss - jjjj-MM-tt HH:mm - MM/dd/yyyy - jjjj-MM-tt Dabei ist „a“ ein am-/pm-Marker („a“ für a.m. und „p“ für p.m.) und „Z“ ein Zeitzonen-Marker (z. B. „-0800“ oder „GMT“).
-EndDate -ed	end_date_time	Optional. Gibt die Protokollereignisse zurück, die bis zu diesem Datum und dieser Uhrzeit enden. Geben Sie Datum und Uhrzeit im selben Format wie die StartDate-Option ein. Wenn Sie ein Enddatum eingeben, das vor dem Startdatum liegt, gibt GetLog keine Protokollereignisse zurück.
-ReverseOrder -ro	-	Optional. Ruft Protokollereignisse entsprechend dem aktuellen Zeitstempel ab.
-Format -fm	format	Optional. Format für Protokollereignisse. Gültige Typen umfassen: - Text - XML - Bin (binär) Wenn Sie „Binär“ auswählen, müssen Sie einen Dateinamen mithilfe der OutputFile-Option angeben. Wenn Sie kein Format angeben, verwendet infacmd Textformat mit einer Zeilenlänge von 80 Zeichen.

Option	Argument	Beschreibung
-OutputFile -lo	output_file_name	Name und Dateipfad, in den die Protokolldatei geschrieben werden soll. Standardmäßig verwendet der Dienstmanager das Verzeichnis „server\infa_shared\log“ auf dem Master-Gateway-Knoten. Lassen Sie diese Option aus, um die Protokollereignisse auf dem Bildschirm anzuzeigen. Wenn Sie „Binär“ als Ausgabedateityp auswählen, müssen Sie einen Dateinamen mithilfe dieser Option angeben.
-ServiceType -st	service_type	Optional. Typ des Diensts, für den Sie Protokollereignisse abrufen möchten. Sie können einen Diensttyp angeben. Lassen Sie diese Option aus, um Protokollereignisse für alle Diensttypen abzurufen. Zu den Diensttypen gehören: - AS. Analyst-Dienst - BW. SAP BW-Dienst - CMS. Content-Managementdienst - DIS. Datenintegrationsdienst - IS. PowerCenter-Integrationsdienst - MM. Metadata Manager-Dienst - MRS. Modellrepository-Dienst - RPS. Berichterstellungsdienst - RS. PowerCenter-Repository-Dienst - WS. Webdienst-Hub - ES. E-Mail-Dienst - SCH. Scheduler-Dienst - RMS. Ressourcenmanager-Dienst - DOMAIN. Domäne - SEARCH. Suchdienst
-ServiceName -sn	service_name	Optional. Name des Diensts, für den Sie Protokollereignisse abrufen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-Severity -svt	severity_level	Optional. Schweregrad von Meldungen. Schweregradtypen umfassen: - Schwerwiegend - Fehler - Warnung - Info - Ablaufverfolgung - Debug

GetNodeName

Gibt den Namen eines Knotens zurück.

Ruft den Knotennamen aus der nodemeta.xml-Datei auf dem Knoten ab. Sie müssen diesen Befehl auf dem Knoten eingeben, für den Sie den Namen abrufen möchten.

Der infacmd isp GetNodeName-Befehl verwendet die folgende Syntax:

```
GetNodeName
[<-OutputFile|-o>] output_file
```

Wenn Sie den Befehl ohne die Option -o verwenden, druckt der Befehl den Knotennamen in das Befehlsfenster. Wenn Sie die Option -o zum Angeben einer Ausgabedatei verwenden, geben Sie den Dateinamen und den Pfad an. Beispiel:

```
isp\bin\infacmd.bat getNodeName -o c:\node_name.txt
```

Der Befehl erstellt unter dem von Ihnen angegebenen Pfad eine Datei mit der Bezeichnung „node_name.txt“. Er druckt den Knotennamen in die Datei. Falls die Datei vorhanden ist, überschreibt der Befehl sie.

GetServiceOption

Ruft den Wert einer Diensteigenschaft für einen PowerCenter-Integrationsdienst, PowerCenter-Repository-Dienst, SAP BW-Dienst oder Webdienst-Hub ab. Führen Sie für Datenintegrationsdienst- oder Analyst-Dienst-Optionen „infacmd dis“ oder „infacmd“ als ListServiceOptions aus.

Sie können beispielsweise den Repository-Datenbanktyp abrufen.

Der Befehl „infacmd isp GetServiceOption“ verwendet die folgende Syntax:

```
GetServiceOption

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-OptionName|-op> option_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp GetServiceOption“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Diensts, für den Sie einen Wert abrufen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-OptionName -op	option_name	Erforderlich. Name der Option, für die Sie einen Wert abrufen möchten. Die angegebenen Optionen richten sich nach dem Diensttyp: - Weitere Informationen zu den Optionen des Integrationsdiensts finden Sie unter "Integrationsdienst-Optionen" auf Seite 364. - Für einen SAP BW-Dienst geben Sie „BWSystemConXString" (den R-Typ für SAP-Ziel) oder „RetryPeriod" (den Wiederholungszeitraum in Sekunden) ein. - Weitere Informationen zu den Optionen des Webdienst-Hubs finden Sie unter "Web Services Hub-Optionen" auf Seite 397.

GetServiceProcessOption

Ruft den Wert für eine Eigenschaft auf einem PowerCenter-Integrationsdienst-Prozess ab, der auf einem Knoten ausgeführt wird.

Der Befehl „infacmd isp GetServiceProcessOption" verwendet die folgende Syntax:

```
GetServiceProcessOption

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-NodeName|-nn> node_name

<-OptionName|-op> option_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp GetServiceProcessOption“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Diensts, für den Sie einen Wert abrufen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Dienstprozess ausgeführt wird.
-OptionName -op	option_name	Erforderlich. Name der Option, für die Sie einen Wert abrufen möchten.

Verwandte Themen:

- "Integration Service-Prozessoptionen" auf Seite 369

GetServiceProcessStatus

Ruft den Status eines Anwendungsdienstprozesses auf einem Knoten ab. Ein Dienstprozess kann aktiviert oder deaktiviert werden.

Der Befehl „infacmd isp GetServiceProcessStatus" verwendet die folgende Syntax:

```
GetServiceProcessStatus

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-NodeName|-nn> node_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp GetServiceProcessStatus“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Diensts, der den Prozess ausführt, für den Sie den Status abrufen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Dienstprozess ausgeführt wird.

GetServiceStatus

Ruft den Status eines Anwendungsdiensts ab.

Sie können den Status eines Dienst abrufen, z. B. des Repository-Diensts, des Datenintegrationsdiensts, des Analyst-Diensts, des Integrationsdiensts, des Webdienst-Hub oder des SAP BW-Diensts. Ein Dienst kann aktiviert oder deaktiviert werden.

Der Befehl „infacmd isp GetServiceStatus“ verwendet die folgende Syntax:

```
GetServiceStatus

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp GetServiceStatus“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des Diensts, für den Sie den Status abrufen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

GetSessionLog

Ruft Log-Ereignisse für eine Sitzung ab, die zuletzt ausgeführt wurde. Der PowerCenter-Repository-Dienst muss bei Ausführung dieses Befehls ausgeführt werden.

Der Befehl „infacmd isp GetSessionLog“ verwendet die folgende Syntax:

```
GetSessionLog

<-DomainName|-dn> domain_name

[<-UserName|-un> user_name]

[<-Password|-pd> password]

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-Format|-fm> format_TEXT_XML_BIN]

[<-OutputFile|-lo> output_file_name]

<-IntegrationService|-is> integration_service_name

<-RepositoryService|-rs> repository_service_name

[<-RepositoryDomain|-rd> domain_of_repository]

<-RepositoryUser|-ru> repository_user]

<-RepositoryPassword|-rp> repository_password]

[<-RepositoryUserSecurityDomain|-rsdn> repository_user_security_domain]

<-FolderName|-fn> repository_folder_name

<-Workflow|-wf> workflow_name

[<-RunInstance|-in> run_instance_name] | <-RunId|-id> workflow_run_id]

<-Session|-ss> session_name
```

Hinweis: Wenn Sie die Optionen -un, -pd und -sdn nicht festlegen, verwendet der infacmd isp GetSessionLog-Befehl die entsprechenden Werte aus den Optionen -ru, -rp und -rsdn options.

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp GetSessionLog“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
–UserName –un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, gilt der während der Installation festgelegte Benutzerbereich als Standardeinstellung.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-Format -fm	format	Optional. Format für das Sitzungsprotokoll. Gültige Typen umfassen: - Text - XML - Bin (binär) Wenn Sie „Binär“ auswählen, müssen Sie einen Dateinamen mithilfe der OutputFile-Option angeben. Wenn Sie kein Format angeben, verwendet *infacmd* Textformat mit einer Zeilenlänge von 80 Zeichen.
-OutputFile -lo	output_file_name	Name und Dateipfad für die Sitzungsprotokolldatei. Standardmäßig verwendet der Dienstmanager das Verzeichnis „server\infa_shared\log“ auf dem Master-Gateway-Knoten. Lassen Sie diese Option aus, um die Protokollereignisse auf dem Bildschirm anzuzeigen. Wenn Sie „Binär“ als Ausgabedateityp auswählen, müssen Sie einen Dateinamen mithilfe dieser Option angeben.
-IntegrationService -is	integration_service_name	Erforderlich. Name des Integrationsdiensts, der die Sitzung ausführt. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RepositoryService -rs	repository_service_name	Erforderlich. Name des Repository-Diensts, der die Sitzung enthält. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RepositoryDomain -rd	domain_of_repository	Erforderlich, wenn das Repository sich in einer anderen als der lokalen Domäne befindet. Domäne des Repository-Diensts. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RepositoryUser -ru	repository_user	Erforderlich für native und LDAP-Authentifizierung. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zum Repository. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

Option	Argument	Beschreibung
-RepositoryPassword -rp	repository_password	Erforderlich für native und LDAP-Authentifizierung. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Benutzerpasswort. Sie können ein Passwort mit der Option -rp oder der Umgebungsvariable INFA_REPOSITORY_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -rp festgelegte Passwort Vorrang.
-RepositoryUserSecurity Domain -rsdn	repository_user_security _domain	Erforderlich für LDAP- oder Kerberos-Authentifizierung. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der PowerCenter-Repository-Benutzer gehört. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn Sie diese Option nicht angeben, setzt der Befehl die Sicherheitsdomäne des Repository-Benutzers auf nativ.
-FolderName -fn	repository_folder_name	Erforderlich. Name des Ordners, der die Sitzung enthält. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-Workflow -wf	workflow_name	Erforderlich. Name des Arbeitsablaufs, der die Sitzung enthält. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RunInstance -in	run_instance_name	Name der Arbeitsablaufausführungsinstanz, die die Sitzung enthält. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen. Verwenden Sie die Option -in oder die Option -id, jedoch nicht beide.
-RunId -id	workflow_run_id	Führen Sie die ID-Nummer (Ausführungs-ID) der Arbeitsablaufausführungsinstanz aus, die die Sitzung enthält. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen. Verwenden Sie die Option -in oder die Option -id, jedoch nicht beide. **Hinweis:** Verwenden Sie diese Option, wenn der Arbeitsablauf keinen eindeutigen Ausführungsinstanznamen aufweist.
-Session -ss	session_name	Erforderlich. Sitzungsname. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

GetSystemLogDirectory

Gibt den Pfad des Systemprotokollverzeichnisses zurück.

Geben Sie diesen Befehl in der Domäne ein, deren Verzeichnispfad für Systemprotokolle abgerufen werden soll.

Der infacmd isp GetSystemLogDirectory-Befehl verwendet die folgende Syntax:

```
GetSystemLogDirectory
[<-OutputFile|-o> output_file]
```

Wenn Sie den Befehl ohne die Option -o verwenden, zeigt der Befehl den Verzeichnispfad im Befehlsfenster an. Wenn Sie die Option -o zum Angeben einer Ausgabedatei verwenden, stellen Sie den Dateinamen und den Pfad für die Ausgabedatei bereit. Beispiel:

```
isp\bin\infacmd.bat getSystemLogDirectory -o c:\sys_log_dir.txt
```

Der Befehl erstellt die Datei „sys_log_dir.txt“ im angegebenen Pfad und zeigt den Pfad des Systemprotokollverzeichnisses in der Datei an. Wenn die Datei vorhanden ist, wird sie vom Befehl überschrieben.

getUserActivityLog

Ruft Benutzeraktivitätsprotokolle für einen einzelnen oder mehrere Benutzer ab. Sie können Benutzeraktivitätsprotokolle in eine Datei schreiben oder in der Konsole anzeigen.

Der Befehl „infacmd isp getUserActivityLog“ verwendet die folgende Syntax:

```
getUserActivityLog

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-Users|-usrs> user1:[securitydomain] user2:[securitydomain]...

[<-StartDate|-sd> start_date]

[<-EndDate|-ed> end_date]

[<-ActivityCode|-ac> activity_code]

[<-ActivityText|-atxt> activity_text]

[<-ReverseOrder|-ro> true]

[<-OutputFile|-lo> output_file_name]

[<-Format|-fm> output_format_BIN_TEXT_XML]
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp getUserActivityLog“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung

-Users
-usrs
	user1:[securitydomain] user2:[securitydomain]
	...
		Optional. Die Liste der Benutzer, für die Sie Protokollereignisse erhalten möchten. Trennen Sie mehrere Benutzer mit einem Leerzeichen. Verwenden Sie das Platzhaltersymbol (*), um Protokolle für mehrere Benutzer in einer einzelnen Sicherheitsdomäne oder in allen Sicherheitsdomänen anzuzeigen. Beispiel: Die folgenden Zeichenfolgen sind gültige Werte für diese Option:
		`user:Native`
		`"user:*"`
		`"user*"`
		`"*_users_*"`
		`"*:Native"`
		Wenn Sie das Platzhaltersymbol verwenden, setzen Sie das Argument in Anführungszeichen.
		Wenn Sie keinen Benutzer eingeben, ruft der Befehl die Protokollereignisse für alle Benutzer ab.

-StartDate -sd	start_date	Optional. Gibt die Protokollereignisse beginnend mit dem Datum und der Uhrzeit zurück, die Sie angegeben haben. Geben Sie das Datum und die Uhrzeit in einem der folgenden Formate ein: - MM/tt/jjjj - MM/tt/jjjj HH:mm:ss - jjjj-MM-tt - jjjj-MM-tt HH:mm:ss
-EndDate -ed	end_date	Optional. Gibt die Protokollereignisse zurück, die bis zu diesem Datum und dieser Uhrzeit enden. Geben Sie Datum und Uhrzeit im selben Format wie die Option „Startdatum“ ein. Wenn Sie ein Enddatum eingeben, das vor dem Startdatum liegt, gibt der Befehl keine Protokollereignisse zurück.
-ActivityCode -ac	activity_code	Optional. Gibt Protokollereignisse auf Basis des Aktivitätscodes zurück. Verwenden Sie das Platzhaltersymbol (*), um Protokollereignisse für mehrere Aktivitätscodes abzurufen. Gültige Aktivitätscodes: - CCM_10437. Gibt an, dass eine Aktivität erfolgreich war. - CCM_10438. Gibt an, dass eine Aktivität fehlgeschlagen ist.

Option	Argument	Beschreibung
-ActivityText -atxt	activity_text	Optional. Gibt die Protokollereignisse auf Basis einer im Aktivitätstext gefundenen Zeichenfolge zurück. Verwenden Sie das Platzhaltersymbol (*), um Protokolle für mehrere Ereignisse abzurufen. Beispiel: Der folgende Parameter gibt alle Protokollereignisse zurück, die „Dienst wird aktiviert“ in ihrer Beschreibung enthalten: `"*Enabling service*"` Wenn Sie das Platzhaltersymbol verwenden, setzen Sie das Argument in Anführungszeichen.
-ReverseOrder -ro	Wahr	Optional. Druckt Protokollereignisse in umgekehrter chronologischer Reihenfolge. Wenn Sie diesen Parameter nicht angeben, zeigt der Befehl Protokollereignisse in chronologischer Reihenfolge an.
-OutputFile -lo	output_file_name	Optional. Name der Ausgabedatei. Wenn Sie diesen Parameter nicht angeben, zeigt der Befehl das Protokoll in der Befehlszeile an.
-Format -fm	output_format_BIN_TEXT_XML	Optional. Format der Protokollausgabedatei. Gültige Formate umfassen: - Bin (binär) - Text - XML Das Standardformat lautet „Text“. Wenn Sie das Format auf „Binär“ festlegen, müssen Sie einen Dateinamen mit der -OutputFile-Option angeben.

GetWorkflowLog

Ruft Log-Ereignisse für einen Arbeitsablauf ab, der zuletzt ausgeführt wurde. Der PowerCenter-Repository-Dienst muss bei Ausführung dieses Befehls ausgeführt werden.

Der Befehl „infacmd isp GetWorkflowLog“ verwendet die folgende Syntax:

```
GetWorkflowLog

<-DomainName|-dn> domain_name

[<-UserName|-un> user_name]

[<-Password|-pd> password]

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

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

```
[<-Format|-fm> format_TEXT_XML_BIN]

[<-OutputFile|-lo> output_file_name]

<-IntegrationService|-is> integration_service_name

<-RepositoryService|-rs> repository_service_name

[<-RepositoryDomain|-rd> domain_of_repository]

<-RepositoryUser|-ru> repository_user

<-RepositoryPassword|-rp> repository_password

[<-RepositoryUserSecurityDomain|-rsdn> repository_user_security_domain]

<-FolderName|-fn> repository_folder_name

<-Workflow|-wf> workflow_name

[<-RunInstance|-in> run_instance_name] | <-RunId|-id> workflow_run_id]
```

Hinweis: Wenn Sie die Optionen „-un“, „-pd“ und „-sdn“ nicht festlegen, verwendet der Befehl „infacmd isp GetWorkflowLog“ die entsprechenden Werte aus den Optionen „-ru“, „-rp“ und „-rsdn“.

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp GetWorkflowLog“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, gilt der während der Installation festgelegte Benutzerbereich als Standardeinstellung.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-Format -fm	format	Optional. Format für das Sitzungsprotokoll. Gültige Typen umfassen: - Text - XML - Bin (binär) Wenn Sie „Binär“ auswählen, müssen Sie einen Dateinamen mithilfe der OutputFile-Option angeben. Wenn Sie kein Format angeben, verwendet *infacmd* Textformat mit einer Zeilenlänge von 80 Zeichen.
-OutputFile -lo	output_file_name	Name und Dateipfad für die Arbeitsablaufprotokolldatei. Standardmäßig verwendet der Dienstmanager das Verzeichnis „server\infa_shared\log“ auf dem Master-Gateway-Knoten. Lassen Sie diese Option aus, um die Protokollereignisse auf dem Bildschirm anzuzeigen. Wenn Sie „Binär“ als Ausgabedateityp auswählen, müssen Sie einen Dateinamen mithilfe dieser Option angeben.
-IntegrationService -is	integration_service_name	Erforderlich. Name des Integrationsdiensts, der den Arbeitsablauf ausführt. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RepositoryService -rs	repository_service_name	Erforderlich. Name des Repository-Diensts, der den Arbeitsablauf enthält. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

Option	Argument	Beschreibung
-RepositoryDomain -rd	domain_of_repository	Erforderlich, wenn das Repository sich in einer anderen als der lokalen Domäne befindet. Domäne des Repository-Diensts. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RepositoryUser -ru	user	Erforderlich für native und LDAP-Authentifizierung. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zum Repository. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RepositoryPassword -rp	Passwort	Erforderlich für native und LDAP-Authentifizierung. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Benutzerpasswort. Sie können ein Passwort mit der Option -rp oder der Umgebungsvariable INFA_REPOSITORY_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -rp festgelegte Passwort Vorrang.
-RepositoryUserSecurity Domain -rsdn	repository_user_security _domain	Erforderlich für LDAP- oder Kerberos-Authentifizierung. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der PowerCenter-Repository-Benutzer gehört. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn Sie diese Option nicht angeben, setzt der Befehl die Sicherheitsdomäne des Repository-Benutzers auf nativ.
-FolderName -fn	repository_folder_name	Erforderlich. Name des Ordners, der den Arbeitsablauf enthält. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-Workflow -wf	workflow_name	Erforderlich. Name des Arbeitsablaufs. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RunInstance -in	run_instance_name	Name der Arbeitsablaufausführungsinstanz Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen. Verwenden Sie die Option -in oder die Option -id, jedoch nicht beide.
-RunId -id	workflow_run_id	Führen Sie die ID-Nummer (Ausführungs-ID) der Arbeitsablaufausführungsinstanz aus. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen. Verwenden Sie die Option -in oder die Option -id, jedoch nicht beide. **Hinweis:** Verwenden Sie diese Option, wenn der Arbeitsablauf keinen eindeutigen Ausführungsinstanznamen aufweist.

Hilfe

Zeigt die Optionen und Argumente für einen infacmd-Befehl an.

Wenn Sie den Befehlsnamen auslassen, listet infacmd alle Befehle auf.

Der infacmd Help-Befehl verwendet die folgende Syntax:

```
Help <-plugin_ID> [command]
```

Wenn Sie beispielsweise `infacmd isp Help GetServiceStatus` eingeben, gibt infacmd die folgenden Optionen und Argumente für den infacmd isp GetServiceStatus-Befehl zurück:

```
GetServiceStatus
<-DomainName|-dn> domain_name <-UserName|-un> user_name <-Password|-pd> password [<-
Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds] <-ServiceName|-sn> service_name
```

Wenn Sie beispielsweise `infacmd isp Help UpdateGatewayInfo` eingeben, gibt infacmd die folgenden Optionen und Argumente für den infacmd isp UpdateGatewayInfo-Befehl zurück:

```
UpdateGatewayInfo

<-DomainName|-dn> domain_name

<-GatewayAddress|-dg> domain_gateway_host:port
```

In der folgenden Tabelle werden die infacmd Help-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-	plugin_ID	Optional. Beschreibt, für welches infacmd-Programm Hilfe angezeigt werden soll. Standardwert ist isp.
-	befehl	Optional. Name des Befehls. Wenn Sie den Befehlsnamen auslassen, listet infacmd alle Befehle auf.

ImportDomainObjects

Importiert native Benutzer, native Gruppen, Rollen und Verbindungen aus einer XML-Datei in eine Informatica-Domäne.

Wenn Sie nicht alle Objekte in der Datei importieren möchten, verwenden Sie eine infacmd-Importsteuerdatei zum Filtern der Objekte, die Sie importieren möchten.

Verwenden Sie die Befehle „ExportDomainObjects“ und „ImportDomainObjects“, um Objekte zwischen zwei unterschiedlichen Domänen derselben Version zu migrieren. Verwenden Sie zum Importieren nativer Benutzer und Gruppen aus Domänen unterschiedlicher Versionen den infacmd isp ImportUsersAndGroups-Befehl.

Beim Importieren einer Gruppe werden alle Untergruppen und Benutzer in der Gruppe importiert.

Wenn der Befehl mit einem Java-Speicherfehler fehlschlägt, erhöhen Sie den verfügbaren Speicher für „infacmd“. Um den Systemspeicher zu erhöhen, legen Sie den Wert „-Xmx“ in der Umgebungsvariable ICMD_JAVA_OPTS fest.

Der Befehl „infacmd isp ImportDomainObjects“ verwendet die folgende Syntax:

```
ImportDomainObjects

<-DomainName|-dn> domain_name
```

```
<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ImportFilePath|-fp> import_file_path

[<-ImportControlFile|-cp> import_control_file]

[<-ConflictResolution|-cr> resolution_type]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ImportDomainObjects“ beschrieben:

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

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänenname n mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE _TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ImportFilePath -fp	import_file_path	Erforderlich. Pfad und Dateiname der XML-Datei, aus der Sie die Objekte importieren.
-ImportControlFile -cp	import_control_file	Optional. Pfad und Dateiname der Importsteuerungsdatei, die die zu importierenden Objekte filtert.
-ConflictResolution -cr	resolution_type	Optional. Konfliktlösungsstrategie. Sie können eine der folgenden Optionen angeben: - umbenennen - ersetzen - erneut verwenden Die Option wird ignoriert, wenn Sie eine Konfliktlösungsstrategie in der Importsteuerdatei angeben. Wenn Sie keine Konfliktlösungsstrategie definieren und ein Konflikt auftritt, schlägt der Import fehl.

ImportUsersAndGroups

Importiert native Benutzer und Gruppen in die Domäne.

Führen Sie „infacmd isp ImportUsersAndGroups“ aus, um Benutzer und Gruppen aus einer XML-Datei zu importieren.

Wenn der Befehl mit einem Java-Speicherfehler fehlschlägt, erhöhen Sie den verfügbaren Speicher für „infacmd“. Um den Systemspeicher zu erhöhen, legen Sie den Wert „-Xmx“ in der Umgebungsvariable ICMD_JAVA_OPTS fest.

Der Befehl „infacmd isp ImportUsersAndGroups“ verwendet die folgende Syntax:

```
ImportUsersAndGroups

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ExportFile|-ef> export_file_name

[<-ReuseDomainUsersAndGroups|-rd> If there is a conflict use the users and groups
defined in the target domain]

[<-exportedFromPowercenter|-epc> The export file containing users and groups has been
exported from an Informatica PowerCenter 8.6.1 domain]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ImportUsersAndGroups“ beschrieben:

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

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ExportFile -ef	export_file_name	Erforderlich. Name und Dateipfad der Exportdatei, die Informationen über die Benutzer und Gruppen enthält.
-ReuseDomainUsersAndGroups -rd	-	Optional. Wenn ein Namenskonflikt besteht, behält infacmd die in der Zieldomäne definierten Benutzer und Gruppen bei. Der Befehl schlägt standardmäßig fehl, wenn ein Konflikt auftritt.
-exportedFromPowercenter -epc	-	Erforderlich, wenn die Exportdatei aus einer PowerCenter-Domäne der Version 8.6.1 exportiert wurde.

Verwandte Themen:

- "ExportUsersAndGroups" auf Seite 421

ListAlertUsers

Listet Benutzer auf, die Alarme abonnieren.

Der Befehl „infacmd isp ListAlertUsers" verwendet die folgende Syntax:

```
ListAlertUsers

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListAlertUsers" beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

ListAllGroups

Listet alle Gruppen in der nativen Sicherheitsdomäne auf.

Der Befehl „infacmd isp ListAllGroups“ verwendet die folgende Syntax:

```
ListAllGroups

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListAllGroups“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

ListAllRoles

Listet alle Rollen in der Domäne auf.

Der Befehl „infacmd isp ListAllRoles“ verwendet die folgende Syntax:

```
ListAllRoles

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListAllRoles“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

ListAllUsers

Listet alle Benutzerkonten in der Domäne auf.

Der Befehl „infacmd isp ListAllUsers“ verwendet die folgende Syntax:

```
ListAllUsers

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListAllUsers“ beschrieben:

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

Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

ListConnectionPermissions

Listet alle Berechtigungen auf, die ein Benutzer oder eine Gruppe für die Verbindung besitzen.

Der Befehl „infacmd isp ListConnectionPermissions“ verwendet die folgende Syntax:

```
ListConnectionPermissions

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<<-RecipientUserName|-run> recipient_user_name|<RecipientGroupName|-rgn>
recipient_group_name>

<-RecipientSecurityDomain|-rsd> recipient_security_domain]

<-ConnectionName|-cn> connection_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListConnectionPermissions“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-RecipientUserName -run	recipient_user_name	Erforderlich, wenn Sie den Gruppennamen des Empfängers nicht angeben. Name des Benutzers, für den Berechtigungen aufgelistet werden.
-RecipientGroupName -rgn	recipient_group_name	Erforderlich, wenn Sie den Benutzernamen des Empfängers nicht angeben. Name der Gruppe, für die Berechtigungen aufgelistet werden.
-RecipientSecurityDomain -rsd	recipient_security_domain_name	Erforderlich, wenn der Empfänger zu einer LDAP-Sicherheitsdomäne gehört. Name der Sicherheitsdomäne, zu der der Empfänger gehört. Standardwert ist „Native“.
-ConnectionName -cn	connection_name_security_domain	Erforderlich. Name der Verbindung.

ListConnectionPermissionsByGroup

Listet alle Gruppen mit Verbindungsberechtigungen sowie den jeweiligen Verbindungstyp auf.

Der Befehl „infacmd isp ListConnectionPermissionsByGroup“ verwendet die folgende Syntax:

```
ListConnectionPermissionsByGroup

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ConnectionName|-cn> connection_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListConnectionPermissionsByGroup“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ConnectionName -cn	connection_name_security_domain	Erforderlich. Name der Verbindung.

ListConnectionPermissionsByUser

Listet alle Benutzer mit Verbindungsberechtigungen sowie den jeweiligen Verbindungstyp auf.

Der Befehl „infacmd isp ListConnectionPermissionsByUser“ verwendet die folgende Syntax:

```
ListConnectionPermissionsByUser

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ConnectionName|-cn> connection_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListConnectionPermissionsByUser“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ConnectionName -cn	connection_name_security_domain	Erforderlich. Name der Verbindung.

ListConnections

Listet jeden Verbindungstyp und die Verbindungsobjektnamen für jeden Verbindungstyp auf. Listet alle gültigen Verbindungstypen auf.

Der Befehl „infacmd isp ListConnections“ verwendet die folgende Syntax:

```
ListConnections

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListConnections“ beschrieben:

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

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

ListConnectionOptions

Listet Optionen für eine Verbindung auf. Führen Sie diesen Befehl aus, um verfügbare Optionen anzuzeigen, die beim Update einer Verbindung konfiguriert werden können.

Der Befehl „infacmd isp ListConnectionOptions“ verwendet die folgende Syntax:

```
ListConnectionOptions

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ConnectionName|-cn> connection_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListConnectionOptions“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ConnectionName -cn	connection_name_security_domain	Erforderlich. Name der Verbindung.

ListDefaultOSProfiles

Listet die Standardbetriebssystemprofile für den angegebenen Benutzer bzw. die angegebene Gruppe auf.

Der Befehl „infacmd isp ListDefaultOSProfiles“ verwendet die folgende Syntax:

```
ListDefaultOSProfiles

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-RecipientName|-nm> recipient_name]

[<-RecipientSecurityDomain|-ns> security_domain_of_recipient]

[<-RecipientType|-ty> recipient_type]

[<-IndirectInheritance|-in> indirect_inheritance]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListDefaultOSProfiles“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-RecipientName -nm	recipient_name	Optional. Benutzer- oder Gruppenname, der dem Standardbetriebssystemprofil zugewiesen wird.
-RecipientSecurityDomain -ns	security_domain_of_recipient	Optional. Name der Sicherheitsdomäne, zu der der Benutzer gehört, wenn Sie LDAP-Authentifizierung verwenden.
-RecipientType -ty	recipient_type	Optional. Geben Sie an, ob der Empfänger ein Benutzer oder eine Gruppe ist. Geben Sie einen der folgenden Werte ein: - UserIdentity - GroupIdentity
-IndirectInheritance -in	indirect_inheritance	Optional. Geben Sie einen der folgenden Werte ein: - True. Listet die Betriebssystemprofile auf, die von den Benutzern bzw. Gruppen übernommen wurden. - false. Listet die Betriebssystemprofile auf, die den Benutzern bzw. Gruppen direkt zugewiesen werden.

ListDomainLinks

Listet die Domänen auf, mit der die lokale Domäne verknüpft werden kann. Sie stellen Links zwischen zwei Domänen her, wenn Sie Repository-Metadaten zwischen diesen Domänen austauschen möchten.

Der Befehl „infacmd isp ListDomainLinks“ verwendet die folgende Syntax:

```
ListDomainLinks

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListDomainLinks“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der lokalen Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeitraum in Sekunden, in dem infacmd versucht, eine Verbindung zur lokalen Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

ListDomainOptions

Listet allgemeine Eigenschaften der Domäne auf. Die Eigenschaften beinhalten Resistenz-Timeout, Grenzwert für Resistenz-Timouts, maximale Neustartversuche, Neustartzeitraum, SSL-Modus und Sendemodus.

Um den infacmd isp ListDomainOptions-Befehl auszuführen, müssen Sie über Berechtigungen für die Domäne verfügen.

Der Befehl „infacmd isp ListDomainOptions“ verwendet die folgende Syntax:

```
ListDomainOptions

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListDomainOptions“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

ListFolders

Listet die Ordner in der Domäne auf.

Der Befehl „infacmd isp ListFolders“ verwendet die folgende Syntax:

```
ListFolders

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListFolders“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

ListGridNodes

Listet die einem Gitter zugewiesenen Knoten auf.

Um den infacmd isp ListGridNodes-Befehl auszuführen, müssen Sie über Berechtigungen für das Gitter verfügen.

Der Befehl „infacmd isp ListGridNodes“ verwendet die folgende Syntax:

```
ListGridNodes

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-GridName|-gn> grid_name
```

In der folgenden Tabelle werden *infacmd isp* ListGridNodes“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-GridName -gn	grid_name	Erforderlich. Name des Gitters.

ListGroupPermissions

Listet Gruppenberechtigungen für ein Objekt auf.

Der Befehl „infacmd isp ListGroupPermissions“ verwendet die folgende Syntax:

```
ListGroupPermissions

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ExistingGroup|-eg> existing_group_name

[<-ExistingGroupSecurityDomain|-egn> existing_group_security_domain]

[<-ObjectType|-ot> object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListGroupPermissions“ beschrieben:

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

Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Gateway-Konnektivitätsinformationen in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ExistingGroup -eg	existing_group_name	Erforderlich. Name der Gruppe, der Sie eine Berechtigung für ein Objekt zuweisen möchten.
-ExistingGroupSecurityDomain -egn	existing_group_security_domainth_name	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der die Gruppe gehört, der Sie eine Berechtigung zuweisen möchten. Standardwert ist „Native“.
-ObjectType -ot	object_type	Erforderlich. Typ des Objekts, das Sie auflisten möchten: - Dienst - License - Knoten - Gitter - Folder - OSProfile

ListGroupPrivileges

Listet Berechtigungen auf, die einer Gruppe in der Domäne zugewiesen sind. Sie können ebenfalls Gruppenberechtigungen für jeden Anwendungsdienst in der Domäne zuweisen.

Der Befehl „infacmd isp ListGroupPrivileges“ verwendet die folgende Syntax:

```
ListGroupPrivileges

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-GroupName|-gn> group_name
```

```
[<-GroupSecurityDomain|-gsf> group_security_domain]

<-ServiceName|-sn> service_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListGroupPrivileges“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-GroupName -gn	group_name	Erforderlich. Name der Gruppe, für die Sie Berechtigungen auflisten möchten.
-GroupSecurityDomain -gsf	group_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der die Gruppe gehört, für die Sie Berechtigungen auflisten möchten. Standardwert ist „Native“.
-ServiceName -sn	service_name	Erforderlich. Domäne oder Anwendungsdienstname, für die bzw. den Sie Berechtigungen anzeigen möchten.

ListGroupsForUser

Listet die nativen Gruppen auf, zu denen der Benutzer zugewiesen ist.

Der infacmd isp-Befehl ListGroupsForUser verwendet folgende Syntax:

```
ListGroupsForUser

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ExistingUserName|-eu> existing_user_Name

[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListGroupsForUser“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ExistingUserName -eu	existing_user_Name	Erforderlich. Name des Benutzers, für den Sie Gruppen auflisten möchten.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Standardwert ist „Native“.

ListLDAPConnectivity

Listet die Verbindungsinformationen für einen LDAP-Server auf.

Der Befehl „infacmd isp ListLDAPConnectivity“ verwendet die folgende Syntax:

```
ListLDAPConnectivity

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListLDAPConnectivity“ beschrieben:

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

Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

ListLicenses

Listet die Lizenzen in der Domäne auf. Sie können den Lizenznamen und die Seriennummer für jede Lizenz anzeigen.

Um den infacmd isp ListLicenses-Befehl auszuführen, müssen Sie über Berechtigungen für die Lizenzen verfügen.

Der Befehl „infacmd isp ListLicenses“ verwendet die folgende Syntax:

```
ListLicenses

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port ...]

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListLicenses“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

ListMonitoringOptions

Listet allgemeine Überwachungseigenschaften auf.

Der infacmd isp listMonitoringOptions-Befehl verwendet die folgende Syntax:

```
listMonitoringOptions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp listMonitoringOptions“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, gilt der während der Installation festgelegte Benutzerbereich als Standardeinstellung.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Anzahl der Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang. Standardwert ist 180 Sekunden.

ListNodeOptions

Listet die allgemeinen Eigenschaften für einen Knoten auf. Allgemeine Eigenschaften beinhalten das Backup-Verzeichnis, das CPU-Profil, die Fehlerschweregradstufe, maximale und minimale Prozessports und Ressourcenbereitstellungsgrenzen.

Um den infacmd isp ListNodeOptions-Befehl auszuführen, müssen Sie über Berechtigungen für den Knoten verfügen.

Der Befehl „infacmd isp ListNodeOptions“ verwendet die folgende Syntax:

```
ListNodeOptions

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListNodeOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, für den Sie die Optionen auflisten möchten.

ListNodeResources

Listet alle für einen Knoten definierten Ressourcen auf. Dieser Befehl gibt für jede Ressource den Ressourcentyp zurück und gibt an, ob die Ressource verfügbar ist.

Um den infacmd isp ListNodeResources-Befehl auszuführen, müssen Sie über Berechtigungen für den Knoten verfügen.

Der Befehl „infacmd isp ListNodeResources“ verwendet die folgende Syntax:

```
ListNodeResources

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name

[<-ResourceCategory|-rc> resource_category ("PCIS", "DIS")]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListNodeResources“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, für den Sie die Ressourcen auflisten möchten.
-ResourceCategory -rc	resource_category	Optional. Kategorie der Ressourcen, die Sie auflisten möchten. Gültige Kategorien umfassen: - PCIS. Ressource für den PowerCenter-Integrationsdienst. - DIS. Für zukünftige Verwendung reserviert. Standardwert ist PCIS.

ListNodeRoles

Listet alle Rollen auf einem Knoten in der Domäne auf.

Der infacmd isp ListNodeRoles-Befehl verwendet die folgende Syntax:

```
ListNodeRoles

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
```

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

<-NodeName|-nn> node_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListNodeRoles“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeName -nn	node_name	Erforderlich. Name des Knotens.

ListNodes

Listet die Knoten in der Domäne auf. Wenn Sie die Knotenrollenoption nicht verwenden, listet der Befehl alle Knoten in der Domäne auf. Wenn Sie die Knotenrollenoption verwenden, listet der Befehl die Knoten mit der angegebenen Rolle auf.

Der Befehl „infacmd isp ListNodes“ verwendet die folgende Syntax:

```
ListNodes

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-NodeRole|-nr> node_role SERVICE|COMPUTE|SERVICE_COMPUTE]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListNodes“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeRole -nr	node_role	Optional. Aktivierte Rolle für die Knoten, die Sie auflisten möchten. Geben Sie einen der folgenden Werte ein: - „Service“. Listet Knoten auf, die mindestens über die Dienstrolle verfügen. - „Compute“. Listet Knoten auf, die mindestens über die Berechnungsrolle verfügen. - „Service_compute“. Listet Knoten auf, die über die Dienst- und Berechnungsrolle verfügen. Wenn Sie die Option nicht angeben, listet der Befehl alle Knoten in der Domäne auf.

ListOSProfiles

Listet die Betriebssystemprofile in der Domäne auf.

Der Befehl „infacmd isp ListOSProfile“ verwendet die folgende Syntax:

```
ListOSProfiles

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListOSProfile“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

ListRepositoryLDAPConfiguration

Listet die LDAP-Serverkonfigurationsoptionen wie LDAP-Serveradresse, Suchbereich und Anmeldeattribute auf.

Verwenden Sie nach dem Installieren von Informatica diesen Befehl, um die Verbindung zwischen der Domäne und dem externen LDAP-Verzeichnisdienst zu überprüfen.

Verwenden Sie infacmd isp SetRepositoryLDAPConfiguration, um die LDAP-Serverkonfigurationsoptionen für eine Informatica-Domäne zu aktualisieren. Verwenden Sie diesen Befehl, wenn Sie ein Repository aktualisieren, das LDAP-Authentifizierung verwendet.

Der Befehl „infacmd isp ListRepositoryLDAPConfiguration“ verwendet die folgende Syntax:

```
ListRepositoryLDAPConfiguration

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListRepositoryLDAPConfiguration“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

ListRolePrivileges

Listet Berechtigungen auf, die einer Rolle in der Domäne zugewiesen sind. Sie können ebenfalls Rollenberechtigungen für jeden Anwendungsdienst in der Domäne auflisten.

Sie können einer Rolle zugewiesene Berechtigungen für die Domäne und für jeden Anwendungsdiensttyp in der Domäne auflisten.

Der Befehl „infacmd isp ListRolePrivileges“ verwendet die folgende Syntax:

```
ListRolePrivileges

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

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

```
<-RoleName|-rn> role_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „ListRolePrivileges“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-RoleName -rn	role_name	Erforderlich. Name der Rolle, für die Berechtigungen aufgelistet werden. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

ListSecurityDomains

Listet die nativen und LDAP-Sicherheitsdomänen in der Domäne auf.

Der Befehl „infacmd isp ListSecurityDomains“ verwendet die folgende Syntax:

```
ListSecurityDomains

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListSecurityDomains“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

ListServiceLevels

Listet die Dienstebenen auf, die für die Domäne definiert sind. Sie können den Namen, die Dispatch-Priorität und die maximale Dispatch-Wartezeit für jede Dienstebene auflisten.

Der Befehl „infacmd isp ListServiceLevels“ verwendet die folgende Syntax:

```
ListServiceLevels

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListServiceLevels“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

ListServiceNodes

Listet die Knoten oder Gitter auf, die einem Dienst zugewiesen sind.

Wenn dieser Befehl einen Gitternamen zurückgibt, können Sie den infacmd isp ListGridNodes-Befehl ausführen, um die Knoten in einem Gitter aufzulisten.

Um den infacmd isp ListServiceNodes-Befehl auszuführen, müssen Sie über Berechtigungen für den Dienst verfügen.

Der Befehl „infacmd isp ListServiceNodes“ verwendet die folgende Syntax:

```
ListServiceNodes

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListServiceNodes“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des Diensts.

Verwandte Themen:

- "ListGridNodes" auf Seite 482

ListServicePrivileges

Listet die Berechtigungen für eine Domäne oder einen Anwendungsdiensttyp auf.

Der Befehl „infacmd isp ListServicePrivileges" verwendet die folgende Syntax:

```
ListServicePrivileges

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-ServiceType|-st> service_type AS|CMS|MM|MRS|RPS|RS|DOMAIN]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListServicePrivileges“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceType -st	service_type	Optional. Domäne oder Anwendungsdiensttyp, für die bzw. den Sie Berechtigungen anzeigen möchten. Diensttypen umfassen: - AS. Analyst-Dienst - CMS. Content-Managementdienst - MM. Metadata Manager-Dienst - MRS. Modellrepository-Dienst - RPS. Berichterstellungsdienst - RS. PowerCenter-Repository-Dienst - DOMAIN. Domäne

ListServices

Listet die Dienste in der Domäne auf.

Der Befehl „infacmd isp ListServices“ verwendet die folgende Syntax:

```
ListServices

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-ServiceType|-st> service_type AS|BW|CMS|DIS|IS|MM|MRS|RPS|RS|WS|ES|SCH|RMS|SEARCH]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListServices“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
–UserName –un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceType -st	service_type	Optional. Listet alle Dienste eines bestimmten Typs auf. Zu den Diensttypen gehören: - AS. Analyst-Dienst - BW. SAP BW-Dienst - CMS. Content-Managementdienst - DIS. Datenintegrationsdienst - IS. PowerCenter-Integrationsdienst - MM. Metadata Manager-Dienst - MRS. Modellrepository-Dienst - RPS. Berichterstellungsdienst - RS. PowerCenter-Repository-Dienst - WS. Webdienst-Hub - ES. E-Mail-Dienst - SCH. Scheduler-Dienst - RMS. Ressourcenmanager-Dienst - SEARCH. Suchdienst

ListSMTPOptions

Listet die SMTP-Konfigurationseigenschaften für die Domäne auf. Die SMTP-Konfiguration dient zum Senden von Domänenwarnungen und Scorecard-Benachrichtigungen.

Der Befehl „infacmd isp ListSMTPOptions“ verwendet die folgende Syntax:

```
ListSMTPOptions

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListSMTPOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Verwandte Themen:

- "UpdateSMTPOptions" auf Seite 652

ListUserPermissions

Listet die Domänenobjekte auf, für die ein Benutzer Berechtigungen hat.

Der Befehl „infacmd isp ListUserPermissions" verwendet die folgende Syntax:

```
ListUserPermissions

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ExistingUserName|-eu> existing_user_name

[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]

[<-ObjectType|-ot> object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListUserPermissions" beschrieben:

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

Option	Argument	Beschreibung
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Gateway-Konnektivitätsinformationen in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_second s	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ExistingUserName -eu	existing_user_name	Erforderlich. Benutzerkonto, für das Sie Berechtigungen auflisten möchten. Um einen Namen einzugeben, der Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

Option	Argument	Beschreibung
-ExistingUserSecurityDomain -esd	existing_user_security_domainth_name	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört, für den Sie Berechtigungen auflisten möchten. Standardwert ist „Native“.
-ObjectType -ot	object_type	Erforderlich. Typ des Objekts, das Sie auflisten möchten: - Dienst - License - Knoten - Gitter - Folder - OSProfile

ListUserPrivileges

Listet Berechtigungen auf, die einem Benutzer in der Domäne zugewiesen sind. Sie können ebenfalls Benutzerberechtigungen für jeden Anwendungsdienst in der Domäne auflisten.

Der Befehl „infacmd isp ListUserPrivileges“ verwendet die folgende Syntax:

```
ListUserPrivileges

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ExistingUserName|-eu> existing_user_Name

[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]

<-ServiceName|-sn> service_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListUserPrivileges“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
ExistingUserName -eu	existing_user_name	Erforderlich. Benutzerkonto, für das Sie Berechtigungen auflisten möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört, für den Sie Berechtigungen auflisten möchten. Standardwert ist „Native“.
-ServiceName -sn	service_name	Erforderlich. Domäne oder Anwendungsdienstname, für die bzw. den Sie Berechtigungen anzeigen möchten.

migrateUsers

Migriert die Gruppen, Rollen, Rechte und Berechtigungen der Benutzer in der nativen Sicherheitsdomäne für Benutzer auf eine oder mehrere LDAP-Sicherheitsdomänen. Bevor Sie eine Domäne zur Verwendung von Kerberos-Authentifizierung konfigurieren, müssen Sie die Benutzer auf eine LDAP-Sicherheitsdomäne migrieren.

Weitere Informationen zum Befehl „migrateUsers“ finden Sie im *Informatica-Sicherheitshandbuch*.

Der Befehl „infacmd isp migrateUsers“ verwendet die folgende Syntax:

```
migrateUsers

<-DomainName|-dn> domain_name

<-UserName|-un> administrator_user_name

<-Password|-pd> administrator_password

[<-SecurityDomain|-sdn>|security_domain]

[<-Gateway|-hp>|gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds ]

<-UserMigrationFile|-umf> user_migration_file
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp migrateUsers“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	administrator_user_name	Erforderlich. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.
-Password -pd	administrator_password	Erforderlich. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Optional. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. **Hinweis:** Diese Sicherheitsdomäne ist die Sicherheitsdomäne des Benutzerkontos, das zum Herstellen einer Verbindung zur Domäne verwendet wird, nicht zur Sicherheitsdomäne, auf die die Benutzer migriert werden.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Optional. Verwenden, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

-UserMigrationFile
-umf
	user_migration_file	Erforderlich. Pfad und Dateiname der Benutzermigrationsdatei. Die Benutzermigrationsdatei ist eine Textdatei, die die Liste der nativen Benutzer und die entsprechenden LDAP-Benutzer enthält. Einträge müssen im folgenden Format vorliegen:
		`Native/<SourceUserName>,LDAP/<TargetUsername>`
		Beispiel: Um einen Benutzer namens Benutzer1 aus der nativen Sicherheitsdomäne in einen Benutzer namens Benutzer1 in einer LDAP-Sicherheitsdomäne zu migrieren, fügen Sie der Benutzermigrationsdatei die folgende Zeile hinzu:
		`Native/User1,LDAP/User1`
		Der Befehl überspringt Einträge mit einem doppelten Quell- oder Zielbenutzernamen.

MoveFolder

Entfernt einen Ordner.

Der Befehl „infacmd isp MoveFolder“ verwendet die folgende Syntax:

```
MoveFolder

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-OriginalPath|-op> original_folder_path

<-FolderPath|-fp> full_folder_path
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp MoveFolder“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-OriginalPath -op	original_folder_path	Erforderlich. Vollständiger Pfad (ohne Domänenname) des zu verschiebenden Ordners. Folgendes Format ist erforderlich: */parent_folder/child_folder*
-FolderPath -fp	full_folder_path	Erforderlich. Vollständiger Pfad (ohne Domänenname) zum Speicherort des Zielordners. Folgendes Format ist erforderlich: */parent_folder/child_folder*

MoveObject

Verschiebt ein Objekt in einen anderen Ordner.

Der Befehl „infacmd isp MoveObject“ verwendet die folgende Syntax:

```
MoveObject

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ObjectName|-on> object_name

<-ObjectType|-ot> object_type_SERVICE_LICENSE_NODE_GRID

<-FolderPath|-fp> full_folder_path
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp MoveObject“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ObjectName -on	object_name	Erforderlich. Name des Objekts, das Sie verschieben möchten.

Option	Argument	Beschreibung
-ObjectType -ot	object_type	Erforderlich. Typ des Objekts, das Sie verschieben möchten: - Dienst - Lizenz - Knoten - Gitter
-FolderPath -fp	full_folder_path	Erforderlich. Vollständiger Pfad (ohne Domänenname) des Ordners, in den Sie das Objekt verschieben möchten. Folgendes Format ist erforderlich: */parent_folder/child_folder*

Ping

Pingt eine Domäne, einen Dienst, einen Domänen-Gateway-Host oder einen Knoten. Wenn das Objekt verfügbar ist, zeigt dieser Befehl eine Meldung an, dass das Objekt an einem bestimmten Port auf dem Gateway-Host-Computer verfügbar ist. Wenn das Objekt nicht verfügbar ist, zeigt dieser Befehl eine Meldung darüber an, dass keine Antwort von der Domäne empfangen wurde.

Verwenden Sie diesen Befehl zur Fehlerbehebung von Netzwerkverbindungen. Um den infacmd isp Ping-Befehl auszuführen, müssen Sie über Berechtigungen für das Objekt verfügen, das Sie pingen möchten.

Der infacmd isp Ping-Befehl zeigt keine Ergebnisse für einzelne Dienstprozesse an.

Der infacmd isp Ping-Befehl verwendet die folgende Syntax:

```
Ping

[<-DomainName|-dn> domain_name]

[<-ServiceName|-sn> service_name]

[<-GatewayAddress|-dg> domain_gateway_host:port]

[<-NodeName|-nn> node_name]

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

In der folgenden Tabelle werden infacmd isp Ping-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Optional. Name des Diensts, den Sie anpingen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

Option	Argument	Beschreibung
-GatewayAddress -dg	domain_gateway_host:port	Erforderlich, wenn Sie die Option -DomainName nicht angeben oder wenn Sie eine andere Domäne anpingen müssen. Name und Portnummer des Gateway-Hostcomputers.
-NodeName -nn	node_name	Optional. Name des Knotens.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

PrintSPNAndKeytabNames

Generiert die Liste der SPN- und Keytab-Dateinamen für die Knoten und Dienste in der Domäne. In der Informatica-Domäne muss jeder SPN eine Keytab-Datei enthalten. Sie müssen unter Umständen den Kerberos-Administrator bitten, die SPNs zur Prinzipaldatenbank hinzuzufügen und die Keytab-Dateien zu erstellen. Die SPNs und Keytab-Dateinamen unterliegen der Groß-/Kleinschreibung.

Der Befehl „infacmd isp PrintSPNAndKeytabNames“ verwendet die folgende Syntax:

```
PrintSPNAndKeytabNames

<-DomainName|-dn> domain_name

<-ServiceRealmName|-srn> realm_name_of_node_spn

[<-Format|-fm> format_TEXT_CSV]

[<-OutputFile|-of> output_file_name]

[<-DomainNodes|-dns> Node1:HostName1 Node2:HostName2 ...]

[<-ServiceProcesses|-sps> ServiceName1:NodeName1 ServiceName2:NodeName2...]

[<-SPNShareLevel|-spnSL> SPNShareLevel PROCESS|NODE]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp PrintSPNAndKeytabNames“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceRealmName -srn	realm_name_of_node_spn	Erforderlich. Name des Kerberos-Bereichs, zu dem die Informatica-Domänendienste gehören. Der Bereichsname muss in Großbuchstaben angegeben werden und die Groß-/Kleinschreibung wird unterschieden.
-Format -fm	format_TEXT_CSV	Optional. Format der Ausgabedatei. Gültige Typen umfassen: - Text - CSV Wenn Sie kein Format angeben, verwendet infacmd Textformat mit einer Zeilenlänge von 80 Zeichen.
-OutputFile -of	output_file_name	Optional. Name und Dateipfad für die Ausgabedatei. Wenn Sie keinen Ausgabedateinamen angeben, zeigt infacmd die Protokollereignisse auf dem Bildschirm an.
-DomainNodes -dns	NodeName:HostName [NodeName:Hostname]	Name des Knotens und der voll qualifizierte Hostname des Computers, der den Knoten hostet. Verwenden Sie das folgende Format: NodeName:HostName Sie können SPNs und Keytab-Dateinamen für mehrere Knoten generieren. Trennen Sie jedes Knotennamen- und Hostnamen-Paar mit einem Leerzeichen.

Option	Argument	Beschreibung
-ServiceProcesses -sps	ServiceName:Nodename [ServiceName:Knotenname]	Optional. Name des Diensts, den Sie in der Informatica-Domäne erstellen möchten, sowie der Name des Knotens, auf dem der Dienst ausgeführt werden soll. Verwenden Sie das folgende Format: ServiceName:NodeName Sie können SPNs und Keytab-Dateinamen für mehrere Dienste generieren. Trennen Sie jedes aus Dienst- und Knotenname bestehende Paar durch ein Leerzeichen. **Hinweis:** Die Schlüsseltabellen-Dateien für Anwendungsdienste in der Domäne müssen für die Konfiguration der Domäne zwecks Kerberos-Authentifizierung nicht verfügbar sein. Sie können den Dienst-SPN zur Prinzipaldatenbank hinzufügen und die Schlüsseltabelle erstellen, nachdem Sie die Authentifizierung der Informatica-Domäne geändert haben, bevor Sie jedoch den Dienst aktivieren.
SPNShareLevel -spnSL	SPNShareLevel PROCESS|NODE]	Optional. Gibt die Dienst-Prinzipalebene für die Domäne an. Legen Sie eine der folgenden Ebenen für die Eigenschaft fest: - Prozess Die Domäne erfordert einen eindeutigen Dienst-Prinzipalnamen (SPN) und eine Keytab-Datei für jeden Knoten und für jeden Dienst auf einem Knoten. Die Anzahl der für jeden Knoten erforderlichen SPNs und Keytab-Dateien hängt von der Anzahl der Dienstprozesse ab, die auf dem Knoten ausgeführt werden. Empfohlen für Produktionsdomänen. - Knoten. Die Domäne verwendet einen SPN und eine Keytab-Datei für den Knoten und für alle Dienste, die auf dem Knoten ausgeführt werden. Sie erfordert außerdem einen separaten SPN und eine separate Keytab-Datei für alle HTTP-Prozesse auf dem Knoten. Empfohlen für Test- und Entwicklungsdomänen. Empfohlen für Test- und Entwicklungsdomänen. Standardwert ist „Prozess“.

PurgeLog

Löscht Log-Ereignisse. Sie können Log-Ereignisse für eine Domäne oder für Anwendungsdienste löschen, wie zum Beispiel der PowerCenter-Integrationsdienst, der Datenintegrationsdienst und der Web Services Hub.

Der Befehl „infacmd isp PurgeLog“ verwendet die folgende Syntax:

```
PurgeLog

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-BeforeDate|-bd> before_date

[<-LicenseUsage|-lu>]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp PurgeLog“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-BeforeDate -bd	before_date	Erforderlich. Bereinigt Protokollereignisse, die vor diesem Datum und dieser Uhrzeit aufgetreten sind. Geben Sie Datum und Uhrzeit in einem der folgenden Formate ein: - MM/tt/jjjj - jjjj-MM-tt
-LicenseUsage -lu	-	Optional. Bereinigt Protokollereignisse und Datensätze für die Lizenzverwendung.

PurgeMonitoringData

Bereinigt Überwachungsdaten im Modellrepository.

Der infacmd isp purgeMonitoringData-Befehl verwendet die folgende Syntax:

```
purgeMonitoringData
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-NumDaysToRetain|-ndr> num_days_to_retain]
[<-NumDaysToRetainDetailedStat|-ndrds> num_days_to_retain_detailed_stat]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp purgeMonitoringData“ beschrieben:

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

Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Anzahl der Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang. Standardwert ist 180 Sekunden.
-NumDaysToRetain -ndr	num_days_to_retain	Optional. Anzahl der Tage, die gemittelte Daten im Modellrepository beibehalten werden. Wenn Sie beispielsweise 180 eingeben, bereinigt der Modellrepository-Dienst alle gemittelten Daten, die älter als 180 Tage sind. Wenn Sie diese Option nicht konfigurieren, bereinigt PurgeMonitoringData alle gemittelten Überwachungsdaten im Modellrepository. Minimalwert ist 0. Maximalwert ist 366.
-NumDaysToRetainDetailedStat -ndrds	num_days_to_retain_detailed_stat	Optional. Anzahl der Tage, die minutengenaue Daten im Modellrepository beibehalten werden. Wenn Sie beispielsweise 7 eingeben, bereinigt der Modellrepository-Dienst alle gemittelten Daten, die älter als 7 Tage sind. Wenn Sie diese Option nicht konfigurieren, bereinigt PurgeMonitoringData alle minutengenauen Überwachungsdaten im Modellrepository. Minimalwert ist 0. Maximalwert ist 14.

RemoveAlertUser

Hebt das Abonnement von Alarm-E-Mail-Nachrichten für einen Benutzer auf. Sie können infacmd isp RemoveAlertUser für alle Benutzer ausführen.

Der Befehl „infacmd isp RemoveAlertUser“ verwendet die folgende Syntax:

```
RemoveAlertUser

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password
```

```
[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-AlertUser|-au> user_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveAlertUser“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-AlertUser -au	user_name	Erforderlich. Name des Benutzers, für den Sie das Abonnement von Alarmen aufheben möchten.

RemoveConnection

Entfernt eine Verbindung aus der Domäne.

Der Befehl „infacmd isp RemoveConnection“ verwendet die folgende Syntax:

```
RemoveConnection

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ConnectionName|-cn> connection_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveConnection“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ConnectionName -cn	connection_name	Name der zu entfernenden Verbindung.

RemoveConnectionPermissions

Entfernt Verbindungsberechtigungen für einen Benutzer oder eine Gruppe.

Der Befehl „infacmd isp RemoveConnectionPermissions“ verwendet die folgende Syntax:

```
RemoveConnectionPermissions

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<<-RecipientUserName|-run> recipient_user_name|<ReceipeintGroupName|-rgn>
recipeint_group_name>

<-RecipientSecurityDomain|-rsd> recipient_security_domain]

<-ConnectionName|-cn> connection_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveConnectionPermissions“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-RecipientUserName -run	recipient_user_name	Erforderlich, wenn Sie den Gruppennamen des Empfängers nicht angeben. Name des Benutzers, für den Berechtigungen entfernt werden.
-RecipientGroupName -rgn	recipient_group_name	Erforderlich, wenn Sie den Benutzernamen des Empfängers nicht angeben. Name der Gruppe, für die Berechtigungen für die Verbindung entfernt werden.
-RecipientSecurityDomain -rsd	recipient_security_domain_name	Erforderlich, wenn der Empfänger zu einer LDAP-Sicherheitsdomäne gehört. Name der Sicherheitsdomäne, zu der der Empfänger gehört. Standardwert ist „Native“.
-ConnectionName -cn	connection_name_security_domain	Erforderlich. Name der Verbindung.

RemoveDomainLink

Entfernt eine verknüpfte Domäne. Wenn Sie eine verknüpfte Domäne entfernen, können Sie keine Repository-Metadaten zwischen der lokalen und der verknüpften Domäne herstellen. Möglicherweise gehen Sie so vor, wenn Sie in einer anderen Domäne nicht mehr auf den PowerCenter-Repository-Dienst zugreifen müssen.

Der Befehl „infacmd isp RemoveDomainLink“ verwendet die folgende Syntax:

```
RemoveDomainLink

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-LinkedDomainName|-ld> linked_domain_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveDomainLink“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der lokalen Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeitraum in Sekunden, in dem infacmd versucht, eine Verbindung zur lokalen Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-LinkedDomainName -ld	linked_domain_name	Erforderlich. Name der Domäne, aus der Sie eine Verbindung entfernen möchten.

RemoveFolder

Entfernt alle Ordner aus der Domäne. Bevor Sie einen Ordner entfernen, müssen Sie sicherstellen, dass der Ordner leer ist.

Der Ordner muss leer sein.

Der Befehl „infacmd isp RemoveFolder“ verwendet die folgende Syntax:

```
RemoveFolder

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-FolderPath|-fp> full_folder_path
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveFolder“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-FolderPath -fp	full_folder_path	Erforderlich. Vollständiger Pfad (ohne Domänenname) des zu entfernenden Ordners. Folgendes Format ist erforderlich: */parent_folder/child_folder*

RemoveGrid

Entfernt ein Gitter aus der Domäne. Bevor Sie ein Gitter entfernen können, müssen Sie die Zuweisung des Gitters aus dem PowerCenter Integration Service oder dem Data Integration Service aufheben.

Der infacmd isp RemoveGrid-Befehl verwendet die folgende Syntax:

```
RemoveGrid

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-GridName|-gn> grid_name
```

In der folgenden Tabelle werden infacmd isp RemoveGrid-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.

Option	Argument	Beschreibung
-Password -pd	passwort	Erforderlich. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -pd festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-GridName -gn	grid_name	Erforderlich. Name des Gitters, das Sie entfernen möchten.

RemoveGroup

Entfernt eine Gruppe aus der nativen Sicherheitsdomäne.

Der Befehl „infacmd isp RemoveGroup“ verwendet die folgende Syntax:

```
RemoveGroup

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
```

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

<-GroupName|-gn> group_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveGroup“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-GroupName -gn	group_name	Erforderlich. Name der Gruppe, die Sie entfernen möchten.

RemoveGroupPermission

Entfernt eine Gruppenberechtigung für ein Objekt.

Der Befehl „infacmd isp RemoveGroupPermission“ verwendet die folgende Syntax:

```
RemoveGroupPermission

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ExistingGroup|-eg> existing_group_name

[<-GroupSecurityDomain|-gsf> group_security_domain]

<-ObjectName|-on> object_name

<-ObjectType|-ot> object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveGroupPermission“ beschrieben:

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

Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ExistingGroup -eg	existing_group_name	Erforderlich. Name der Gruppe, der Sie eine Berechtigung für ein Objekt zuweisen möchten.
-GroupSecurityDomain -gsf	group_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der die Gruppe gehört, der Sie eine Berechtigung zuweisen möchten. Standardwert ist „Native“.
-ObjectName -on	object_name	Name des Objekts, dem Sie die Gruppenzugriffsberechtigung entziehen möchten.
-ObjectType -ot	object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE	Erforderlich. Typ des Objekts Geben Sie einen der folgenden Werte ein: - Dienst - License - Knoten - Gitter - Folder - OSProfile

RemoveGroupPrivilege

Entfernt eine Berechtigung aus einer Gruppe in der Domäne. Sie können eine Berechtigung aus einer Gruppe für die Domäne oder einen Anwendungsdienst in der Domäne entfernen.

Der Befehl „infacmd isp RemoveGroupPrivilege“ verwendet die folgende Syntax:

```
RemoveGroupPrivilege

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

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

```
<-GroupName|-gn> group_name

[<-GroupSecurityDomain|-gsf> group_security_domain]

<-ServiceName|-sn> service_name

<-PrivilegePath|-pp> path_of_privilege
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveGroupPrivilege“ beschrieben:

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

Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-GroupName -gn	group_name	Erforderlich. Name der Gruppe, aus der Sie die Berechtigung entfernen. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-GroupSecurityDomain -gsf	group_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der die Gruppe gehört, aus der Sie Berechtigungen entfernen. Standardwert ist „Native“.
-ServiceName -sn	service_name	Erforderlich. Domäne oder Anwendungsdienstname, für die bzw. den Sie Berechtigungen anzeigen möchten.

-PrivilegePath
-pp
	path_of_privilege	Erforderlich. Vollqualifizierter Name der Berechtigung, die Sie der Gruppe zuweisen möchten. Ein vollqualifizierter Name enthält den Namen der Berechtigungsgruppe und den Namen der Berechtigung. Ein vollqualifizierter Berechtigungsname für den Repository-Dienst ist z. B. „folder/create“. Wenn der Berechtigungsname Leerzeichen enthält, setzen Sie den Pfad wie folgt in Anführungszeichen:
		`“Runtime Objects/Monitor/Execute/Manage Execution”`
		Wenn der Berechtigungsname das Sonderzeichen „/“ enthält, fügen Sie das Escape-Zeichen „\“ davor folgendermaßen ein:
		`“Model/View Model/Export\/Import Models”`

RemoveLicense

Entfernt eine Lizenz aus der Domäne. Bevor Sie diesen Befehl ausführen, müssen Sie zuerst die der Lizenz zugewiesenen Dienste deaktivieren.

Entfernt einen Lizenz aus einer Domäne, wenn sie abläuft oder wenn Sie die Lizenz in eine andere Domäne verschieben möchten.

Der Befehl „infacmd isp RemoveLicense“ verwendet die folgende Syntax:

```
RemoveLicense

<-DomainName|-dn> domain_name

<-UserName|-un> user_name
```

```
<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-LicenseName|-ln> license_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveLicense“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-LicenseName -ln	license_name	Erforderlich. Name der Lizenz, die Sie entfernen möchten.

Verwandte Themen:

- "DisableService" auf Seite 402
- "UnassignLicense" auf Seite 601

RemoveNode

Entfernt alle Knoten aus der Domäne. Wenn der Knoten ausgeführt wird, müssen Sie ihn zunächst herunterfahren.

Der Befehl „infacmd isp RemoveNode" verwendet die folgende Syntax:

```
RemoveNode

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveNode“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, den Sie entfernen möchten.

RemoveNodeResource

Entfernt eine Ressource aus dem Knoten. Sie können eine benutzerdefinierte Ressource oder eine Datei- bzw. Verzeichnisressource aus einem Knoten entfernen. Sie können keine Verbindungsressource aus einem Knoten entfernen.

Wenn ein PowerCenter-Integrationsdienst in einem Gitter ausgeführt wird, kann der Load Balancer Ressourcen verwenden, um Sitzungs-, Befehls- und vordefinierte Event-Wait-Aufgaben zu verteilen. Wenn der PowerCenter-Integrationsdienst für die Überprüfung von Ressourcen konfiguriert ist, verteilt der Load Balancer Aufgaben an Knoten, auf denen Ressourcen hinzugefügt und aktiviert werden. Wenn Sie eine Ressource entfernen, die von der Sitzungs- oder Befehlsaufgabe benötigt wird, kann die Aufgabe auf diesem Knoten nicht länger ausgeführt werden.

Der Befehl „infacmd isp RemoveNodeResource“ verwendet die folgende Syntax:

```
RemoveNodeResource

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name

[<-ResourceCategory|-rc> resource_category ("PCIS", "DIS")]

<-ResourceType|-rt> resource_type("Custom", "File Directory")

<-ResourceName|-rn> resource_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveNodeResource“ beschrieben:

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

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeName -nn	node_name	Erforderlich. Name des Knotens mit der Ressource, die Sie entfernen möchten.
-ResourceCategory -rc	resource_category	Optional. Kategorie der Ressource, die Sie entfernen möchten. Gültige Kategorien umfassen: - PCIS. Ressource für den PowerCenter-Integrationsdienst. - DIS. Für zukünftige Verwendung reserviert. Standardwert ist PCIS.
-ResourceType -rt	resource_type	Erforderlich. Typ der Ressource, die Sie entfernen möchten. Gültige Typen umfassen: - Benutzerdefiniert - Dateiverzeichnis
-ResourceName -rn	resource_name	Erforderlich. Vollständiger Name der zu entfernenden Ressource. Um die Namen aller für einen Knoten verfügbaren Ressourcen aufzulisten, führen Sie den infacmd isp ListNodeResources-Befehl aus.

RemoveOSProfile

Entfernt ein Betriebssystemprofil aus der Domäne.

Der Befehl „infacmd isp RemoveOSProfile“ verwendet die folgende Syntax:

```
RemoveOSProfile

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-OSProfileName|-on> OSProfile_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveOSProfile“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-OSProfileName -on	OSProfile_name	Erforderlich. Name des Betriebssystemprofils, das Sie entfernen möchten.

RemoveRole

Entfernt eine benutzerdefinierte Rolle aus der Domäne. Wenn Sie eine benutzerdefinierte Rolle entfernen, werden die benutzerdefinierte Rolle und alle damit verbundenen Berechtigungen für alle Benutzer und Gruppen entfernt, die der Rolle zugewiesen sind.

Der Befehl „infacmd isp RemoveRole“ verwendet die folgende Syntax:

```
RemoveRole

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-RoleName|-rn> role_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveRole“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-RoleName -rn	role_name	Erforderlich. Name der Rolle, die Sie entfernen möchten.

RemoveRolePrivilege

Entfernt eine Berechtigung aus einer Rolle in der Domäne oder aus einer Rolle im Anwendungsdienst innerhalb der Domäne.

Der Befehl „infacmd isp RemoveRolePrivilege“ verwendet die folgende Syntax:

```
RemoveRolePrivileges

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-RoleName|-rn> role_name

<-ServiceType|-st> service_type AS|CMS|MM|MRS|RPS|RS|DOMAIN

<-PrivilegePath|-pp> path_of_privilege
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveRolePrivilege“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-RoleName -rn	role_name	Erforderlich. Name der Rolle, aus der Sie die Berechtigung entfernen. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

Option	Argument	Beschreibung
-ServiceType -st	service_type	Erforderlich. Domäne oder Anwendungsdiensttyp, aus der bzw. dem Sie die Berechtigung für die Rolle entfernen möchten. Diensttypen umfassen: - AS. Analyst-Dienst - CMS. Content-Managementdienst - MM. Metadata Manager-Dienst - MRS. Modellrepository-Dienst - RPS. Berichterstellungsdienst - RS. PowerCenter-Repository-Dienst - DOMAIN. Domäne

-PrivilegePath
-pp>
	path_of_privilege	Erforderlich. Vollqualifizierter Name der Berechtigung, die Sie der Gruppe zuweisen möchten. Ein vollqualifizierter Name enthält den Namen der Berechtigungsgruppe und den Namen der Berechtigung. Ein vollqualifizierter Berechtigungsname für den Repository-Dienst ist z. B. „folder/create“. Wenn der Berechtigungsname Leerzeichen enthält, setzen Sie den Pfad wie folgt in Anführungszeichen:
		`“Runtime Objects/Monitor/Execute/Manage Execution”`
		Wenn der Berechtigungsname das Sonderzeichen „/“ enthält, fügen Sie das Escape-Zeichen „\“ davor folgendermaßen ein:
		`“Model/View Model/Export\/Import Models”`

RemoveService

Entfernt einen Anwendungsdienst aus der Domäne. Bevor Sie einen Dienst entfernen, müssen Sie ihn deaktivieren.

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

```
RemoveService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name
```

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

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des Diensts, den Sie entfernen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

RemoveServiceLevel

Entfernt eine Dienstebene. Wenn Sie eine Dienstebene entfernen, aktualisiert der Workflow Manager keine Aufgaben, die die Dienstebene verwenden. Wenn eine Arbeitsablauf-Dienstebene in der Domäne nicht vorhanden ist, sendet der Load Balancer die Aufgaben mit einer Standarddienstebene.

Der Befehl „infacmd isp RemoveServiceLevel“ verwendet die folgende Syntax:

```
RemoveServiceLevel

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceLevelName|-ln> service_level_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveServiceLevel“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceLevelName -ln	service_level_name	Erforderlich. Name der Dienstebene, die Sie entfernen möchten.

RemoveUser

Entfernt ein Benutzerkonto aus der nativen Sicherheitsdomäne. Benutzerkonten können nicht aus LDAP-Sicherheitsdomänen entfernt werden.

Der Befehl „infacmd isp RemoveUser“ verwendet die folgende Syntax:

```
RemoveUser

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ExistingUserName|-eu> existing_user_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveUser“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ExistingUserName -eu	existing_user_name	Erforderlich. Benutzerkonto, das Sie entfernen möchten.

RemoveUserFromGroup

Entfernt einen nativen oder LDAP-Benutzer aus der nativen Gruppe in der Domäne.

Der Befehl „infacmd isp RemoveUserFromGroup“ verwendet die folgende Syntax:

```
RemoveUserFromGroup

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ExistingUserName|-eu> existing_user_name

[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]

<-GroupName|-gn> group_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveUserFromGroup“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ExistingUserName -eu	existing_user_name	Erforderlich. Name des Benutzers, den Sie entfernen möchten.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört, den Sie entfernen möchten. Standardwert ist „Native“.
-GroupName -gn	group_name	Erforderlich. Name der Gruppe, aus der Sie den Benutzer entfernen möchten.

RemoveUserPermission

Entfernt eine Benutzerberechtigung für ein Objekt.

Der Befehl „infacmd isp RemoveUserPermission“ verwendet die folgende Syntax:

```
RemoveUserPermission

<-DomainName|-dn> domain_name
```

```
<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ExistingUserName|-eu> existing_user_name

[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]

<-ObjectName|-on> object_name

<-ObjectType|-ot> object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE
```

Die folgende Tabelle beschreibt die Optionen und Argumente für „infacmd isp RemoveUserPermission“:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Gateway-Konnektivitätsinformationen in der Datei „domains.infa“ veraltet sind. Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert.
-ExistingUserName -eu	existing_user_name	Erforderlich. Name des Benutzers, dem Sie eine Berechtigung für ein Objekt zuweisen möchten.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört, dem Sie eine Berechtigung zuweisen möchten. Standardwert ist „Native“.
-ObjectName -on	object_name	Name des Objekts, dem Sie die Benutzerzugriffsberechtigung entziehen möchten.
-ObjectType -ot	object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE	Erforderlich. Typ des Objekts Geben Sie einen der folgenden Werte ein: - Dienst - License - Knoten - Gitter - Folder - OSProfile

RemoveUserPrivilege

Entfernt eine Berechtigung von einem Benutzer in der Domäne oder von einem Benutzer im Anwendungsdienst innerhalb der Domäne.

Der Befehl „infacmd isp RemoveUserPrivilege“ verwendet die folgende Syntax:

```
RemoveUserPrivilege

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ExistingUserName|-eu> existing_user_Name

[<-ExistingUserSecurityDomain|-esd> existing_user_security

<-ServiceName|-sn> service_name

<-PrivilegePath|-pp> path_of_privilege
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RemoveUserPrivilege“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
ExistingUserName -eu	existing_user_name	Erforderlich. Benutzerkonto, aus dem Sie die Berechtigung entfernen. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört, dessen Berechtigung entfernt werden soll. Standardwert ist „Native“.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Domäne oder Anwendungsdienstname, für die bzw. den Sie Berechtigungen anzeigen möchten.

-PrivilegePath
-pp
	path_of_privilege	Erforderlich. Vollqualifizierter Name der Berechtigung, die Sie der Gruppe zuweisen möchten. Ein vollqualifizierter Name enthält den Namen der Berechtigungsgruppe und den Namen der Berechtigung. Ein vollqualifizierter Berechtigungsname für den Repository-Dienst ist z. B. „folder/create“. Wenn der Berechtigungsname Leerzeichen enthält, setzen Sie den Pfad wie folgt in Anführungszeichen:
		`“Runtime Objects/Monitor/Execute/Manage Execution”`
		Wenn der Berechtigungsname das Sonderzeichen „/“ enthält, fügen Sie das Escape-Zeichen „\“ davor folgendermaßen ein:
		`“Model/View Model/Export\ /Import Models”`

RenameConnection

Benennt eine Verbindung um. Wenn Sie eine Verbindung umbenennen, aktualisieren das Developer-Tool und das Analyst-Tool die Jobs, die die Verbindung verwenden.

Hinweis: Bereitgestellte Anwendungen und Parameterdateien identifizieren eine Verbindung nach Namen, nicht nach Verbindungs-ID. Beim Umbenennen einer Verbindung müssen Sie daher alle Anwendungen erneut bereitstellen, die die Verbindung verwenden. Außerdem müssen Sie alle Parameterdateien aktualisieren, die den Verbindungsparameter verwenden.

Der Befehl „infacmd isp RenameConnection“ verwendet folgende Syntax:

```
RenameConnection

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ConnectionName|-cn> connection_name

<-NewConnectionName|-ncn> new_connection_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RenameConnection“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ConnectionName -cn	connection_name	Erforderlich. Vorhandener Verbindungsname.
-NewConnectionName -ncn	new_connection_name	Erforderlich. Name der neuen Verbindung. Der Name unterliegt der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die maximale Länge beträgt 128 Zeichen. Das Leer- und die folgenden Sonderzeichen sind möglich: `~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /`

ResetPassword

Setzt das Passwort für einen Benutzer in der Domäne zurück.

Der Befehl „infacmd isp ResetPassword“ verwendet die folgende Syntax:

```
ResetPassword

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ResetUserName|-ru> reset_user_name

<-ResetUserPassword|-rp> reset_user_password
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ResetPassword“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-ResetUserName -ru	reset_user_name	Erforderlich. Name des Benutzers, dessen Passwort Sie zurücksetzen möchten.
-ResetUserPassword -rp	reset_user_password	Erforderlich. Neues Passwort für den Benutzer. Sie können ein Passwort mit der Option -rp oder der Umgebungsvariable INFA_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -rp festgelegte Passwort Vorrang. Das Passwort unterliegt der Groß-/Kleinschreibung und darf 1 bis 80 Zeichen umfassen. Um ein Passwort einzugeben, das Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie es in Anführungszeichen.

RunCPUProfile

Berechnet das CPU-Profil für einen Knoten.

Hinweis: Die Ausführung dieses Befehls dauert etwa fünf Minuten und lastet die CPU des Computers zu 100% aus.

Der Befehl „infacmd isp RunCPUProfile“ verwendet die folgende Syntax:

```
RunCPUProfile

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RunCPUProfile“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, für den Sie das CPU-Profil berechnen möchten.

SetConnectionPermissions

Weist einem Benutzer oder einer Gruppe Verbindungsberechtigungen nach dem Entfernen der vorherigen Berechtigungen zu.

Der Befehl „infacmd isp SetConnectionPermissions“ verwendet die folgende Syntax:

```
SetConnectionPermissions

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<<-RecipientUserName|-run> recipient_user_name|<RecipientGroupName|-rgn>
recipient_group_name>

<-RecipientSecurityDomain|-rsd> recipient_security_domain]

<-ConnectionName|-cn> connection_name

[<-Permission|-p> permission_READ|WRITE|EXECUTE|GRANT|ALL
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp SetConnectionPermissions“ beschrieben:

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

Option	Argument	Beschreibung
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-RecipientUserName -run	recipient_user_name	Erforderlich, wenn Sie den Gruppennamen des Empfängers nicht angeben. Name des Benutzers, dem Berechtigungen für die Verbindung zugewiesen werden
-RecipientGroupName -rgn	recipient_group_name	Erforderlich, wenn Sie den Benutzernamen des Empfängers nicht angeben. Name der Gruppe, der Berechtigungen für die Verbindung zugewiesen werden.
-RecipientSecurityDomain -rsd	recipient_security_domain th_name	Erforderlich, wenn der Empfänger zu einer LDAP-Sicherheitsdomäne gehört. Name der Sicherheitsdomäne, zu der der Empfänger gehört. Standardwert ist „Native“.

Option	Argument	Beschreibung
-ConnectionName -cn	connection_name_security_domain	Erforderlich. Name der Verbindung.
-Permission -p	permission	Erforderlich. Typ der zuzuweisenden Berechtigung. Geben Sie mindestens einen der folgenden Werte durch Leerzeichen getrennt ein: - READ - WRITE. Lesen und Schreiben. - EXECUTE - GRANT. Lesen und Gewähren. - ALL. Lesen, Schreiben, Ausführen, Gewähren

SetLDAPConnectivity

Richtet die Verbindung zu einem LDAP-Server ein. Wenn Sie eine Verbindung zu einem LDAP-Server einrichten, importiert der Dienstmanager die Benutzerkonten aller LDAP-Sicherheitsdomänen aus dem LDAP-Server.

Der Befehl „infacmd isp SetLDAPConnectivity“ verwendet die folgende Syntax:

```
SetLDAPConnectivity

<-DomainName|-dn> domain_name

<-UserName|-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, SunJavaSystemDirectory, NovellE-
Directory, IBMTivoliDirectory, OpenLDAP

[<-MaxSecurityDomainSize|-ms> Max_Security_Domain_size]

[<-GroupMembershipAttr|-gm> LDAP_Group_Membership_Attribute]

[<-LDAPNotCaseSensitive|-lnc> ldap_not_case_sensitive]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp SetLDAPConnectivity“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-LDAPAddress -la	ldap_server_address	Erforderlich. Hostname und Portnummer für den Computer, auf dem der LDAP-Verzeichnisdienst gehostet wird. In der Regel weist der LDAP-Server die Portnummer 389 auf. Wenn der LDAP-Server SSL verwendet, lautet dessen Portnummer 636.
-LDAPPrincipal -lp	ldap_principal	Optional. Distinguished Name (DN) für den Prinzipal-Benutzer. Lassen Sie diese Option aus, um sich als anonymer Benutzer anzumelden. Weitere Informationen finden Sie in der Dokumentation für den LDAP-Verzeichnisdienst.
-LDAPCredential -lc	ldap_credential	Optional. Passwort für den Prinzipal-Benutzer. Sie können ein Passwort mit der Option -lc oder der Umgebungsvariable INFA_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -lc festgelegte Passwort Vorrang. Lassen Sie diese Option aus, um sich als anonymer Benutzer anzumelden.
-UseSSL -us	use_ssl	Optional. Wenn Sie die Option einbeziehen, verwendet der LDAP-Verzeichnisdienst das SSL-Protokoll (Secure Socket Layer).
-TrustLDAPCertificate -tc	trust_ldap_certificate	Optional. Wenn Sie die Option einbeziehen, stellt PowerCenter eine Verbindung zum LDAP-Server ohne Überprüfung des SSL-Zertifikats aus. Wenn Sie die Option nicht einbeziehen, stellt PowerCenter vor dem Herstellen einer Verbindung zum LDAP-Server sicher, dass das SSL-Zertifikat von einer Zertifizierungsstelle signiert ist.
-LDAPType -lt	ldap_types=value	Erforderlich. Typ des LDAP-Verzeichnisdiensts. Verzeichnisdienste umfassen: - MicrosoftActiveDirectory - SunJavaSystemDirectory - NovellE-Directory - IBMTivoliDirectory - OpenLDAP
-MaxSecurityDomainSize -ms	Max_Security_Domain_size	Optional. Maximale Anzahl an Benutzerkonten zum Importieren in eine Sicherheitsdomäne. Standardwert ist „1000“.

Option	Argument	Beschreibung
-GroupMembershipAttr -gm	LDAP_Group_Membership_Attribute	Optional. Name des Attributs, das Informationen zur Gruppenmitgliedschaft eines Benutzers enthält.
-LDAPNotCaseSensitive -lnc	LDAP_Not_Case_Sensitive	Optional. Gibt an, dass die Benutzernamen aus dem LDAP-Verzeichnisdienst der Groß-/Kleinschreibung nicht unterliegen. Standardwert ist „false“.

SetRepositoryLDAPConfiguration

Aktualisiert die LDAP-Serverkonfigurationsoptionen für ein PowerCenter-Repository.

Möglicherweise ist es erforderlich, die Verbindungsinformationen zwischen dem Repository und dem externen LDAP-Verzeichnisdienst nach der Installation von Informatica zu aktualisieren.

Verwenden Sie infacmd isp ListRepositoryLDAPConfiguration, um die aktuellen Werte für die LDAP-Serverkonfigurationsoptionen anzuzeigen.

Der Befehl „infacmd isp SetRepositoryLDAPConfiguration“ verwendet die folgende Syntax:

```
SetRepositoryLDAPConfiguration

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-LDAPAddress|-la> ldap_server_address

<-SearchBase|-sb> search base

<-SearchScope|-ss> search scope

<-LDAPPrincipal|-lp> ldap_principal

<-LDAPCredential|-lc> ldap_credential

<-LoginAttribute|-lt> login attribute

<-LoginFilter|-lf> login filter

[<-UseSSL|-us> use_ssl]

[<-CertificateDatabase|-cd> certificate database for ssl]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp SetRepositoryLDAPConfiguration“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-LDAPAddress -la	ldap_server_address	Erforderlich. Hostname und Portnummer für den Computer, auf dem der LDAP-Verzeichnisdienst gehostet wird. In der Regel weist der LDAP-Server die Portnummer 389 auf.
-SearchBase -sb	search base	Erforderlich. Distinguished Name (DN) des Eintrags, der als Ausgangspunkt für die Suche nach Benutzernamen in der LDAP-Verzeichnisstruktur verwendet wird. LDAP findet ein Objekt im Verzeichnis entsprechend dem Pfad im Distinguished Name des Objekts. Beispiel: In Microsoft Active Directory könnte der Distinguished Name des Benutzers cn=UserName,ou=OrganizationalUnit,dc=DomainName lauten, wobei die Reihe der durch dc=DomainName benannten relativen Distinguished Names die DNS-Domäne des Objekts kennzeichnet.
-SearchScope -ss	Suchbereich	Erforderlich. Bereich der Benutzersuche. Wählen Sie eine der folgenden Optionen aus: - Basis. Durchsuchen Sie den durch die Suchbasis gekennzeichneten Eintrag. - Eine Ebene. Durchsuchen Sie alle Einträge eine Ebene unterhalb des Suchbasiseintrags, jedoch ausschließlich des Suchbasiseintrags. - Unterstruktur. Durchsuchen Sie die gesamte Unterstruktur auf allen Ebenen unterhalb des Suchbasiseintrags.
-LDAPPrincipal -lp	ldap_principal	Erforderlich. Distinguished Name (DN) für den Prinzipal-Benutzer. Der Benutzername besteht häufig aus einem allgemeinen Namen (Common Name, CN), einer Organisation (Organization, O) und einem Land (Country, C). Der Name des Prinzipal-Benutzers bezeichnet einen Administratorbenutzer mit Zugriff auf das Verzeichnis und ist nicht der zu authentifizierende Name. Geben Sie einen Benutzer an, der über die Berechtigung zum Lesen anderer Benutzereinträge auf dem LDAP-Server verfügt. Lassen Sie diese Option aus, um sich als anonymer Benutzer anzumelden. Weitere Informationen erhalten Sie in der LDAP-Serverdokumentation.
-LDAPCredential -lc	ldap_credential	Erforderlich. Passwort für den Prinzipal-Benutzer. Sie können ein Passwort mit der Option -lc oder der Umgebungsvariable INFA_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -lc festgelegte Passwort Vorrang. Lassen Sie diese Option aus, um sich als anonymer Benutzer anzumelden.
-LoginAttribute -lt	login_attribute	Erforderlich. Verzeichnisattribut, das Anmeldenamen enthält.

Option	Argument	Beschreibung
-LoginFilter -lf	login_filter	Erforderlich. Eine LDAP-Abfragezeichenfolge zum Filtern von Benutzersuchergebnissen. Der Filter kann Attributtypen, Assertionswerte und Vergleichskriterien angeben. Beispiel: (objectclass=*) durchsucht alle Objekte. (&(objectClass=user)(!(cn=susan))) sucht alle Benutzerobjekte außer „susan“. Weitere Informationen zu Suchfiltern erhalten Sie in der LDAP-Serverdokumentation.
-UseSSL -us	use_ssl	Verwenden Sie diese Option nicht. Informatica unterstützt keinen LDAP-Server, der SSL für 8.1.1-Versionen verwendet.
-CertificateDatabase -cd	certificate_database_for_ssl	Verwenden Sie diese Option nicht. Informatica unterstützt keinen LDAP-Server, der SSL für 8.1.1-Versionen verwendet.

ShowLicense

Zeigt Lizenzdetails an. Die angezeigten Lizenzdetails sind ein kumulatives Ergebnis aller angewendeter Lizenzschlüssel. Der Dienstmanager aktualisiert die vorhandenen Lizenzdetails, wenn Sie einen inkrementellen Schlüssel zur Lizenz hinzufügen.

Um den infacmd isp ShowLicense-Befehl auszuführen, müssen Sie über Berechtigungen für die Lizenz verfügen.

Der Befehl „infacmd isp ShowLicense“ verwendet die folgende Syntax:

```
ShowLicense

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-LicenseName|-ln> license_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ShowLicense“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-LicenseName -ln	license_name	Erforderlich. Name der Lizenz.

ShutdownNode

Fährt den Knoten herunter. Nach dem Starten des Knotens können Sie den Knoten neu starten, indem Sie den Informatica-Dienst auf dem Computer starten. Ein Knoten kann unter Verwendung von infacmd gestartet werden.

Der Befehl „infacmd isp ShutdownNode“ verwendet die folgende Syntax:

```
ShutdownNode

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ShutdownNode“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, den Sie herunterfahren möchten.

SwitchToGatewayNode

Konvertiert einen vorhandenen Arbeitsknoten in einen Gateway-Knoten. Die Dienstrolle muss für den Arbeitsknoten aktiviert sein.

Der Befehl „infacmd isp SwitchToGatewayNode“ verwendet die folgende Syntax:

```
SwitchToGatewayNode

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name

[<-AdminconsolePort|-ap> admin_tool_port]
```

```
[<-AdminconsoleShutdownPort|-asp> admin_tool_shutdown_port]

<-LogServiceDirectory|-ld> log_service_directory

[<-DatabaseTruststorePassword|-dbtp> database_truststore_password]

[<-DatabaseTruststoreLocation|-dbtl> database_truststore_location]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp SwitchToGatewayNode“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, den Sie in einen Gateway-Knoten umwandeln möchten.
-AdminconsolePort -ap	admin_tool_port	Port für den Zugriff auf Informatica Administrator.
-AdminconsoleShutdownPort -asp	admin_tool_shutdown_port	Portnummer, die das Herunterfahren für Informatica Administrator steuert.
-LogServiceDirectory -ld	log_service_directory	Erforderlich. Freigegebener Verzeichnispfad, der vom Protokollmanager zum Speichern von Protokollereignisdateien verwendet wird.
-DatabaseTruststorePassword -dbtp	database_truststore_password	Optional. Passwort für die Datenbank-Truststore-Datei für die sichere Datenbank. Erforderlich, wenn Sie eine sichere Domänenrepository-Datenbank für die Domäne konfigurieren.
-DatabaseTruststoreLocation -dbtl	database_truststore_location	Pfad und Dateiname der Truststore-Datei für die sichere Datenbank Erforderlich, wenn Sie eine sichere Domänenrepository-Datenbank für die Domäne konfigurieren.

SwitchToWorkerNode

Wandelt einen Gateway-Knoten in einen Arbeitsknoten um. Der Befehl schlägt fehl, wenn der zu wechselnde Knoten der einzige Gateway-Knoten in der Domäne ist.

Wenn der Knoten als Master-Gateway-Knoten dient, müssen Sie ihn herunterfahren, bevor Sie ihn in einen Arbeitsknoten umwandeln können. Fahren Sie den Knoten herunter und warten Sie darauf, dass das Master-Gateway zur Ausfallsicherung an einen anderen Knoten übergeben wird. Sie können den Knoten dann neu starten und den infacmd isp SwitchToWorkerNode-Befehl ausführen.

Der Befehl „infacmd isp SwitchToWorkerNode“ verwendet die folgende Syntax:

```
SwitchToWorkerNode

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password
```

```
[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp SwitchToWorkerNode“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, den Sie in einen Arbeitsknoten umwandeln möchten.

SyncSecurityDomains

Synchronisiert Benutzer und Gruppen in einer Sicherheitsdomäne mit den Benutzern und Gruppen im LDAP-Verzeichnisdienst.

Der Befehl „infacmd isp SyncSecurityDomains“ verwendet die folgende Syntax:

```
SyncSecurityDomains

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-SynchronizingNamespace|-sn> namespace_to_sync
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp SyncSecurityDomain“ beschrieben:

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

Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
<-SynchronizingNamespace -sn	namespace_to_sync	Name der Sicherheitsdomäne, die Sie mit dem LDAP-Verzeichnisdienst synchronisieren möchten.

UnassignDefaultOSProfile

Entfernt das Betriebssystemprofil, das einem Benutzer oder einer Gruppe zugewiesen ist.

Der Befehl „infacmd isp UnassignDefaultOSProfile“ verwendet die folgende Syntax:

```
UnassignDefaultOSProfile
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-RecipientName|-nm> recipient_name
<-RecipientSecurityDomain|-ns> security_domain_of_recipient
<-RecipientType|-ty> recipient_type
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UnassignDefaultOSProfile“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-RecipientName -nm	recipient_name	Erforderlich. Benutzer- oder Gruppenname, der dem Standardbetriebssystemprofil zugewiesen wird.
-RecipientSecurityDomain -ns	security_domain_of_recipient	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden und Benutzerberechtigungen gewähren. Name der Sicherheitsdomäne, zu der der Benutzer gehört.
-RecipientType -ty	recipient_type	Erforderlich. Geben Sie an, ob das Standardbetriebssystemprofil einem Benutzer oder einer Gruppe zugewiesen werden soll. Geben Sie einen der folgenden Werte ein: - UserIdentity - GroupIdentity

UnassignISMMService

Hebt die Verbindung zwischen dem PowerCenter-Integrationsdienst und dem Metadata Manager-Dienst auf. Wenn Sie einen PowerCenter-Integrationsdienst entfernen, müssen Sie einen anderen PowerCenter-Integrationsdienst verbinden, bevor Sie Ressourcen laden.

Der Befehl „infacmd isp UnassignISMMService“ verwendet die folgende Syntax:

```
UnassignISMMService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> securitydomain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-IntegrationService|-is> integration_service_name
```

Die folgende Tabelle beschreibt die Optionen und Argumente für „infacmd isp UnassignISMMService“:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Metadata Manager-Diensts, dessen Zuweisung zum Integrationsdienst aufgehoben werden soll.
-IntegrationService -is	integration_service_name	Erforderlich. Name des Integrationsdiensts, dessen Zuordnung zum Metadata Manager-Dienst Sie aufheben möchten.

UnassignLicense

Entfernt eine Lizenz aus einem Anwendungsdienst. Der Dienst muss gestoppt werden. Nachdem Sie eine Lizenz aus dem Dienst entfernt haben, müssen Sie eine gültige Lizenz zuweisen, um den Dienst erneut zu aktivieren.

Der Befehl „UnassignLicense“ verwendet die folgende Syntax:

```
UnassignLicense

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-LicenseName|-ln> license_name

<-ServiceNames|-sn> service1_name service2_name ...
```

In der folgenden Tabelle werden die Optionen und Argumente für „*infacmd isp* UnassignLicense“ beschrieben:

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

Option	Argumente	Beschreibung
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der *infacmd* versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet *infacmd* den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-LicenseName -ln	license_name	Erforderlich. Name der Lizenz, deren Zuweisung Sie aufheben möchten.
-ServiceNames -sn	service_name1 service_name2 ...	Erforderlich. Namen der Dienste, für die Sie die Lizenz entfernen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

UnassignRoleFromGroup

Entfernt eine Rolle aus einer Gruppe für eine Domäne oder einen Anwendungsdienst.

Der Befehl „infacmd isp UnassignRoleFromGroup“ verwendet die folgende Syntax:

```
UnassignRoleFromGroup

<-DomainName|-dn> domain_name

<-UserName|-un> user_name
```

```
<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-GroupName|-gn> group_name

[<-GroupSecurityDomain|-gsf> group_security_domain]

<-RoleName|-rn> role_name

<-ServiceName|-sn> service_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UnassignRoleFromGroup“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-GroupName -gn	group_name	Erforderlich. Name der Gruppe, aus der Sie eine Rolle entfernen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-GroupSecurityDomain -gsf	group_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der die Gruppe gehört, aus der Sie die Rolle entfernen. Standardwert ist „Native“.
-RoleName -rn	role_name	Erforderlich. Name der Rolle, die Sie aus der Gruppe entfernen möchten.
-ServiceName -sn	service_name	Erforderlich. Domäne oder Anwendungsdienstname, aus der bzw. dem Sie die Rolle entfernen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

UnassignRoleFromUser

Entfernt eine Rolle von einem Benutzer für eine Domäne oder einen Anwendungsdienst.

Der Befehl „infacmd isp UnassignRoleFromUser“ verwendet die folgende Syntax:

```
UnassignRoleFromUser

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ExistingUserName|-eu> existing_user_Name

[<-ExistingUserSecurityDomain|-esd> existing_user_securit

<-RoleName|-rn> role_name

<-ServiceName|-sn> service_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UnassignRoleFromUser“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ExistingUserName -eu	existing_user_Name	Erforderlich. Benutzerkonto, aus dem Sie die Rolle entfernen. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört, dessen Rolle entfernt werden soll. Standardwert ist „Native“.
-RoleName -rn	role_name	Erforderlich. Name der Rolle, die Sie für einen Benutzer entfernen möchten.
-ServiceName -sn	service_name	Erforderlich. Domäne oder Anwendungsdienstname, aus der bzw. dem Sie die Rolle entfernen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

UnassignRSWSHubService

Hebt die Verbindung zwischen einem PowerCenter-Repository und einem Web Services Hub in der Domäne auf.

Der Befehl „infacmd isp UnassignRSWSHubService“ verwendet die folgende Syntax:

```
UnassignRSWSHubService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-NodeName|-nn> node_name

<-RepositoryService|-rs> repository_service_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UnassignRSWSHubService“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des Webdienst-Hubs, von dem Sie ein Repository trennen möchten.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Prozess des Webdienst-Hubs ausgeführt wird. Wenn die Informatica-Umgebung für hohe Verfügbarkeit konfiguriert ist, gibt diese Option den Namen des primären Knotens an.
-RepositoryService -rs	repository_service_name	Erforderlich. Name des Repository-Diensts, von dem der Webdienst-Hub abhängig ist. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

UnassociateDomainNode

Trennen Sie den Knoten in einer Domäne von seiner Adresse. Der Knotenname bleibt Teil der Domäne, aber er hat keine physische Adresse.

In einer Domäne ist z. B. „Node1“ mit dem Computer „MyHost:9090“ verbunden. Wenn Sie diesen Befehl ausführen, wird die Verbindung zwischen dem Namen „Node1“ und der Hostadresse „MyHost:9090“ entfernt. Sie können „Node1“ dann mit einem neuen Host verbinden. Sie müssen den Befehl „infasetup

DefineGatewayNode“ oder „DefineWorkerNode“ auf dem neuen Host ausführen, um „Node1“ auf diesem Computer zu definieren.

Der Befehl „infacmd isp UnassociateDomainNode“ verwendet die folgende Syntax:

```
UnassociateDomainNode

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UnassociateDomainNode“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, den Sie von der Domäne trennen möchten.

UpdateConnection

Aktualisiert eine Verbindung. Führen Sie Verbindung infacmd isp ListConnectionOptions aus, um Verbindungsoptionen aufzulisten.

Der Befehl „infacmd isp UpdateConnection“ verwendet die folgende Syntax:

```
UpdateConnection

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ConnectionName|-cn> connection_name

[<-ConnectionUserName|-cun> connection_user_name]

[<-ConnectionPassword|-cpd> connection_password]
```

```
[-o options] (name-value pairs separated by space)
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateConnection“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ConnectionName -cn	connection_name_security_domain	Erforderlich. Name der zu aktualisierenden Verbindung.
ConnectionUserName -cun	connection_user_name	Erforderlich. Name des Datenbankbenutzers.

Option	Argument	Beschreibung
-ConnectionPassword -cpd	connection_password	Erforderlich. Passwort für den Datenbankbenutzernamen. Wenn Sie eine ADABAS-, DB2I-, DB2Z-, IMS-, SEQ- oder VSAM-Verbindung aktualisieren, müssen Sie eine gültige PowerExchange-Passphrase statt eines Passworts eingeben. Passphrasen für den Zugriff auf Datenbanken und Datasets auf z/OS können zwischen 9 und 128 Zeichen umfassen. Passphrasen für den Zugriff auf DB2 für i5/OS können maximal 31 Zeichen umfassen. Passphrasen können die folgenden Zeichen enthalten: - Groß- und Kleinbuchstaben - Die Zahlen 0 bis 9 - Leerzeichen - Die folgenden Sonderzeichen: `' - ; # \ , . / ! % & * ( ) _ + { } : @ | < > ?` **Hinweis:** Das erste Zeichen ist ein Apostroph. Passphrasen dürfen keine einfachen Anführungszeichen ('), doppelten Anführungszeichen (") oder Währungssymbole enthalten. Wenn eine Passphrase Leerzeichen enthält, müssen Sie sie in doppelte Anführungszeichen einschließen, wie z. B. `„Das ist eine Beispiel-Passphrase"`. Wenn eine Passphrase Sonderzeichen enthält, müssen Sie sie in dreifache doppelte Anführungszeichen einschließen (`"""`), wie z. B. Zeichen `"""Diese Passphrase enthält Sonderzeichen ! % & *."""`. Wenn eine Passphrase nur alphanumerische Zeichen ohne Leerzeichen enthält, können Sie sie ohne Delimiter eingeben. **Hinweis:** Auf z/OS kann eine gültige RACF-Passphrase bis zu 100 Zeichen umfassen. PowerExchange schneidet Passphrasen mit mehr als 100 Zeichen ab, wenn diese zur Validierung an RACF übergeben werden. Stellen Sie vor der Verwendung von Passphrasen sicher, dass der PowerExchange-Listenerdienst im DBMOVER-Mitglied mit der Sicherheitseinstellung SECURITY=(1,N) oder höher ausgeführt wird. Weitere Informationen finden Sie unter „SECURITY-Anweisung" im *PowerExchange-Referenzhandbuch*. Stellen Sie zur Verwendung von Passphrasen für IMS-Verbindungen sicher, dass die folgenden zusätzlichen Anforderungen erfüllt sind: - Sie müssen ODBA-Zugriff auf IMS gemäß der Beschreibung im *PowerExchange Navigator-Benutzerhandbuch* konfigurieren. - Sie müssen IMS-Daten-Maps verwenden, die IMS ODBA als Zugriffsmethode festlegen. Verwenden Sie keine Daten-Maps, die die Zugriffsmethode DL/1 BATCH angeben, da diese Zugriffsmethode

Option	Argument	Beschreibung
		die Verwendung von Netport-Jobs erfordert, die keine Unterstützung für Passphrasen bietet. - Die IMS-Datenbank muss im IMS-Steuerbereich online sein, damit ODBA-Zugriff auf IMS verwendet werden kann.
-Options -o	options	Geben Sie Name-Wert-Paare durch Leerzeichen getrennt ein. Führen Sie zum Anzeigen gültiger Optionen infacmd isp ListConnectionOptions aus.

UpdateDomainOptions

Aktualisiert Domäneneigenschaften. Die Domäneneigenschaften beinhalten Resistenz-Timeout, Grenzwert für Resistenz-Timouts, maximale Neustartversuche, Neustartzeitraum, TLS-Modus und Sendemodus.

Der Befehl „infacmd isp UpdateDomainOptions“ verwendet die folgende Syntax:

```
UpdateDomainOptions

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-DomainOptions|-do> option_name=value ...
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateDomainOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-DomainOptions -do	option_name=value	Erforderlich. Domäneneigenschaften, die Sie aktualisieren möchten. Sie können die folgenden Eigenschaften aktualisieren: - LicenseUsageDetailMinDays. Die Mindestanzahl an Tagen, an denen der Protokollmanager Protokollereignisse für die Lizenznutzung aufbewahrt. - LicenseUsageSummaryMinDays. Die Mindestanzahl an Tagen, an denen der Protokollmanager Datensätze für die Lizenznutzung aufbewahrt. - ResilTimeout. Zeitraum in Sekunden, in dem Dienste versuchen, als Clients eine Verbindung zu anderen Diensten herzustellen. - RestartsMaxAttempts. Anzahl der in einem angegebenen Zeitraum durchgeführten Versuche der Domäne, einen Anwendungsdienstprozess neu zu starten, wenn dieser fehlschlägt. - RestartsWithinSeconds. Maximaler Zeitraum in Sekunden, in dem die Domäne versucht, einen Anwendungsdienstprozess neu zu starten, wenn dieser fehlschlägt. - ServiceResilTimeout. Zeitraum in Sekunden, in dem ein Dienst versucht, eine Verbindung zu einem anderen Dienst herzustellen oder erneut herzustellen. - TaskDispatchMode. Load Balancer-Sendemodus für Aufgaben: RoundRobin, MetricBased oder Adaptive. Starten Sie den Integrationsdienst neu, damit die Änderungen wirksam werden. - TLSMode. Konfiguriert die sichere Kommunikation zwischen Diensten innerhalb der Domäne. Starten Sie die Domäne neu, damit die Änderungen wirksam werden. Gültige Werte sind „true“ oder „false“.

UpdateFolder

Aktualisiert die Ordnerbeschreibung.

Der Befehl „infacmd isp UpdateFolder“ verwendet die folgende Syntax:

```
UpdateFolder

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]
```

```
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-FolderPath|-fp> full_folder_path

<-FolderDescription|-fd> description_of_folder
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateFolder“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-FolderPath -fp	full_folder_path	Erforderlich. Vollständiger Pfad (ohne Domänenname) des Ordners, den Sie aktualisieren möchten. Folgendes Format ist erforderlich: */parent_folder/child_folder*
-FolderDescription -fd	description_of_folder	Erforderlich. Beschreibung des Ordners. Wenn die Ordnerbeschreibung Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie sie in Anführungszeichen.

UpdateGatewayInfo

Aktualisiert die Konnektivitätsinformationen für den Gateway-Knoten in der domains.infa-Datei.

Der infacmd isp UpdateGatewayInfo-Befehl verwendet die folgende Syntax:

```
UpdateGatewayInfo

<-DomainName|-dn> domain_name

<-GatewayAddress|-dg> domain_gateway_host:port

[<-Force|-f>]
```

In der folgenden Tabelle werden infacmd isp UpdateGatewayInfo-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Domäne.
-GatewayAddress -dg	domain_gateway_host:port	Erforderlich. Name und Portnummer des Gateway-Hostcomputers.
-Force -f	-	Optional. Aktualisiert oder erstellt die Datei „domains.infa“ auch dann, wenn die Verbindung zur Domäne fehlschlägt. Die Option -Force legt die Kerberos- und TLS-fähigen Optionen in der Datei „domains.infa“ als „false“ fest, wenn die Verbindung zur Domäne fehlschlägt. Wenn Sie die Option -Force nicht angeben, aktualisiert der Befehl die Datei „domains.infa“ nicht, wenn die Verbindung zur Domäne fehlschlägt.

UpdateGrid

Aktualisiert die Liste der Knoten, die einem Gitter zugewiesen sind.

Der Befehl „infacmd isp UpdateGrid“ verwendet die folgende Syntax:

```
UpdateGrid

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-GridName|-gn> grid_name

<-NodeList|-nl> node1 node2 ...

[<-UpdateNodeList|-ul> true|false]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateGrid“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-GridName -gn	grid_name	Erforderlich. Name des Gitters.
-NodeList -nl	node1 node2 ...	Erforderlich. Namen der Knoten, die Sie dem Gitter zuweisen möchten. Diese Knotenliste ersetzt oder aktualisiert die Liste der zuvor dem Gitter zugewiesenen Knoten auf Basis der definierten Option -ul. Wenn Sie die Option -ul angeben, aktualisiert die Option -nl die Liste der zuvor dem Gitter zugewiesenen Knoten. Wenn Sie die Option -ul nicht angeben, ersetzt die Option -nl die Liste der zuvor dem Gitter zugewiesenen Knoten.
-UpdateNodeList -ul	true|false	Optional. Aktualisiert die aktuelle Knotenliste mit den Werten in der Option -nl, anstatt die Liste der zuvor dem Gitter zugewiesenen Knoten zu ersetzen. Wenn TRUE, aktualisiert infacmd die Knotenliste mit der Liste der Knoten, die mithilfe der Option -nl angegeben wurden, sowie mit den zuvor dem Gitter zugewiesenen Knoten. Wenn FALSE, ersetzt infacmd die Knotenliste mit der Liste der Knoten, die mithilfe der Option -nl angegeben wurden. Standardwert ist „False“.

UpdateIntegrationService

Aktualisiert die Konfigurationseigenschaften für den PowerCenter-Integrationsdienst.

Der Befehl „infacmd isp UpdateIntegrationService“ verwendet die folgende Syntax:

```
UpdateIntegrationService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

[<-NodeName|-nn> node_name|<-GridName|-gn> grid_name]

[<-BackupNodes|-bn> node1 node2 ...]

[<-RepositoryService|-rs> repository_service_name]

[<-RepositoryUser|-ru> repository_user]

[<-RepositoryPassword|-rp> repository_password]

[<-RepositoryUserSecurityDomain|-rsdn> repository_user_security_domain]

[<-ServiceOptions|-so> option_name=value ...]
```

Hinweis: Für infacmd isp UpdateIntegrationService dürfen die Optionen -ru, -rp und -rsdn nicht in der Kerberos-Authentifizierung verwendet werden. Wenn Sie diese Optionen im Kerberos-Modus verwenden, schlägt der Befehl fehl.

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateIntegrationService“ beschrieben:

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

Option	Argument	Beschreibung
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, gilt der während der Installation festgelegte Benutzerbereich als Standardeinstellung.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des Integrationsdiensts. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-NodeName -nn	node_name	Optional. Name des Knotens, auf dem der Integrationsdienstprozess ausgeführt wird. Wenn die PowerCenter-Umgebung für hohe Verfügbarkeit konfiguriert ist, gibt diese Option den Namen des primären Knotens an. Geben Sie keinen Wert für diese Option ein, wenn Sie den Gitternamen angeben.
-GridName -gn	grid_name	Optional. Name des Gitters, in dem der Integrationsdienstprozess ausgeführt wird. Geben Sie keinen Wert für diese Option ein, wenn Sie den Knotennamen angeben.
-BackupNodes -bn	node1 node2 ...	Optional. Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist. Sie können Sicherungsknoten konfigurieren, wenn Sie hohe Verfügbarkeit haben.

Option	Argument	Beschreibung
-RepositoryService -rs	repository_service_name	Optional. Name des Repository-Diensts, von dem der Integrationsdienst abhängig ist. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RepositoryUser -ru	user	Erforderlich für native und LDAP-Authentifizierung. Benutzername zum Herstellen einer Verbindung zum Repository. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-RepositoryPassword -rp	Passwort	Erforderlich für native und LDAP-Authentifizierung. Benutzerpasswort. Sie können ein Passwort mit der Option -rp oder der Umgebungsvariable INFA_REPOSITORY_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -rp festgelegte Passwort Vorrang.
-RepositoryUserSecurityDomain -rsdn	repository_user_security_domain	Erforderlich für LDAP-Authentifizierung. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der PowerCenter-Repository-Benutzer gehört. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn Sie diese Option nicht angeben, setzt der Befehl die Sicherheitsdomäne des Repository-Benutzers auf nativ.
-ServiceOptions -so	option_name=value	Optional. Diensteigenschaften, mit denen definiert wird, wie der PowerCenter-Integrationsdienst ausgeführt wird.

UpdateLicense

Aktualisiert die Lizenzinformationen für die Domäne. Führen Sie diesen Befehl aus, um Ihre Lizenz mit einem inkrementellen Lizenzschlüssel zu aktualisieren. Sie verwenden diesen Schlüssel, um lizenzierte Optionen hinzuzufügen oder zu entfernen.

Wenn Sie einer Lizenz einen inkrementellen Schlüssel hinzufügen, aktualisiert der Dienstmanager das Lizenzablaufdatum, wenn das Ablaufdatum für den inkrementellen Schlüssel nach dem des ursprünglichen Schlüssels liegt.

Der Befehl „infacmd isp UpdateLicense“ verwendet die folgende Syntax:

```
UpdateLicense

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]
```

```
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-LicenseName|-ln> license_name

<-LicenseKeyFile|-lf> license_key_file
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateLicense“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-LicenseName -ln	license_name	Erforderlich. Name des Lizenzobjekts, das Sie aktualisieren möchten.
-LicenseKeyFile -lf	license_key_file	Erforderlich. Name und Pfad der Datei, die den inkrementellen Schlüssel enthält.

UpdateMMService

Aktualisiert oder erstellt die Dienstoptionen für einen Metadata Manager-Dienst. Um die Dienstoptionen zu aktualisieren oder zu erstellen, deaktivieren Sie den Metadata Manager-Dienst, aktualisieren Sie die Optionen und aktivieren Sie den Dienst erneut.

Der Befehl „infacmd isp UpdateMMService“ verwendet die folgende Syntax:

```
UpdateMMService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

[<-LicenseName|-ln> license_name]

<-ServiceOptions|-so> option_name=value ...>
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateMMService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Metadata Manager-Diensts, den Sie aktualisieren möchten.
-LicenseName -ln	license_name	Erforderlich. Name der Lizenz, die Sie dem Metadata Manager-Dienst zuweisen möchten.
-ServiceOptions -so	option_name=value	Optional. Diensteigenschaften, mit denen definiert wird, wie der Metadata Manager-Dienst ausgeführt wird.

UpdateMonitoringOptions

Aktualisiert die allgemeinen Eigenschaften, um Aktionen in der Domäne zu überwachen.

Wenn Sie einen Modellrepository-Dienst mit der Option -ModelRepositoryService festlegen, müssen Sie auch Werte für die Optionen -RepositoryUserName und -RepositoryPassword eingeben. Sie müssen Werte für alle drei oder für keine der Optionen angeben.

Der Befehl infacmd isp UpdateMonitoringOptions verwendet die folgende Syntax:

```
UpdateMonitoringOptions

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-ModelRepositoryService|-rs> model_repository_service]

[<-RepositoryUserName|-rsun> model_repository_user_name]

[<-RepositoryPassword|-rspd> model_repository_password]

[<-RepositorySecurityDomain|-rsdn> model_repository_security_domain]

[<-AdministratorOptions|-ao> option_name=value ...(MaxSortedRecords, ShowMilliSeconds)]

[<-CachingOption|-co> option_name=value ...(DefaultNotificationDelay)]

[<-PurgeOptions|-po> option_name=value ...(PurgeScheduleTime, PurgeTaskFrequency,
StatisticsExpiryTime, DetailedStatisticsExpiryTime)]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateMonitoringOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, gilt der während der Installation festgelegte Benutzerbereich als Standardeinstellung.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Anzahl der Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang. Standardwert ist 180 Sekunden.
-ModelRepositoryService -rs	model_repository_service	Optional. Name des Modellrepository-Diensts, der die Verlaufsdaten speichert.
-RepositoryUserName -rsun	model_repository_user_name	Erforderlich für native und LDAP-Authentifizierung. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Benutzername zum Zugriff auf den Modellrepository-Dienst.
-RepositoryPassword -rspd	model_repository_password	Erforderlich für native und LDAP-Authentifizierung. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Benutzerpasswort zum Zugriff auf den Modellrepository-Dienst.
-RepositorySecurityDomain -rsdn	model_repository_security_domain	Erforderlich für LDAP- oder Kerberos-Authentifizierung. Optional, wenn in der Domäne native Authentifizierung verwendet wird. Name der Sicherheitsdomäne, zu der der Benutzer des PowerCenter-Repositorys gehört. Bei der Sicherheitsdomäne wird die Groß-/Kleinschreibung beachtet. Wenn Sie diese Option nicht angeben, setzt der Befehl die Sicherheitsdomäne des Repository-Benutzers auf nativ.
-AdministratorOptions -ao	option_name=value	Optional. Allgemeine Verwaltungseinstellungen für Datensätze und Überwachungsberichte. Sie können die folgenden Optionen einrichten: - MaxSortedRecords. Maximale Anzahl der Datensätze, die sortiert werden können. Standardwert ist 3.000. - ShowMilliseconds. Einschließlich Millisekunden für Datums- und Uhrzeitfeld in Überwachungsberichten. Kann auf „True“ oder „False“ eingestellt werden. Standardwert ist „False“.

Option	Argument	Beschreibung
-CachingOption -co	option_name=value	Optional. Einstellungen für das Zwischenspeichern von Statistiken. Sie können die folgenden Optionen einrichten: - DefaultNotificationDelay. Maximale Anzahl der Sekunden, die der Datenintegrationsdienst die Statistiken puffert, bevor er die Statistiken im Modellrepository beibehält und sie in einen Überwachungsbericht schreibt. Standardwert ist 10.
-PurgeOptions -po	option_name=value	Optional. Einstellungen für das Bereinigen von Statistiken. Sie können die folgenden Optionen einrichten: - PurgeScheduleTime. Uhrzeit, zu der der Modellrepository-Dienst Statistiken bereinigt. Standardwert ist 1:00 morgens. - PurgeTaskFrequency. Intervall in Tagen, in dem der Modellrepository-Dienst Statistiken bereinigt, die älter als die für die ExpiryTime-Optionen konfigurierten Werte sind. Standardwert ist 1. - StatisticsExpiryTime. Anzahl an Tagen, die das Modellrepository gemittelte Statistiken speichert. Wenn die Bereinigung deaktiviert ist, werden die Statistiken unbegrenzt im Modellrepository gespeichert. Standardwert ist 180. Minimalwert ist 0. Maximalwert ist 366. - DetailedStatisticsExpiryTime. Anzahl an Tagen, die das Modellrepository minutengenaue Statistiken speichert. Wenn die Bereinigung deaktiviert ist, werden die Statistiken unbegrenzt im Modellrepository gespeichert. Standardwert ist 14. Minimalwert ist 1. Maximalwert ist 14.

UpdateNamespace

Aktualisiert eine LDAP-Sicherheitsdomäne mit den Filtern für den Benutzer und die Gruppe. Aktualisiert die LDAP-Sicherheitsdomäne, wenn die Informatica-Domäne LDAP oder die Kerberos-Authentifizierung verwendet.

Der Befehl „infacmd isp UpdateNamespace“ verwendet die folgende Syntax:

```
UpdateNamespace

 <-DomainName|-dn> domain_name

 <-UserName|-un> user_name

 <-Password|-pd> password

 [<-SecurityDomain|-sdn> security_domain]

 [<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

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

```
<-NameSpace|-ns> namespace
[<-UserSearchBase|-usb> usersearchbase]
[<-UserFilter|-uf> userfilter]
[<-GroupSearchBase|-gsb> groupsearchbase]
[<-GroupFilter|-gf> groupfilter]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateNamespace“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Sie können einen Wert für -sdn angeben oder den Standardwert basierend auf dem Authentifizierungsmodus verwenden: - Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Standardwert ist „Native". Zum Arbeiten mit der LDAP-Authentifizierung müssen Sie den Wert für -sdn angeben. - Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Standardwert ist „Native" für native Authentifizierung. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa" veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn Sie die Umgebungsvariable nicht angeben, wird der Standardwert von 180 Sekunden verwendet.
-NameSpace -ns	namespace	Erforderlich. Name der LDAP- oder Kerberos-Sicherheitsdomäne. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf weder Leerzeichen noch folgende Sonderzeichen enthalten: , + / < > @ ; \ % ? Der Name darf nicht länger als 128 Zeichen sein. Der Name kann ein ASCII-Leerzeichen enthalten, jedoch nicht als erstes oder letztes Zeichen. Sie können keine anderen Leerzeichen verwenden.
-UserSearchBase -usb	usersearchbasesu	Distinguished Name (DN) des Eintrags, der als Ausgangspunkt für die Suche nach Benutzernamen im LDAP-Verzeichnisdienst dient. Der LDAP-Verzeichnisdienst sucht nach einem Objekt im Verzeichnis entsprechend dem Pfad im Distinguished Name des Objekts. Beispiel: In Microsoft Active Directory könnte der Distinguished Name des Benutzers cn=UserName,ou=OrganizationalUnit,dc=DomainName lauten. Die Reihe der durch dc=DomainName benannten relativen Distinguished Names kennzeichnet die DNS-Domäne des Objekts.

Option	Argument	Beschreibung
-UserFilter -uf	userfilter	Ein LDAP-Abfragestring, der die Suchkriterien für die Suche nach Benutzern im Verzeichnisdienst festgelegt. Der Filter kann Attributtypen, Assertionswerte und Abgleichkriterien angeben. Beispiel: Der Filter `(objectclass=*)` sucht alle Objekte. Der Filter `(&(objectClass=user)(!(cn=susan)))` sucht alle Benutzerobjekte außer „susan“. Weitere Informationen über Suchfilter finden Sie in der Dokumentation für den LDAP-Verzeichnisdienst:
-GroupSearchBase -gsb	groupsearchbase	Distinguished Name (DN) des Eintrags, der als Ausgangspunkt für die Suche nach Gruppennamen im LDAP-Verzeichnisdienst dient.
-GroupFilter -gf	groupfilter	Ein LDAP-Abfragestring, der die Kriterien für die Suche nach Gruppen im Verzeichnisdienst festgelegt.

UpdateNodeOptions

Aktualisiert allgemeine Knoteneigenschaften, wie z. B. das Backup-Verzeichnis, das CPU-Profil, die Fehlerschweregradstufe, Dienstprozessports und Ressourcenbereitstellungsgrenzen.

Der Befehl „infacmd isp UpdateNodeOptions“ verwendet die folgende Syntax:

```
UpdateNodeOptions

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name

[<-NodeOptions|-no> option_name=value ...]

[<-ResourceProvision|-rp> option_name=value ...]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateNodeOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-NodeName -nn	node_name	Optional. Name des Knotens, dessen Ressourcenbereitstellungsgrenzen aktualisiert werden sollen.
-NodeOptions -no	option_name=value	Optional. Die Knotenoptionen, die Sie aktualisieren möchten. Sie können die folgenden Optionen aktualisieren: - BackupDir. Verzeichnis zum Speichern der Repository-Backup-Dateien. - CPUProfile. Einstufung der CPU-Leistung des Knotens im Vergleich zum Baseline-System. ErrorSeverityLevel. Level der Fehlerprotokollierung für den Knoten: error, warning, info, trace, debug. - MaxProcessPort. Höchste von den Dienstprozessen auf dem Knoten verwendete Portnummer. - MinProcessPort. Niedrigste von den Dienstprozessen auf dem Knoten verwendete Portnummer. Das folgende Beispiel legt MaxProcessPort auf 1515 fest: `infacmd UpdateNodeOptions ... -no MaxProcessPort=1515`
-ResourceProvision -rp	option_name=value	Optional. Die Ressourcenbereitstellungsgrenzen, die Sie aktualisieren möchten. Sie können die folgenden Schwellenwerte aktualisieren: - MaxCPURunQueueLength. Die maximale Anzahl an ausführbaren Threads, die auf CPU-Ressourcen auf dem Knoten warten. - MaxMemoryPercent. Der maximale Prozentsatz des virtuellen Speichers, der auf dem Knoten relativ zur Gesamtgröße des physischen Speichers zugeordnet ist. - MaxProcesses. Die maximale Anzahl an Sitzungs- und Befehlsaufgaben, die in jedem auf dem Knoten ausgeführten Integrationsdienst ausgeführt werden können. Das folgende Beispiel legt MaxProcesses auf 15 fest: `infacmd UpdateNodeOptions ... -rp MaxProcesses=15`

UpdateNodeRole

Aktualisiert die Rolle auf einem Knoten in der Domäne. Sie können die Dienst- oder Berechnungsrolle auf einem Knoten aktivieren oder deaktivieren.

Standardmäßig verfügt jeder Knoten sowohl über die Dienstrolle als auch die Berechnungsrolle. Wenn ein Knoten einem Datenintegrationsdienst-Gitter zugewiesen wird, können Sie die Knotenrolle bei Bedarf aktualisieren. Aktivieren Sie nur die Dienstrolle, wenn der Knoten den Datenintegrationsdienst-Prozess ausführen soll. Aktivieren Sie nur die Berechnungsrolle, wenn der Knoten Datenintegrationsdienst-Mappings ausführen soll.

Wenn Sie die Rolle auf einem Knoten aktualisieren, der einem Datenintegrationsdienst oder einem Datenintegrationsdienstgitter zugewiesen ist, müssen Sie den Datenintegrationsdienst recyceln, damit die Änderungen wirksam werden.

Der infacmd isp UpdateNodeRole-Befehl verwendet die folgende Syntax:

```
UpdateNodeRole

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name

[<-EnableServiceRole|-esr> true|false]

[<-EnableComputeRole|-ecr> true|false]

[<-disableComputeRoleMode|-mo> disable_mode]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateNodeRole“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeName -nn	node_name	Erforderlich. Name des zu aktualisierenden Knotens.
-EnableServiceRole -esr	true | false	Optional. Aktiviert die Dienstrolle auf dem Knoten. Bei „True“ können Anwendungsdienste auf dem Knoten ausgeführt werden. Bei „False“ können Anwendungsdienste nicht auf dem Knoten ausgeführt werden. Legen Sie den Befehl nur auf „False“ fest, wenn der Knoten einem Datenintegrationsdienst-Gitter zugewiesen ist und Sie den Knoten für ausgeführte Mappings dedizieren möchten. Standardwert ist „True“.

Option	Argument	Beschreibung
-EnableComputeRole -esr	true | false	Optional. Aktiviert die Berechnungsrolle auf dem Knoten. Bei „True“ kann der Knoten Berechnungen durchführen, die von Remote-Anwendungsdiensten angefragt werden. Bei „False“ kann der Knoten keine von Remote-Anwendungsdiensten angefragten Berechnungen durchführen. Für einen Knoten ist die Berechnungsrolle erforderlich, wenn der Datenintegrationsdienst Jobs auf diesem Knoten ausführt. Wenn der Datenintegrationsdienst auf diesem Knoten keine Jobs ausführt, können Sie die Berechnungsrolle deaktivieren. Eine aktivierte oder deaktivierte Berechnungsrolle hat allerdings keine Auswirkungen auf die Leistung. Standardwert ist „True“.
-disableComputeRoleMode -mo	disable_mode	Optional. Legt fest, wie die Berechnungsrolle deaktiviert wird: - Abschließen. Berechnungen können abgeschlossen werden, bevor die Berechnungsrolle deaktiviert wird. - Stoppen. Stoppt alle laufenden Berechnungen und deaktiviert dann die Berechnungsrolle. - Abbrechen. Versucht, alle laufenden Berechnungen vor deren Abbruch und der Deaktivierung der Berechnungsrolle zu stoppen. Standardwert ist „Abbrechen“.

UpdateOSProfile

Aktualisiert Eigenschaften für ein Betriebssystemprofil in der Domäne.

Hinweis: Um Arbeitsabläufe auszuführen, die Betriebssystemprofile verwenden, benötigen Sie die Betriebssystemprofil-Option.

Der Befehl „infacmd isp UpdateOSProfile“ verwendet die folgende Syntax:

```
UpdateOSProfile

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-OSProfileName|-on> OSProfile_name

[<-IntegrationServiceProcessOptions|-po> option_name=value ...
[<-DISProcessVariables|-diso> option_name=value ...]

[<-DISEnvironmentVariables|-dise> name=value ...]

[<-HadoopImpersonationProperties|-hipr> hadoop_impersonation_properties]

[<-HadoopImpersonationUser|-hu> hadoop_impersonation_user]
```

```
[<-UseLoggedInUserAsProxy|-ip> use_logged_in_user_as_proxy]

[<-ProductExtensionName|-pe> product_extension_name]

[<-ProductOptions|-o> optionGroupName.optionName=Value ...]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateOSProfile“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-OSProfileName -on	OSProfile_name	Erforderlich. Name des Betriebssystemprofils.
-IntegrationServiceProcessOptions -po	option_name=value	Optional. Dienstprozesseigenschaften, mit denen definiert wird, wie der PowerCenter-Integrationsdienst ausgeführt wird.
-EnvironmentVariables -ev	name=value	Optional. Name und Wert von Umgebungsvariablen, die vom PowerCenter-Integrationsdienst zur Laufzeit verwendet werden.
-DISProcessVariables -diso	option_name=value	Optional. Dienstprozesseigenschaften, mit denen definiert wird, wie der Datenintegrationsdienst ausgeführt wird.
-DISEnvironmentVariables -dise	name=value	Optional. Name und Wert von Umgebungsvariablen, die vom Datenintegrationsdienst zur Laufzeit verwendet werden.

Option	Argument	Beschreibung
-HadoopImpersonationProperties -hipr	hadoop_impersonation_properties	Optional. Gibt an, ob der Datenintegrationsdienst den Hadoop-Identitätswechselbenutzer zum Ausführen von Mappings, Arbeitsabläufen und Profiling-Aufträgen in einer Hadoop-Umgebung verwendet. Gültige Werte sind „True“ oder „False“.
-HadoopImpersonationUser -hu	hadoop_impersonation_user	Optional. Geben Sie einen Benutzernamen für den Datenintegrationsdienst zum Identitätswechsel an, wenn er einen Auftrag in einer Hadoop-Umgebung ausführt.
-UseLoggedInUserAsProxy -ip	use_logged_in_user_as_proxy	Optional. Gibt an, ob der angemeldete Benutzer als Hadoop-Identitätswechselbenutzer verwendet werden soll. Gültige Werte sind „True“ oder „False“.
-ProductExtensionName -pe	product_extension_name	Optional. Für zukünftige Verwendung reserviert.
-ProductOptions -o	optionGroupName.optionName=Value	Optional. Für zukünftige Verwendung reserviert.

UpdateRepositoryService

Aktualisiert oder erstellt Dienstoptionen für den PowerCenter-Repository-Dienst.

Sie können z. B. den Betriebsmodus des PowerCenter-Repository-Diensts aktualisieren und auf „normal“ oder „exklusiv“ festlegen. Im normalen Modus können mehrere Benutzer auf den PowerCenter-Repository-Dienst zugreifen und Repository-Inhalte aktualisieren. Im exklusiven Modus kann ein einzelner Benutzer auf den PowerCenter-Repository-Dienst zugreifen und Repository-Inhalte aktualisieren. Legen Sie den Betriebsmodus auf exklusiv fest, wenn Sie Verwaltungsaufgaben durchführen, die erfordern, dass sich ein einzelner Benutzer anmeldet und die Konfiguration aktualisiert. Um den Betriebsmodus des PowerCenter-Repository-Diensts zu aktualisieren, deaktivieren Sie den PowerCenter-Repository-Dienst, aktualisieren Sie den Betriebsmodus und aktivieren Sie den PowerCenter-Repository-Dienst dann erneut.

Der Befehl „infacmd isp UpdateRepositoryService“ verwendet die folgende Syntax:

```
UpdateRepositoryService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

[<-NodeName|-nn> node_name]
```

```
[<-BackupNodes|-bn> node1 node2 ...]

[<-ServiceOptions|-so> option_name=value ...]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateRepositoryService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des zu aktualisierenden PowerCenter-Repository-Diensts. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-NodeName -nn	node_name	Optional. Name des Knotens, auf dem der PowerCenter-Repository-Dienstprozess ausgeführt wird. Wenn die PowerCenter-Umgebung für hohe Verfügbarkeit konfiguriert ist, gibt diese Option den Namen des primären Knotens an.
-BackupNodes -bn	node1 node2 ...	Optional. Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist. Sie können Sicherungsknoten konfigurieren, wenn Sie hohe Verfügbarkeit haben.
-ServiceOptions -so	option_name=value	Erforderlich. Diensteigenschaften, mit denen definiert wird, wie der PowerCenter-Repository-Dienst ausgeführt wird.

Repository-Dienst-Optionen (-so)

Geben Sie Repository-Dienst-Optionen im folgenden Format ein:

```
infacmd CreateRepositoryService ... -so option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Repository-Dienst-Optionen beschrieben:

Option	Beschreibung
AllowWritesWithRACaching	Optional. Verwendet PowerCenter Client-Tools zum Ändern von Metadaten im Repository, wenn „RepAgent cachen“ aktiviert ist. Standardwert ist „Ja“.
CheckinCommentsRequired	Optional. Beim Einchecken von Repository-Objekten müssen Benutzer Kommentare hinzufügen. Standardwert ist „Ja“. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
CodePage	Erforderlich. Codepage-Beschreibung für die Datenbank. Zur Eingabe einer Codepage, die ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
ConnectString	Erforderlich. Die während der Einrichtung des PowerCenter-Repository-Diensts angegebene Datenbankverbindungszeichenfolge. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.

Option	Beschreibung
DBPassword	Erforderlich. Repository-Datenbankpasswort für den Datenbankbenutzer. Sie können ein Passwort mit der Option -so oder der Umgebungsvariable INFA_DEFAULT_DATABASE_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -so festgelegte Passwort Vorrang. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
DBPoolExpiryThreshold	Optional. Die Mindestanzahl an inaktiven Datenbankverbindungen, die im PowerCenter-Repository-Dienst zulässig sind. Beispiel: Wenn 20 inaktive Verbindungen vorhanden sind und Sie diesen Schwellenwert auf 5 festlegen, schließt der PowerCenter-Repository-Dienst höchstens 15 Verbindungen. Die Mindestanzahl beträgt 3. Standardwert ist 5.
DBPoolExpiryTimeout	Optional. Der Zeitraum in Sekunden, in dem der PowerCenter-Repository-Dienst nach inaktiven Datenbankverbindungen sucht. Ist eine Verbindung für einen Zeitraum inaktiv, der diesen Wert überschreitet, kann der PowerCenter-Repository-Dienst die Verbindung schließen. Der Mindestwert beträgt 300. Der Höchstwert beträgt 2.592.000 (30 Tage). Standardwert ist 3.600 (1 Stunde).
DBUser	Erforderlich. Konto für die Datenbank, die das Repository enthält. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
DatabaseArrayOperationSize	Optional. Anzahl der Zeilen, die bei jedem Array-Datenbankvorgang abgerufen werden, beispielsweise Einfügen oder Abrufen. Standardwert ist 100. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
DatabaseConnectionTimeout	Optional. Zeitraum in Sekunden, in dem der PowerCenter-Repository-Dienst versucht, eine Verbindung zum Datenbankverwaltungssystem herzustellen. Standardwert ist 180.
DatabasePoolSize	Optional. Maximale Anzahl der Verbindungen zur Repository-Datenbank, die der PowerCenter-Repository-Dienst herstellen kann. Der Mindestwert beträgt 20. Standardwert ist 500.
DatabaseType	Erforderlich. Typ der Datenbank, die die Repository-Metadaten speichert. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
EnableRepAgentCaching	Optional. Aktiviert die Funktion „Repository Agent Caching“. Standardwert ist „Ja“.
ErrorSeverityLevel	Optional. Mindestebene der Fehlermeldungen, die in das PowerCenter-Repository-Dienstprotokoll geschrieben werden: - Fatal - Fehler Warnung - Info - Trace - Debug Der Standardwert lautet „Info“.
HeartBeatInterval	Optional. Zeitraum, in dem der PowerCenter-Repository-Dienst seine Verbindungen zu den Clients in diesem Dienst überprüft. Standardwert ist 60 Sekunden.

Option	Beschreibung
MaxResilienceTimeout	Optional. Maximaler Zeitraum in Sekunden, in dem der Dienst die Ressourcen zwecks Belastbarkeit beibehält. Standardwert ist 180.
MaximumConnections	Optional. Maximale Anzahl der Verbindungen, die das Repository von den Repository-Clients akzeptiert. Standardwert ist 200.
MaximumLocks	Optional. Maximale Anzahl an Sperren, die das Repository für Metadatenobjekte verwendet. Standardwert ist 50.000.
OperatingMode	Optional. Modus, in dem der PowerCenter-Repository-Dienst ausgeführt wird: - Normal - Exklusiv Standardwert ist „Normal“. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
OptimizeDatabaseSchema	Optional. Optimiert das Repository-Datenbankschema beim Erstellen von Repository-Inhalten oder Sichern und Wiederherstellen eines IBM DB2- oder Microsoft SQL Server-Repositorys. Bei Aktivierung versucht der PowerCenter-Repository-Dienst Repository-Tabellen zu erstellen, die Varchar-Spalten mit einer Genauigkeit von 2000 anstelle von CLOB-Spalten enthalten. Verwenden Sie Varchar-Spalten, um die Leistung des Repositorys zu steigern. Bei Verwendung von Varchar-Spalten verringern Sie die Festplatteneingabe und -ausgabe und die Datenbank kann die Spalten zwischenspeichern. Um diese Option zu verwenden, überprüfen Sie die Anforderungen an die Seitengröße für die folgenden Repository-Datenbanken: - IBM DB2. Datenbank-Seitengröße 4 KB oder größer. Mindestens einen temporären Tablespace mit einer Seitengröße von mindestens 16 KB. - Microsoft SQL Server. Datenbank-Seitengröße 8 KB oder größer. Standardwert ist „Deaktiviert“.
PreserveMXData	Optional. Behält MX-Daten für frühere Versionen von Zuordnungen bei. Standardwert ist „Deaktiviert“.
RACacheCapacity	Optional. Anzahl der Objekte, die der Cache bei aktiviertem Repository Agent Caching enthalten kann. Standardwert ist 10.000.
SecurityAuditTrail	Optional. Verfolgt Änderungen, die an Benutzern, Gruppen und Berechtigungen vorgenommen wurden. Standardwert ist „Nein“.
ServiceResilienceTimeout	Optional. Zeitraum in Sekunden, in dem der Dienst versucht, eine Verbindung zu einem anderen Dienst herzustellen oder erneut herzustellen. Standardwert ist 180. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
TableOwnerName	Optional. Name des Eigentümers der Repository-Tabellen für ein IBM DB2-Repository.
TablespaceName	Optional. Tablespace-Name für IBM DB2-Repositorys. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.
TrustedConnection	Optional. Verwendet Windows-Authentifizierung, um auf die Microsoft SQL Server-Datenbank zuzugreifen. Standardwert ist „Nein“. Starten Sie den PowerCenter-Repository-Dienst neu, um die Änderungen zu übernehmen.

UpdateSAPBWService

Aktualisiert den Dienst und die Dienstprozessoptionen für den SAP BW-Dienst.

Der Befehl „infacmd isp UpdateSAPBWService“ verwendet die folgende Syntax:

```
UpdateSAPBWService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

[<-NodeName|-nn> node_name]

[<-ServiceOptions|-so> option_name=value ...]

[<-ServiceProcessOptions|-po> option_name=value ...]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateSAPBWService“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Name des SAP BW-Diensts erforderlich. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-NodeName -nn	node_name	Optional. Name des Knotens, auf dem der SAP BW-Dienstprozess ausgeführt wird. Wenn die PowerCenter-Umgebung für hohe Verfügbarkeit konfiguriert ist, gibt diese Option den Namen des primären Knotens an.
-ServiceOptions -so	option_name=value	Optional. Diensteigenschaften, mit denen definiert wird, wie der SAP BW-Dienst ausgeführt wird.
-ServiceProcessOptions -po	option_name=value	Optional. Dienstprozesseigenschaften, mit denen definiert wird, wie der SAP BW-Dienstprozess ausgeführt wird.

UpdateServiceLevel

Aktualisiert die Eigenschaften der Dienstebene. Sie können die Dispatch-Priorität und die maximale Dispatch-Wartezeit aktualisieren.

Der Befehl „infacmd isp UpdateServiceLevel“ verwendet die folgende Syntax:

```
UpdateServiceLevel

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceLevelName|-ln> service_level_name

<-ServiceLevel|-sl> option_name=value ...
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateServiceLevel“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceLevelName -ln	service_level_name	Erforderlich. Name der Dienstebene, die Sie aktualisieren möchten.
-ServiceLevel -sl	option_name=value	Erforderlich. Die Eigenschaften der Dienstebene, die Sie aktualisieren möchten. Sie können die folgenden Eigenschaften aktualisieren: - DispatchPriority. Die anfängliche Priorität für den Versand. Kleinere Zahlen haben höhere Priorität. Priorität 1 ist die höchste Priorität. - MaxDispatchWaitTime. Der Zeitraum in Sekunden, bevor der Load Balancer die Dispatch-Priorität für eine Aufgabe in die höchste Priorität eskaliert.

UpdateServiceProcess

Aktiviert die Werte der PowerCenter-Integrationsdienst-Prozessoptionen.

Der Befehl „infacmd isp UpdateServiceProcess“ verwendet die folgende Syntax:

```
UpdateServiceProcess

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password
```

```
[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-NodeName|-nn> node_name

<-ServiceProcessOptions|-po> option_name=value
[<-ProcessEnvironmentVariables|-ev> option_name=value ...]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateServiceProcess“ beschrieben:

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

Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des Diensts. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem Sie Konfigurationsinformationen aktualisieren möchten.
-ServiceProcessOptions -po	option_name=value	Name und neue Werte der Optionen, deren Werte Sie aktualisieren möchten. Sie können mehrere option_name=value-Paare angeben. Sie können eine Prozessvariable im Wert verwenden. Zum Beispiel legt der folgende Befehl das Cache-Verzeichnis auf „$PMRootDir/NewCache“ und das Verzeichnis der Ablehnungsdatei auf „$PMRootDir/NewBadFiles“ fest. `infacmd UpdateServiceProcess ... -po $PMCacheDir=$PMRootDir/NewCache $PMBadFileDir=$PMRootDir/NewBadFiles` Erforderlich, wenn Sie ProcessEnvironmentVariables nicht angeben.
-ProcessEnvironmentVariables -ev	option_name=value	Umgebungsvariablen für den Dienstprozess. Sie können mehrere Umgebungsvariablen angeben. Zum Beispiel fügt der folgende Befehl das JAVA_HOME-Verzeichnis zu „$HOME/java“ und das INFA_HOME-Verzeichnis zu „$HOME/Informatica/9.0.1/install“ für den angegebenen Dienstprozess hinzu oder aktualisiert die Verzeichnisse entsprechend. `infacmd ProcessEnvironmentVariables ... -ev JAVA_HOME=$HOME/java INFA_HOME=$HOME/Informatica/9.0.1/install` Erforderlich, wenn Sie ServiceProcessOptions nicht angeben.

UpdateSMTPOptions

Aktualisiert die SMTP-Konfiguration der Domäne. Die SMTP-Konfiguration dient zum Senden von Domänenwarnungen und Scorecard-Benachrichtigungen.

Nach dem Konfigurieren der SMTP-Einstellungen müssen Sie mit dem AddAlertUser-Befehl Alarme für den Benutzer abonnieren.

Der infacmd isp UpdateSMTPOptions-Befehl verwendet die folgende Syntax:

```
UpdateSMTPOptions

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-SMTPAddress|-sa> smtp_server_address

[<-SMTPUsername|-su> user_name]

[<-SMTPPassword|-sp> password]

[<-SMTPSenderAddress|-ss> sender_email_address]
```

In der folgenden Tabelle werden infacmd isp UpdateSMTPOptions-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.
-Password -pd	password	Erforderlich. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Bei der Sicherheitsdomäne wird die Groß-/Kleinschreibung beachtet. Standardwert ist „Nativ“.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-SMTPAddress -sa	SMTP_server_address	Erforderlich. Der Hostname und die Portnummer für den ausgehenden SMTP-Mailserver. Geben Sie diese Informationen in folgendem Format ein: *host_name:port_number*
-SMTPUserName -su	user_name	Benutzername für die Authentifizierung beim Senden, wenn dies vom ausgehenden Mailserver gefordert wird.
-SMTPPassword -sp	password	Benutzerpasswort für die Authentifizierung beim Senden, wenn dies vom ausgehenden Mailserver gefordert wird. Sie können ein Passwort mit der Option -sp oder der Umgebungsvariable INFA_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -sp festgelegte Passwort Vorrang.
-SMTPSenderAddress -ss	sender_email_address	Optional. Die vom Dienstmanager zum Senden von Benachrichtigungs-E-Mails verwendete E-Mail-Adresse. Wenn Sie dieses Feld leer lassen, verwendet der Dienstmanager den Standardwert „Administrator@<host>“ als Senderadresse.

Verwandte Themen:

- “AddAlertUser” auf Seite 242

UpdateWSHubService

Aktualisiert einen Web Services Hub in der Domäne.

Der Befehl „infacmd isp UpdateWSHubService“ verwendet die folgende Syntax:

```
UpdateWSHubService
```

```
<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

[<-NodeName|-nn> node_name]

[<-ServiceOptions|-so> option_name=value ...]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateWSHubService“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des Webdienst-Hubs, den Sie aktualisieren möchten.
-NodeName -nn	node_name	Optional. Name des Knotens, auf dem der Prozess des Webdienst-Hubs ausgeführt wird.
-ServiceOptions -so	option_name=value ...	Optional. Diensteigenschaften, mit denen definiert wird, wie der Webdienst-Hub ausgeführt wird.

validateFeature

Validiert, dass die Funktion in der angegebenen Plug-In-Datei in der Domäne registriert ist.

Der Befehl „infacmd isp validateFeature“ verwendet die folgende Syntax:

```
validateFeature

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
```

```
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-FeatureFilename|-ff> feature_filename
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp validateFeature“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Gateway-Konnektivitätsinformationen in der Datei „domains.infa“ veraltet sind. Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie den Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-FeatureFilename -ff	feature_filename	Erforderlich. Pfad und Dateiname der Plug-In-XML-Datei der registrierten Funktion, die Sie validieren möchten.

Version

Zeigt die PowerCenter-Version, die Marke Informatica sowie Urheberrechtsinformationen an.

Der version-Befehl verwendet die folgende Syntax:

```
infacmd version
```

KAPITEL 15

infacmd ldm-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- BackupData, 658
- CreateService, 660
- ListServiceOptions, 667
- restoreData, 669
- removesnapshot, 670
- UpdateServiceOptions, 673
- upgrade, 674

BackupData

Erstellt einen Snapshot des HDFS-Verzeichnisses und erstellt eine ZIP-Datei des Snapshots auf der Hostmaschine des Katalogdiensts.

Der Befehl „infacmd ldm BackupData“ verwendet die folgende Syntax:

```
BackupData

<-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]

[<-HDFSSourceDirectory|-hsd> HDFS_source_directory

<-LocalDestination|-ld> local_destination

[<-CustomKeytabFile|-ckf> custom_keytab_file_location

[<-CustomClientUserPrincipal|-ccup> custom_client_user_principal
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ldm BackupData“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-HDFSSourceDirectory -hsd	HDFS_source_directory	Optional. Vollständiger Pfad zum HDFS-Quellverzeichnis, welches gesichert werden muss. Der Standardpfad ist `/Informatica/LDM/<serviceClusterName>`.
-LocalDestination -ld	local_destination	Erforderlich. Vollständiger Pfad auf der Hostmaschine des Katalogdiensts, auf die die Sicherung der HDFS-Daten kopiert werden muss.
-CustomKeytabFile -ckf	custom_keytab_file_location	Optional. Speicherort der benutzerdefinierten Keytab-Datei. Der Standardspeicherort für die Datei ist der Ort, an dem die Keytab-Datei des Katalogdiensts vorhanden ist.
-CustomClientUserPrincipal -ccup	custom_client_user_principal	Optional. Benutzer mit erforderlichen Berechtigungen im angegebenen Verzeichnis für das Sichern und Wiederherstellen in einem Cluster mit aktiviertem Kerberos. Der Standardbenutzer ist der Benutzer des Katalogdiensts.

CreateService

Erstellt einen Katalogdienst. Bevor Sie einen Katalogdienst erstellen, müssen Sie sicherstellen, dass die Hadoop-Cluster-Zertifikate in den Domänen-Truststore für einen Hadoop-Cluster importiert werden, der das SSL-Protokoll verwendet.

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

```
CreateService

<-DomainName|-dn> domain_name

<-NodeName|-nn> node_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ModelRepositoryService|-mrs> model_repository_service_name
```

```
<-MRSUserName|-mrsun> model_repository_service_user_name
<-MRSPassword|-mrspd> model_repository_service_user_password
[<-MRSSecurityDomain|-mrssdn> model_repository_service_user_security_domain]
<-DataIntegrationService|-dis> data_integration_service_name
[<-ContentManagementService|-cms> content_management_service_name]
[<-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]
[<-IsExternalCluster|-ise> is_external_cluster true|false]
[<-InfaHadoopServiceName|-ihsn> infa_hadoop_service_name]
[<-ZookeeperURI(s)|-zk> zk_uris]
[<-HDFSNameNodeURI(s)|-hnnu> hdfs_namenode_uri]
[<-YarnRMUri(s)|-yrmu> yarn_resource_manager_uri]
[<-YarnRMHttpUri(s)|-yrmhu> yarn_resource_manager_http_uri]
[<-HistoryServerHttpUri|-hshu> history_server_http_uri]
[<-YarnRMSchedulerUri(s)|-yrmsu> yarn_resource_manager_scheduler_uri]
[<-ServiceClusterName|-scn> service_cluster_name]
[<-HdfsServiceNameHA|-hsn> hdfs_service_name]
[<-IsClusterSecure|-isc> is_cluster_secure  true|false]
[<-HdfsServicePrincipal|-hspn> hdfs_service_principal]
[<-YarnServicePrincipal|-yspn> yarn_service_principal]
[<-KdcDomain|-kdn> kdc_domain_name]
[<-KeytabLocation|-kl> keytab_location]
[<-ClusterSslEnabled|-cssl> cluster_ssl_enabled  true|false]
[<-SolrKeyStoreFile|-skf> solr keystore file path on cluster]
[<-SolrKeyStorePassword|-skp> solr keystore password]
[<-isEmailEnabled|-iee> is_email_enabled true:false]
[<-OtherOptions|-oo> other options]
```

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

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-NodeName -nn	node_name	Erforderlich. Knoten, auf dem der Katalogdienst ausgeführt werden soll.
-SecurityDomain |-sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Katalogdiensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ModelRepositoryService -mrs	model_repository_service_name	Erforderlich. Name des Modellrepository-Diensts, der dem Katalogdienst zugeordnet wird.

Option	Argument	Beschreibung
-MRSUserName -mrsun	model_repository_service_user_name	Erforderlich, wenn Sie einen Modellrepository-Dienst angeben. Benutzername für die Verbindung zum Modellrepository. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-MRSPassword -mrspd	model_repository_service_user_password	Erforderlich, wenn Sie einen Modellrepository-Dienst angeben. Benutzerpasswort für den Modellrepository-Dienst.
-MRSSecurityDomain -mrssdn	model_repository_service_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Administrator-Benutzer gehört.
-DataIntegrationService -dis	data_integration_service_name	Erforderlich. Name des Datenintegrationsdiensts.
-ContentManagementService -cms	content_management_service_name	Optional. Name des Content-Managementdiensts.
-HttpPort -p	port_name	Erforderlich. Eine eindeutige HTTP-Portnummer, die für jeden Datenintegrationsdienst-Prozess verwendet wird. Der Standard ist 8085.
-HttpsPort -sp	https_port_name	Erforderlich, wenn Sie Transport Layer Security aktivieren. Die Portnummer für die HTTPS-Verbindung.
-EnableTls -tls	enable_tls	Wählen Sie diese Option zum Aktivieren von Transport Layer Security aus.
-KeystoreFile -kf	keystore_file_location	Erforderlich, wenn Sie „Transport Layer Security aktivieren“ auswählen. Pfad und Dateiname der Schlüsselspeicherdatei. Die Schlüsselspeicherdatei enthält die Schlüssel und Zertifikate, die bei Verwendung des SSL-Sicherheitsprotokolls mit dem Administrator von Live Data Map erforderlich sind.

Option	Argument	Beschreibung
-KeystorePassword -kp	keystore_password	Erforderlich, wenn Sie „Transport Layer Security aktivieren“ auswählen. Das Passwort für die Schlüsselspeicherdatei.
-SSLProtocol -sslp	ssl_protocol	Optional. Zu verwendendes Secure Sockets Layer-Protokoll.
-IsExternalCluster -ise	is_external_cluster	Gibt die Bereitstellungsart für Live Data Map an. Sie können wählen, ob Sie einen internen Hadoop-Cluster oder einen externen Hadoop-Cluster bereitstellen möchten.
-InfaHadoopServiceName -ihsn	infa_hadoop_service_name	Optional. Name des Hadoop-Diensts für den externen Cluster.
-ZookeeperURI -zk	zk_uris	Erforderlich. Der URI für die Zookeeper-Dienste, bei dem es sich um einen besonders leistungsfähigen Koordinationsdienst für verteilte Anwendungen handelt. Mehrere Zookeeper-URI-Werte werden durch Kommas getrennt.
-HDFSNameNodeURI -hnnu	hdfs_namenode_uri	Erforderlich. Die URI für den Zugriff auf HDFS. Verwenden Sie das folgende Format, um den NameNode-URI in der Cloudera-Verteilung anzugeben: `hdfs://<namenode>:<port>` Wobei - <namenode> der Hostname oder die IP-Adresse von NameNode ist.• - <port> der Port ist, den NameNode auf Remoteprozeduraufrufe (RPC) abhört. Geben Sie für Cluster mit aktivierter hoher Verfügbarkeit alle Hadoop-NameNode-URI-Werte durch Kommas getrennt ein.

Option	Argument	Beschreibung
-YarnRMUri -yrmu	yarn_resource_manager_uri	Erforderlich. Der Dienst innerhalb von Hadoop, der die MapReduce-Aufgaben an bestimmte Knoten im Cluster sendet. Verwenden Sie das folgende Format:`<hostname>:<port>` Wobei- - Hostname der Name bzw. die IP-Adresse des Yarn-Ressourcenmanagers ist.- - Port die Nummer des Ports ist, den der Yarn-Ressourcenmanager auf Remoteprozeduraufrufe (RPC) abhört. Geben Sie für Cluster mit aktivierter hoher Verfügbarkeit alle Ressourcenmanager-URI-Werte durch Kommas getrennt ein.
-YarnRMHttpUri -yrmhu	yarn_resource_manager_http_uri	Erforderlich. Der HTTP-URI-Wert für den Yarn-Ressourcenmanager. Geben Sie für Cluster mit aktivierter hoher Verfügbarkeit alle Ressourcenmanager-URI-Werte durch Kommas getrennt ein.
-HistoryServerHttpUri -hshu	history_server_http_uri	Erforderlich. Geben Sie einen Wert ein, um das Yarn-Zuweisungsprotokoll für Scanner zu generieren. Wenn Sie den Wert angeben, zeigt der Administrator von Live Data Map die Protokoll-URL als Teil der Aufgabenüberwachung an.
-YarnRMSchedulerUri -yrmsu	yarn_resource_manager_scheduler_uri	Erforderlich. Der Scheduler-URI-Wert für den Yarn-Ressourcenmanager. Geben Sie für Cluster mit aktivierter hoher Verfügbarkeit alle Ressourcenmanager-URI-Werte durch Kommas getrennt ein.
-ServiceClusterName -scn	service_cluster_name	Optional. Name des Dienst-Clusters.
-HdfsServiceNameHA -hsn	hdfs_service_name	Optional. Erforderlich für Cluster mit aktivierter hoher Verfügbarkeit. Name des HDFS-Diensts.
-IsClusterSecure -isc	is_cluster_secure	Gilt für externe Cluster. Wählen Sie die Aktivierung der Cluster-Authentifizierung aus.
-HdfsServicePrincipal -hspn	hdfs_service_principal	Erforderlich. Prinzipalname für den HDFS-Dienst.

Option	Argument	Beschreibung
-YarnServicePrincipal -yspn	yarn_service_principal	Erforderlich. Prinzipalname für den Yarn-Dienst.
-KdcDomain -kdn	kdc_domain_name	Erforderlich. Name der Kerberos-Domäne.
-KeytabLocation -kl	keytab_location	Erforderlich. Pfad zur Keytab-Datei. Eine Keytab-Datei enthält alle Benutzer in LDAP.
-ClusterSslEnabled -cssl	cluster_ssl_enabled	Optional. Wählen Sie die Option aus, um das Cluster-SSL zu aktivieren.
-SolrKeyStoreFile -skf	Solr_KeyStore_File	Optional. Pfad zur Solr-Schlüsselspeicherdatei im Cluster.
-SolrKeyStorePassword -skp	Solr_KeyStore_Password	Optional. Passwort für Solr-Schlüsselspeicher.
-isEmailEnabled -iee	is_email_enabled	Optional. Geben Sie „True“ an, wenn Sie die E-Mail-Benachrichtigung aktivieren möchten. Standardwert ist „False“.
-OtherOptions -oo	other options	Optional. Geben Sie Name-Wert-Paare durch Leerzeichen getrennt ein. Zur Eingabe eines Optionswerts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

ListServiceOptions

Listet Optionen für den Katalogdienst auf.

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

```
ListServiceOptions

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

[<-SecurityDomain|-sdn> security_domain]

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ldm ListServiceOptions“ beschrieben:

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

restoreData

Ruft die ZIP-Datei für die HDFS-Datensicherung aus dem Host des Katalogdiensts ab und stellt die Daten im HDFS-Verzeichnis wieder her.

Der Befehl „infacmd ldm restoreData“ verwendet die folgende Syntax:

```
 restoreData
<-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]
[<-ForcefulRestore|-fr> forceful_restore
[<-HDFSDestinationDir|-hdd> HDFS_destination_dir
<-ZipFileLocation|-zfl> zip_file_location
[<-CustomKeytabFile|-ckf> custom_keytab_file_location
[<-CustomClientUserPrincipal|-ccup> custom_client_user_principal
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ldm restoreData“ beschrieben:

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

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Katalogdiensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ForcefulRestore -fr	forceful_restore	Optional. Überschreibt vorhandene HDFS-Daten im Cluster mit den wiederhergestellten HDFS-Daten. Geben Sie „true“ an, wenn Sie die vorhandenen HDFS-Daten im Cluster überschreiben möchten. Standardwert ist „False“.
-HDFSDestinationDir -hdd	HDFS_destination_dir	Optional. Vollständiger Pfad zu dem HDFS-Verzeichnis, in dem die Daten wiederhergestellt werden müssen. Der Standardpfad ist `/Informatica/LDM/<serviceClusterName>`
-ZipFileLocation -zfl	zip_file_location	Erforderlich. Vollständiger Pfad der ZIP-Backup-Datei auf dem Host des Katalogdiensts. Der Inhalt der ZIP-Datei wird in den HDFS-Pfad kopiert, der in „HDFSDestinationDir“ angegeben ist.
-CustomKeytabFile -ckf	custom_keytab_file_location	Optional. Speicherort der benutzerdefinierten Keytab-Datei. Der Standardspeicherort für die Datei ist der Ort, an dem die Keytab-Datei des Katalogdiensts vorhanden ist.
-CustomClientUserPrincipal -ccup	custom_client_user_principal	Optional. Benutzer mit erforderlichen Berechtigungen im angegebenen Verzeichnis für das Sichern und Wiederherstellen in einem Cluster mit aktiviertem Kerberos. Der Standardbenutzer ist der Benutzer des Katalogdiensts.

removesnapshot

Entfernt Snapshot aus dem HDFS-Verzeichnis.

Hinweis: Verwenden Sie den Befehl „infacmd ldm removesnapshot“, wenn Sie Live Data Map auf einem internen Cluster bereitgestellt haben.

Der Befehl „infacmd ldm removesnapshot“ verwendet die folgende Syntax:

```
removesnapshot

<-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]

[<-HDFSSnapshotDir|-hssd> HDFS_snapshot_dir]

[<-CustomKeytabFile|-ckf> custom_keytab_file_location]

[<-CustomClientUserPrincipal|-ccup> custom_client_user_principal]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ldm removesnapshot“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-HDFSSnapshotDir -hssd	HDFS_snapshot_dir	Optional. Vollständiger Pfad zu dem HDFS-Verzeichnis, in dem der Snapshot gespeichert ist. Der Standardpfad ist `/Informatica/LDM/<serviceClusterName>`
-CustomKeytabFile -ckf	custom_keytab_file_location	Optional. Speicherort der benutzerdefinierten Keytab-Datei. Der Standardspeicherort für die Datei ist der Ort, an dem die Keytab-Datei des Katalogdiensts vorhanden ist.
-CustomClientUserPrincipal -ccup	custom_client_user_principal	Optional. Benutzer mit erforderlichen Berechtigungen im angegebenen Verzeichnis für das Sichern und Wiederherstellen in einem Cluster mit aktiviertem Kerberos. Der Standardbenutzer ist der Benutzer des Katalogdiensts.

UpdateServiceOptions

Aktualisiert Optionen für den Katalogdienst. Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

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

```
UpdateServiceOptions

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Options|-o> options
```

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

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

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

upgrade

Aktualisiert den Katalogdienst.

Der Befehl „infacmd ldm upgrade“ verwendet die folgende Syntax:

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ldm upgrade“ beschrieben:

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

KAPITEL 16

infacmd mrs-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- BackupContents, 677
- CheckInObject, 679
- CreateContents, 680
- CreateFolder, 682
- CreateProject, 684
- CreateService, 686
- DeleteContents, 689
- DeleteFolder, 691
- DeleteProject, 693
- ListBackupFiles, 695
- ListCheckedOutObjects, 697
- listFolders, 699
- ListLockedObjects , 701
- ListProjects, 703
- ListServiceOptions, 705
- ListServiceProcessOptions, 707
- PopulateVCS, 709
- ReassignCheckedOutObject, 711
- rebuildDependencyGraph, 713
- RenameFolder, 715
- RestoreContents, 717
- UndoCheckout, 719
- UnlockObject , 721
- UpdateServiceOptions, 723
- UpdateServiceProcessOptions, 729
- UpgradeContents, 731

BackupContents

Sichert den Inhalt des Modellrepository in einer Datei. Wenn der Repository-Inhalt nicht vorhanden ist, schlägt der Befehl fehl.

Um sicherzustellen, dass eine konsistente Backup-Datei erstellt wird, blockiert die Backup-Operation alle anderen Repository-Operationen so lange, bis das Backup abgeschlossen ist.

Der Befehl „infacmd mrs BackupContents“ verwendet die folgende Syntax:

```
BackupContents

<-DomainName|-dn> domain_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

<-OutputFileName|-of> output_file_name

[<-OverwriteFile|-ow> overwrite_file]

[<-Description|-ds> description]

[<-BackupSearchIndices|-bsi> backup search index]

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

In der folgenden Tabelle werden Optionen und Argumente für „infacmd mrs BackupContents“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Dienst.
OutputFileName -of	output_file_name	Erforderlich. Name der Backup-Datei.
OverwriteFile -ow	overwrite_file	Sie müssen diese Option einbeziehen, um eine Backup-Datei mit demselben Namen zu überschreiben.
Beschreibung -ds	Beschreibung	Beschreibung der Backup-Datei. Wenn die Beschreibung Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie die Beschreibung in Anführungszeichen ein.
-BackupSearchIndices -bsi	-	Optional. Setzen Sie den Wert auf TRUE, um den Suchindex in der Backup-Datei zu speichern und die zum Wiederherstellen der Datei benötigte Zeit zu verringern. Setzen Sie den Wert auf FALSE, um den Suchindex nicht in der Backup-Datei zu speichern. Wenn Sie die Datei wiederherstellen, erstellt der Modellrepository-Dienst den Suchindex neu. Standardwert ist „true“.
-ResilienceTimeout -re	timeout_period_in_second s	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

CheckInObject

Checkt ein einzelnes ausgechecktes Objekt ein. Das Objekt wird in das Modellrepository eingecheckt.

Der infacmd mrs CheckInObject-Befehl verwendet die folgende Syntax:

```
infacmd mrs checkInObject
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ObjectPathandName|-opn> object_path_and_name
[<-Description|-ds> description]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs CheckInObject“ beschrieben:

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

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Diensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ObjectPathAndName -opn	MRS_object_path	Erforderlich. Pfad zum Modellrepository-Objekt, einschließlich Objektname. Setzen Sie den Pfad in doppelte Anführungszeichen. Verwenden Sie folgende Syntax: `"ProjectName/FolderName/.../SubFolder_Name/{ObjectName|ProjectName/ObjectName}"`
-Description -ds	Beschreibung	Optional. Sie können diesen Parameter für die Eincheckbeschreibung oder für Eincheckkommentare verwenden.

CreateContents

Erstellt Repository-Inhalt für ein Modellrepository. Der Befehl schlägt fehl, wenn der Inhalt für das Modellrepository vorhanden ist.

Der Befehl „infacmd mrs CreateContents“ verwendet die folgende Syntax:

```
CreateContents

<-DomainName|-dn> domain_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs CreateContents“ beschrieben:

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

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Diensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

CreateFolder

Erstellt einen Ordner in einem Projekt in einem Modellrepository.

Der infacmd mrs CreateFolder-Befehl verwendet die folgende Syntax:

```
infacmd mrs createFolder
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
<-ProjectName|-pn> project_name
<-Path|-p> folder_path_and_name
[<-CreatePath|-cp> true|false]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs CreateFolder“ beschrieben:

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

Option	Argument	Beschreibung
-Path -p	folder_path_and_name	Erforderlich. Pfad und Name des zu erstellenden Ordners. Der Pfadname muss mit einem Schrägstrich (/) beginnen. Bei diesem Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden. Der Name darf nicht länger als 128 Zeichen sein und keine Wagenrückläufe, Tabulatoren, Leerzeichen oder die folgenden Zeichen enthalten: `/ * ? < > " |`
-CreatePath -cp	true|false	Optional. Wenn TRUE, wird der Ordner im angegebenen Pfad erstellt. Standardwert ist „false“.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

CreateProject

Erstellt ein Projekt in einem Modellrepository.

Der Befehl „infacmd mrs CreateProject“ verwendet die folgende Syntax:

```
infacmd mrs createProject
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
<-ProjectName|-pn> project_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs CreateProject“ beschrieben:

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

Option	Argument	Beschreibung
-ProjectName -pn	project_name	Erforderlich. Name des zu erstellenden Projekts. Beim Projektnamen wird die Groß-/Kleinschreibung nicht beachtet. Der Name darf nicht mehr als 128 Zeichen umfassen und keine Wagenrückläufe, Tabulatoren, Leerzeichen oder die folgenden Zeichen enthalten: `/ * ? < > " |`
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

CreateService

Erstellt einen Modellrepository-Dienst. Bevor Sie den Modellrepository-Dienst erstellen, müssen Sie zum Speichern von Repository-Tabellen eine Datenbank anlegen. Verwenden Sie den Datenbank-Client zum Erstellen der Datenbank.

Jedes Modellrepository muss die folgenden Datenbankanforderungen erfüllen:

- Das Modellrepository muss ein eindeutiges Schema aufweisen. Es ist nicht möglich, dass zwei Modellrepositorys oder ein Modellrepository und die Domänenkonfigurationsdatenbank dasselbe Schema verwenden.
- Das Modellrepository muss einen eindeutigen Repository-Datenbanknamen aufweisen.

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

```
CreateService

<-DomainName|-dn> domain_name

<-NodeName|-nn> node_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

<-DbUser|-du> db_user

<-DbPassword|-dp> db_password

<-DbUrl|-dl> db_url

[<-DbDriver|-dr> db_driver]

[<-DbDialect|-dd> db_dialect]
```

```
[<-SearchIndexRoot|-si> search_index_root]

[<-DbType|-dt> db_type]

[<-DbSchema|-ds> db_schema]

[<-DbTablespace|-db> db_tablespace (used for DB2 only)]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-FolderPath|-fp> full_folder_path]

[<-BackupNodes|-bn> nodename1,nodename2,...]
```

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

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
NodeName -nn	node_name	Erforderlich. Knoten, auf dem der Modellrepository-Dienst ausgeführt werden soll.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Diensts.
-DbUser -du	db_user	Erforderlich. Konto für die Repository-Datenbank. Richten Sie dieses Konto mithilfe des Datenbank-Clients ein.
-DbPassword -dp	db_password	Erforderlich. Passwort der Repository-Datenbank für den Datenbankbenutzer.
-DbUrl -dl	db_url	Erforderlich. Die JDBC-Verbindungszeichenfolge, die zur Verbindung mit der Modellrepository-Datenbank verwendet wird. Verwenden Sie für jede unterstützte Datenbank die folgende Syntax für die JDBC-Verbindungszeichenfolge: - IBM DB2. `jdbc:informatica:db2:// <host_name>:<port_number>;DatabaseName=<database_name>;BatchPerformanceWorkaround=true;DynamicSections=3000` - Microsoft SQL Server, der die Standardinstanz verwendet. `jdbc:informatica:sqlserver:// <host_name>:<port_number>;DatabaseName=<database_name>;SnapshotSerializable=true` - Microsoft SQL Server, der eine benannte Instanz verwendet. `jdbc:informatica:sqlserver:// <host_name> \<named_instance_name>;DatabaseName=<database_name>;SnapshotSerializable=true` - Oracle. `jdbc:informatica:oracle:// <host_name>:<port_number>;SID=<database_name>;MaxPooledStatements=20;CatalogOptions=0;BatchPerformanceWorkaround=true`
-DbDriver -dr	db_driver	Optional. Der Data Direct-Treiber zum Herstellen einer Verbindung zur Datenbank. Beispiel: com.informatica.jdbc.oracle.OracleDriver
-DbDialect -dd	db_dialect	Optional. Der SQL-Dialekt für eine bestimmte Datenbank. Der Dialekt ordnet Objekte zu Datenbankobjekten hinzu. Beispiel: org.hibernate.dialect.Oracle9Dialect
-SearchIndexRoot -si	search_index_root	Optional. Ändert das Verzeichnis für den Suchindex. Geben Sie den vollständigen Pfad zum Verzeichnis ein. Standardmäßig wird das Informatica-Installationsverzeichnis verwendet.

Option	Argument	Beschreibung
-DbType -dt	db_type	Optional. Werte sind „Oracle“, „SQL Server“ oder „DB2“.
-DbSchema -ds	db_schema	Optional. Der Schemaname für eine Microsoft SQL Server-Datenbank.
-DbTablespace -dt	db_tablespace	Nur für eine DB2-Datenbank erforderlich. Beim Konfigurieren eines Tablespace-Namens erstellt der Modellrepository-Dienst alle Repository-Tabellen im selben Tablespace. Sie können im Tablespace-Namen keine Leerzeichen verwenden.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-FolderPath -fp	full_folder_path	Optional. Vollständiger Pfad ohne Domänennamen zu dem Ordner, in dem Sie den Dienst erstellen möchten. Folgendes Format ist erforderlich: */parent_folder/child_folder* Standardwert ist „/“ (die Domäne).
-BackupNodes -bn	nodename1,nodename2,...	Optional. Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist. Sie können Backup-Knoten konfigurieren, wenn Sie hohe Verfügbarkeit haben.

DeleteContents

Löscht den Inhalt des Modellrepository. Der Befehl schlägt fehl, wenn der Inhalt für das Modellrepository nicht vorhanden ist.

Der Befehl „infacmd mrs DeleteContents“ verwendet die folgende Syntax:

```
DeleteContents

<-DomainName|-dn> domain_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs DeleteContents“ beschrieben:

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

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Diensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

DeleteFolder

Löscht einen Ordner aus einem Projekt in einem Modellrepository.

Zum Löschen eines Ordners, der Objekte enthält, legen Sie die Option -ForceDelete auf TRUE fest.

Der infacmd mrs DeleteFolder-Befehl verwendet die folgende Syntax:

```
infacmd mrs deleteFolder
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
<-ProjectName|-pn> project_name
<-Path|-p> folder_path_and_name
[<-ForceDelete|-f> true|false]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs DeleteFolder“ beschrieben:

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

Option	Argument	Beschreibung
-ForceDelete -f	true|false	Optional. Wenn TRUE, wird ein Ordner mit Objekten gelöscht. Standardwert ist „false“.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

DeleteProject

Löscht ein Projekt in einem Modellrepository.

Legen Sie die Option -ForceDelete auf TRUE fest, um ein Projekt mit Ordnern und Objekten zu löschen.

Der infacmd mrs DeleteProject-Befehl verwendet die folgende Syntax:

```
infacmd mrs deleteProject
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
<-ProjectName|-pn> project_name
[<-ForceDelete|-f> true|false]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs DeleteProject“ beschrieben:

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

Option	Argument	Beschreibung
-ForceDelete -f	true|false	Optional. Wenn TRUE, wird ein Projekt mit Ordnern und Objekten gelöscht. Standardwert ist „false“.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

ListBackupFiles

Listet Dateien im Backup-Ordner auf.

Der Befehl „infacmd mrs ListBackupFiles“ verwendet die folgende Syntax:

```
ListBackupFiles

<-DomainName|-dn> domain_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs ListBackupFiles“ beschrieben:

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

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Dienst.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

ListCheckedOutObjects

Zeigt eine Liste von Objekten an, die von einem Benutzer ausgecheckt wurden. Führen Sie diesen Befehl für ein Repository aus, das in ein Versionsverwaltungssystem integriert ist.

Der Befehl „infacmd mrs listCheckedOutObjects“ verwendet die folgende Syntax:

```
infacmd mrs listCheckedOutObjects
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-ByUser|-bu> by_user_name]
[<-ByUserSecurityDomain|-bsd> by_user_security_domain]
[<-ObjectType|-ot> object_type]
[<-ByObjectPathandName|-bopn> object_path_and_name]
[<-objectName|-objn> object_name]
[<-operationType|-optype> operation_type]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs listCheckedOutObjects“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ByUser -bu	checkedout_by_user	Optional. Benutzerkonto, von dem Objekte im Modellrepository ausgecheckt wurden.
-ObjectType -ot	object_type	Optional. Typ des zu suchenden Objekts. Beispiel: Mapping.
-ByObjectPathandName -bopn	object_path_and_name	Optional. Pfad und Name des zu suchenden Objekts.
-ObjectName -objn	object_name	Optional. Name des zu suchenden Objekts.
-LastOperationType -optype	operation_type	Optional. Typ des zu suchenden Vorgangs. Geben Sie einen der folgenden Werte ein: - ADD_OP - EDIT_OP - MOVE_OP - DELETE_OP

listFolders

Listet die Namen aller Ordner im angegebenen Projektordnerpfad auf.

Verwenden Sie die Option -Path, um alle Ordner in einem Projekt oder alle in einem Unterordner enthaltenen Ordner aufzulisten. Verwenden Sie einen Schrägstrich (/) zur Angabe der obersten Ebene eines Projekts.

Der folgende Befehl listet beispielsweise alle Ordner in /MRS_1/Projekt_A/ auf:

```
infacmd mrs listFolders ... -sn MRS_1 -pn Project_A -p /
```

Enthält Projekt_A Ordner_1 und Ordner_2, listet der folgende Befehl alle Unterordner in Ordner_1 auf:

```
infacmd mrs listFolders ... -sn MRS_1 -pn Project_A -p /Folder_1/
```

Der infacmd mrs ListFolders-Befehl verwendet die folgende Syntax:

```
infacmd mrs listFolders
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
<-ProjectName|-pn> project_name
<-Path|-p> path
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs ListFolders“ beschrieben:

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

Option	Argument	Beschreibung
-Path -p	path	Erforderlich. Pfad zu dem übergeordneten Ordner, in dem Ordnerinhalte aufgelistet werden sollen. Der Pfad muss mit einem Schrägstrich (/) beginnen. Bei diesem Namen wird die Groß-/Kleinschreibung nicht beachtet.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

ListLockedObjects

Zeigt eine Liste von Objekten an, die von einem Benutzer gesperrt wurden. Führen Sie diesen Befehl für ein Repository aus, das nicht in ein Versionsverwaltungssystem integriert ist.

Hinweis: Wenn Sie diesen Befehl für ein versioniertes Repository ausführen, schlägt der Befehl fehl.

Der Befehl „infacmd mrs listLockedObjects“ verwendet die folgende Syntax:

```
infacmd mrs listLockedObjects
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-ByUser|-bu> user_name]
[<-ByUserSecurityDomain|-bsd> by_user_security_domain]
[<-ObjectType|-ot> object_type]
[<-ByObjectPathandName|-bopn> object_path_and_name]
[<-objectName|-objn> object_name]
[<-lastOperationType|-optype> operation_type]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs listLockedObjects“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ByUser -bu	locked_by_user	Optional. Benutzerkonto, das Besitzer der Sperre für Objekte im Modellrepository ist. Standard sind von allen Benutzern gesperrte Objekte.
-ObjectType -ot	object_type	Optional. Typ des zu suchenden Objekts. Sie können den Befehl für einen Objekttyp ausführen. Wenn Sie den Parameter nicht angeben, wird der Befehl für alle Objekttypen ausgeführt.
-ByObjectPathAndName -bopn	object_path_and_name	Optional. Modellrepository-Pfad und -Name des zu suchenden Objekts.
-ObjectName -objn	object_name	Optional. Name des zu suchenden Objekts.
-LastOperationType -optype	operation_type	Optional. Typ des zu suchenden Vorgangs. Geben Sie einen der folgenden Werte ein: - ADD_OP - EDIT_OP - MOVE_OP - DELETE_OP

ListProjects

Listet Projekte im Modellrepository auf. Der Befehl schlägt fehl, wenn das Modellrepository keinen Repository-Inhalt aufweist.

Der Befehl „infacmd mrs ListProjects“ verwendet die folgende Syntax:

```
ListProjects

<-DomainName|-dn> domain_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs ListProjects“ beschrieben:

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

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Dienst.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

ListServiceOptions

Listet Optionen für den Modellrepository-Dienst auf.

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

```
ListServiceOptions

<-DomainName|-dn> domain_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs ListServiceOptions“ beschrieben:

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

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Dienst.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

ListServiceProcessOptions

Listet Dienstprozess-Optionen für den Modellrepository-Dienst auf.

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

```
ListServiceOptions

<-DomainName|-dn> domain_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs ListServiceProcessOptions“ beschrieben:

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

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Dienst.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

PopulateVCS

Synchronisiert das Modellrepository mit einem Versionsverwaltungssystem. Bevor Sie das Modellrepository mit einem Versionsverwaltungssystem synchronisieren, konfigurieren Sie Versionierungseigenschaften.

Wenn Sie Versionierungseigenschaften konfigurieren, starten Sie das Modellrepository neu und führen dann den Befehl „PopulateVCS “ aus.

Hinweis: Nach der Ausführung des Befehls ist das Modellrepository bis zum Abschluss der Synchronisierung nicht verfügbar.

Der Befehl „infacmd mrs populateVCS“ verwendet die folgende Syntax:

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs populateVCS“ beschrieben:

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

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Diensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

ReassignCheckedOutObject

Weist die Eigentümerschaft eines ausgecheckten Objekts einem anderen Benutzer neu zu. Wenn der Eigentümer eines ausgecheckten Objekts die Änderungen gespeichert hat, werden diese beim erneuten Zuweisen des Objekts beibehalten. Werden die Änderungen nicht gespeichert, gehen sie beim erneuten Zuweisen des Objekts verloren.

Der Befehl „infacmd mrs reassignCheckedOutObject“ verwendet die folgende Syntax:

```
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ObjectPathandName|-opn> object_path_and_name
<-ToUser|-tu> to_user
[<-ToUserSecurityDomain|-tsd> to_user_security_domain]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs reassignCheckedOutObject“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ObjectPathAndName -opn	MRS_object_path	Erforderlich. Verwenden Sie folgende Syntax: `ProjectName/FolderName/.../SubFolder_Name/{ObjectName|ProjectName/ObjectName}`
-ToUser -tu	Benutzername	Erforderlich. Benutzername des Benutzers, der Besitzer des ausgecheckten Status des Objekts sein soll.
-ToUserSecurityDomain -tsd	Sicherheitsdomäne	Optional. Sicherheitsdomäne des Benutzers, der Besitzer des ausgecheckten Status des Objekts sein soll.

rebuildDependencyGraph

Erstellt die Objektabhängigkeitsgrafik erneut, damit Sie die Objektabhängigkeiten nach einem Upgrade anzeigen können. Führen Sie diesen Befehl aus, wenn beim Upgrade des Modellrepository-Diensts die erneute Erstellung der Objektabhängigkeitsgrafik fehlgeschlagen ist.

Benutzer dürfen nicht auf Modellrepository-Objekte zugreifen, solange der Neuerstellungsvorgang nicht abgeschlossen ist, damit die Objektabhängigkeitsgrafik nicht ungenau wird. Diesen Befehl möchten Sie möglicherweise ausführen, wenn keine Benutzer angemeldet sind.

Der Befehl „infacmd mrs rebuildDependencyGraph“ verwendet die folgende Syntax:

```
rebuildDependencyGraph

<-DomainName|-dn> domain_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs rebuildDependencyGraph“ beschrieben:

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

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Dienst.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

RenameFolder

Benennt einen Ordner in einem Projekt um.

Der infacmd mrs RenameFolder-Befehl verwendet die folgende Syntax:

```
infacmd mrs renameFolder
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
<-ProjectName|-pn> project_name
<-SourceFolder|-sf> source_folder
<-TargetFolder|-tf> target_folder
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs RenameFolder“ beschrieben:

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

Option	Argument	Beschreibung
-TargetFolder -tf	target_folder_path_and_name	Erforderlich. Neuer Name für den Ordner. Sie können einen Ordnernamen oder einen Pfad und Ordnernamen angeben. Der Pfad muss mit einem Schrägstrich (/) beginnen.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

RestoreContents

Stellt den Inhalt eines Modellrepository aus einer Backup-Datei wieder her.

Der Befehl „infacmd mrs RestoreContents“ verwendet die folgende Syntax:

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs RestoreContents“ beschrieben:

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

Option	Argument	Beschreibung
InputFileName -if	input_file_name	Erforderlich. Name der wiederherzustellenden Backup-Datei.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

UndoCheckout

Kehrt das Auschecken eines Modellrepository-Objekts um. Das Objekt wird in das Modellrepository eingecheckt. Das Modellrepository verwirft alle Änderungen, die am Objekt vorgenommen wurden, seit es ausgecheckt wurde. Das Versionsverwaltungssystem erhöht die Versionsnummer nicht bzw. fügt sie nicht der Versionshistorie hinzu.

Der Befehl „infacmd mrs undoCheckout“ verwendet die folgende Syntax:

```
infacmd mrs undoCheckout
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ObjectPathAndName|-opn> Object_path_and_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs undoCheckout“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ObjectPathAndName -opn	MRS_object_path	Erforderlich. Pfad zum Modellrepository-Objekt, einschließlich Objektname. Setzen Sie den Pfad in doppelte Anführungszeichen. Verwenden Sie folgende Syntax: `"ProjectName/FolderName/.../SubFolder_Name/{ObjectName|ProjectName/ObjectName}"`

UnlockObject

Entsperrt ein Modellrepository-Objekt, das von einem Benutzer gesperrt wurde. Führen Sie diesen Befehl für ein Repository aus, das nicht in ein Versionsverwaltungssystem integriert ist.

Hinweis: Wenn Sie diesen Befehl für ein versioniertes Repository ausführen, schlägt der Befehl fehl.

Sie können jeweils ein Objekt entsperren.

Der Befehl „infacmd mrs unlockObject“ verwendet die folgende Syntax:

```
infacmd mrs unlockObject
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ObjectPathAndName|-opn> Object_path_and_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs unlockObject“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ObjectPathAndName -opn	MRS_object_path	Erforderlich. Pfad zum Modellrepository-Objekt, einschließlich Objektname. Verwenden Sie zum Beispiel die folgende Syntax: `ProjectName/FolderName/SubFolder_Name/ObjectName`

UpdateServiceOptions

Aktualisiert Optionen für den Modellrepository-Dienst. Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

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

```
UpdateServiceOptions

<-DomainName|-dn> domain_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Options|-o> options

[<-PrimaryNode|-nn> primary node name]

[<-BackupNode|-bn> nodename1,nodename2,...]

[<-SearchIndexRoot|-si> search_index_root]
```

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

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Options -o	options	Erforderlich. Geben Sie Name-Wert-Paare durch Leerzeichen getrennt ein.
-PrimaryNode -nn	Name des primären Knotens	Optional. Knoten, auf dem der Modellrepository-Dienst ausgeführt werden soll.
-BackupNodes -bn	nodename1,nodename2,...	Optional. Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist. Sie können Backup-Knoten konfigurieren, wenn Sie hohe Verfügbarkeit haben.
-SearchIndexRoot -si		optional. Ändert das Verzeichnis für den Suchindex. Geben Sie den vollständigen Pfad zum Verzeichnis ein. Standardmäßig wird das Informatica-Installationsverzeichnis verwendet.

Optionen des Modellrepository-Diensts

Verwenden Sie die Modellrepository-Dienst-Optionen mit dem Befehl „infacmd mrs UpdateServiceOptions“.

Geben Sie Modellrepository-Dienst-Optionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Modellrepository-Dienst-Optionen beschrieben:

Option	Argument	Beschreibung
CACHE.EnableCache	true | false	Aktiviert den Modellrepository-Dienst für die Speicherung von Modellrepository-Objekten im Cachespeicher. Starten Sie den Modellrepository-Dienst neu, um die Änderungen zu übernehmen.
CACHE.CacheJVMOptions	-Xmx[heap_size]	JVM-Optionen für den Modellrepository-Dienst-Cache. Konfigurieren Sie die maximale Heap-Größe, um die Speichermenge zu konfigurieren, die dem Cache zugewiesen wird. Dieses Feld muss die maximale Heap-Größe, angegeben durch die Option -Xmx, umfassen. Der Standard- und Mindestwert für die maximale Heap-Größe ist -Xmx128m. Die von Ihnen konfigurierten Optionen werden beim Aktivieren des Modellrepository-Dienst-Cache übernommen. Starten Sie den Modellrepository-Dienst neu, um die Änderungen zu übernehmen. Die in diesem Feld konfigurierten Optionen gelten nicht für die JVM, die den Modellrepository-Dienst ausführt.
PERSISTENCE_DB.Username	db_user	Erforderlich. Konto für die Repository-Datenbank. Richten Sie dieses Konto mithilfe des Datenbank-Clients ein.
PERSISTENCE_DB.Password	db_password	Erforderlich. Passwort der Repository-Datenbank für den Datenbankbenutzer.
PERSISTENCE_DB.DatabaseSchema	db_schema	Optional. Der Name des Schemas für eine bestimmte Datenbank.
PERSISTENCE_DB.DatabaseTablespace	db_tablespace	Nur für eine DB2-Datenbank erforderlich. Beim Konfigurieren eines Tablespace-Namens erstellt der Modellrepository-Dienst alle Repository-Tabellen im selben Tablespace. Sie können im Tablespace-Namen keine Leerzeichen verwenden. Bei einer IBM DB2-Datenbank mit mehreren Partitionen muss sich der Tablespace über einen einzelnen Knoten und eine einzelne Partition erstrecken.
PERSISTENCE_DB.DatabaseType	DatabaseType	Erforderlich. Zu den Datenbanktypen gehören: - db2 - oracle - mssqlserver - sybase

Option	Argument	Beschreibung
PERSISTENCE_DB.JDBCConnectString	JDBC-Verbindungszeichenfolge	Die JDBC-Verbindungszeichenfolge, die zur Verbindung mit der Modellrepository-Datenbank verwendet wird. Verwenden Sie für jede unterstützte Datenbank die folgende Syntax für die JDBC-Verbindungszeichenfolge: - IBM DB2. `jdbc:informatica:db2:// <host_name>:<port_number>;DatabaseName=< database_name>;BatchPerformanceWorkaroun d=true;DynamicSections=3000` - Microsoft SQL Server, der die Standardinstanz verwendet. `jdbc:informatica:sqlserver:// <host_name>:<port_number>;DatabaseName=< database_name>;SnapshotSerializable=true` - Microsoft SQL Server, der eine benannte Instanz verwendet. `jdbc:informatica:sqlserver:// <host_name> \<named_instance_name>;DatabaseName=<dat abase_name>;SnapshotSerializable=true` - Oracle. `jdbc:informatica:oracle:// <host_name>:<port_number>;SID=<database_ name>;MaxPooledStatements=20;CatalogOpti ons=0;BatchPerformanceWorkaround=true`
PERSISTENCE_DB.SecureJDBCParameters	Sichere JDBC-Parameter	Wenn die Modellrepository-Datenbank mittels SSL-Protokoll gesichert wird, müssen Sie die sicheren Datenbankparameter eingeben. Geben Sie die Parameter als `name=value`-Paare, getrennt durch ein Semikolon (;) ein. Beispiel: `param1=value1;param2=value2`
PERSISTENCE_DB.Dialect	Dialekt	Der SQL-Dialekt für eine bestimmte Datenbank. Der Dialekt ordnet Objekte zu Datenbankobjekten hinzu. Beispiel: `org.hibernate.dialect.Oracle9Dialect`
PERSISTENCE_DB.Driver	Treiber	Der Data Direct-Treiber zum Herstellen einer Verbindung zur Datenbank. Beispiel: `com.informatica.jdbc.oracle.OracleDriver`

SEARCH.SearchAnalyzer	Vollständig qualifizierter Java-Klassenname	Der vollständig qualifizierte Java-Klassenname des Search Analyzer.
		Standardmäßig verwendet der Modellrepository-Dienst den folgenden Search Analyzer für Englisch:
		`com.informatica.repository.service.provide r.search.analysis.MMStandardAnalyzer`
		Der folgende Java-Klassenname kann für die Sprachen Chinesisch, Japanisch und Koreanisch angegeben werden:
		`org.apache.lucene.analysis.cjk.CJKAnalyzer`
		Alternativ können Sie einen benutzerdefinierten Search Analyzer erstellen.

Option	Argument	Beschreibung
SEARCH.SearchAnalyzerFactory	Vollständig qualifizierter Java-Klassenname	Vollständig qualifizierter Java-Klassenname der Factory-Klasse, wenn Sie eine Factory-Klasse zum Erstellen eines benutzerdefinierten Search Analyzer verwendet haben. Wenn Sie einen benutzerdefinierten Search Analyzer verwenden, geben Sie entweder den Namen der Search Analyzer-Klasse oder der Search Analyzer-Factory-Klasse ein.
VCS.Host	„IP_address“ oder Hostname	Erforderlich, um die Versionierungseigenschaften für das Modellrepository für Perforce zu konfigurieren. Die URL, die IP-Adresse oder der Hostname des Computers, auf dem das Perforce-Versionsverwaltungssystem ausgeführt wird. Verwenden Sie diese Option nicht, wenn Sie SVN als Versionsverwaltungssystem konfigurieren.
VCS.URL	URL des Subversion-Repositorys	Erforderlich, um die Versionierungseigenschaften für das Modellrepository für SVN zu konfigurieren. URL des Subversion-Repositorys. Beispiel: `VCS.URL=https://myserver.company.com/svn/` Verwenden Sie diese Option nicht, wenn Sie Perforce als Versionsverwaltungssystem konfigurieren.
VCS.Port	VCS_port	Erforderlich, um die Versionierungseigenschaften für das Modellrepository zu konfigurieren. Portnummer, die der Host des Versionsverwaltungssystems für das Abhören auf Pakete vom Modellrepository verwendet.
VCS.User	VCS_user	Erforderlich, um die Versionierungseigenschaften für das Modellrepository zu konfigurieren. Benutzerkonto für den Benutzer des Versionsverwaltungssystems. Dieses Konto muss über Schreibberechtigungen für das Versionsverwaltungssystem verfügen. Nachdem Sie die Verbindung mit diesem einzelnen Benutzer und Passwort für das Versionsverwaltungssystem konfiguriert haben, stellen alle Modellrepository-Benutzer die Verbindung zum Versionsverwaltungssystem über dieses Konto her. Für das Perforce-Versionsverwaltungssystem muss der Kontotyp ein Standardbenutzer sein.
VCS.Password	VCS_password	Erforderlich, um die Versionierungseigenschaften für das Modellrepository zu konfigurieren. Passwort für den Benutzer des Versionsverwaltungssystems.

Option	Argument	Beschreibung
VCS.Type	VCS_type	Erforderlich, um die Versionierungseigenschaften für das Modellrepository zu konfigurieren. Das unterstützte Versionsverwaltungssystem, mit dem Sie die Verbindung herstellen möchten. Sie können zwischen „Perforce" und „SVN" wählen.

VCS.MRSPath	MRS_path	Erforderlich, um die Versionierungseigenschaften für das Modellrepository mit Perforce zu konfigurieren.
		Pfad zum Root-Verzeichnis der Kopie von Modellrepository-Objekten des Versionsverwaltungssystems.
		Hinweis: Wenn Sie den Befehl ausführen, stellt das Modellrepository eine Verbindung zum Versionsverwaltungssystem her und generiert das angegebene Verzeichnis, falls noch kein Verzeichnis vorhanden ist.
		Dieses Verzeichnis kann nur für einen Modellrepository-Dienst verwendet werden.
		Verwenden Sie für Perforce die folgende Syntax:
		`//directory/path`
		`directory` ist das Root-Verzeichnis von Perforce und `path` ist der Rest des Pfades zum Root-Verzeichnis des Modellrepository-Objekts.
		Beispiel:
		`//depot/Informatica/repository_copy`
		Verwenden Sie diese Option nicht, wenn Sie SVN als Versionsverwaltungssystem konfigurieren.

UpdateServiceProcessOptions

Aktualisiert Dienstprozessoptionen für den Modellrepository-Dienst. Trennen Sie mehrere Optionen mit einem Leerzeichen. Um einen Wert einzugeben, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Wert in Anführungszeichen.

Geben Sie Dienstprozessoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Der Befehl „infacmd mrs UpdateServiceProcessOptions" verwendet die folgende Syntax:

```
UpdateServiceProcessOptions

<-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
```

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

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Options -o	optionen	Erforderlich. Geben Sie Name-Wert-Paare durch Leerzeichen getrennt ein.

UpgradeContents

Aktualisiert den Inhalt des Modellrepository. Der Befehl schlägt fehl, wenn das Modellrepository keinen Repository-Inhalt aufweist.

Der Befehl „infacmd mrs UpgradeContents“ verwendet die folgende Syntax:

```
UpgradeContents

<-DomainName|-dn> domain_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd mrs UpgradeContents“ beschrieben:

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

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Modellrepository-Dienst.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

KAPITEL 17

infacmd ms-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- GetRequestLog, 734
- ListMappingParams, 736
- ListMappings, 739
- RunMapping, 741
- UpgradeMappingParameterFile, 745

GetRequestLog

Schreibt das Zuordnungsprotokoll in die angegebene Datei. Geben Sie die Job-ID ein, die vom infacmd ms RunMapping-Befehl zurückgegeben wurde.

Der infacmd ms GetRequestLog-Befehl verwendet die folgende Syntax:

```
GetRequestLog

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-RequestId|-id> request_id

<-FileName|-f> file_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ms GetRequestLog“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-RequestId -id	request_id	Erforderlich. Die Job-ID für die Zuordnung, für die die Protokolldatei geschrieben werden soll. Geben Sie die Job-ID ein, die vom infacmd ms RunMapping-Befehl zurückgegeben wurde.
-FileName -f	file_name	Erforderlich. Name und Dateipfad, in den die Protokolldatei geschrieben werden soll.

ListMappingParams

Listet die Parameter für ein Mapping auf und erstellt eine Mapping-Parameterdatei, die Sie beim Ausführen eines Mappings verwenden können. Der Befehl gibt eine XML-Datei mit Standardwerten zurück, die Sie aktualisieren können. Geben Sie den Parameter-Dateinamen ein, wenn Sie das Mapping mit infacmd ms RunMapping ausführen.

Der Befehl „infacmd ms ListMappingParams“ verwendet die folgende Syntax:

```
ListMappingParams

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Application|-a> application_name

<-Mapping|-m> mapping_name

[<-OutputFile|-o> output file_to_write_to]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ms ListMappingParams“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch. Optional. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Bei der Sicherheitsdomäne wird die Groß-/Kleinschreibung beachtet. Standardwert ist „Native“.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	application_name	Erforderlich. Name der Anwendung, die das Mapping enthält.
-Mapping -m	mapping_name	Erforderlich. Name des Mappings.
- OutputFile - o	output file_to_write_to	Optional. Pfad und Dateiname der zu erstellenden Parameterdatei. Wenn Sie keine Datei angeben, zeigt der Befehl die Parameter in der Eingabeaufforderung an.

ListMappingParams-Ausgabe

Der ListMappingParams-Befehl gibt eine Parameterdatei als XML-Datei mit Standardwerten zurück, die Sie aktualisieren können.

Sie führen beispielsweise den ListMappingParams-Befehl für die Anwendung "MyApp" und das Mapping "MyMapping" aus. Das Mapping "MyMapping" hat einen Parameter "MyParameter". Der ListMappingParams-Befehl gibt eine XML-Datei in folgendem Format zurück:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="no"?>
<root xmlns="http://www.informatica.com/Parameterization/1.0" xmlns:xsi="http://
www.w3.org/2001/XMLSchema">
    <!--
    <application name="MyApp">
```

```
        <mapping name="MyMapping">
            <!-- Specify deployed application specific parameters here. -->
        </mapping>
    </application>
    -->
    <project name="MyProject">
        <mapping name="MyMapping">
            <parameter name="MyParameter">DefaultValue</parameter>
        </mapping>
    </project>
</root>
```

Die Ausgabe-XML-Datei hat die folgenden Elemente der obersten Ebene:

Anwendungselement

Wenn Sie einen Parameter innerhalb des Elements auf der obersten Ebene einer Anwendung definieren, wendet der Data Integration Service den Parameterwert an, wenn Sie das angegebene Mapping in der angegebenen Anwendung ausführen. Sie müssen mindestens ein Projektelement in eine Anwendung/ein Mapping-Element einbeziehen.

Standardmäßig befindet sich dieses Element auf der obersten Ebene in den Kommentaren. Entfernen Sie die Kommentare (!-- and -->), um dieses Element zu verwenden.

Projektelement

Wenn Sie einen Parameter innerhalb des Elements auf der obersten Ebene eines Projekts definieren, wendet der Data Integration Service den Parameterwert auf das angegebene Mapping im Projekt in jeder bereitgestellten Anwendung an. Der Dienst wendet den Parameterwert auch auf alle Mappings an, die die Objekte im Projekt verwenden.

Wenn Sie in einem Projekt denselben Parameter in einem Element auf der obersten Ebene einer Anwendung und ein Element in derselben Parameterdatei definieren, hat der im Anwendungselement definierte Parameterwert Vorrang.

ListMappings

Listet die Mappings in einer Anwendung auf.

Der Befehl „infacmd ms ListMappings“ verwendet die folgende Syntax:

```
ListMappings

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-Application|-a> application_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ms ListMappings“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit diesen beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts zum Ausführen des Mappings. Die Anwendung, die das Mapping enthält, muss für einen Datenintegrationsdienst bereitgestellt werden.
-Application -a	application_name	Erforderlich. Name der Anwendung, die das Mapping enthält.

RunMapping

Führt eine Zuordnung aus, die einem Datenintegrationsdienst bereitgestellt wird. Sie können die Zuordnung mit einem Parametersatz oder einer Parameterdatei ausführen.

Führen Sie zum Erstellen einer Parameterdatei den Befehl infacmd ms ListMappingParams aus. Führen Sie zuerst den infacmd dis StartApplication-Befehl für die Anwendung und dann den infacmd ms ListMappingParams-Befehl aus. Stellen Sie vor dem Ausführen von „infacmd ms ListMappingParams“ sicher, dass die Anwendung im Administrator Tool ausgeführt wird.

Führen Sie zum Anzeigen der Parameter und Werte für einen Parametersatz den infacmd dis ListParameterSetEntries-Befehl aus.

Der Befehl „infacmd ms RunMapping“ verwendet die folgende Syntax:

```
RunMapping

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Application|-a> application_name

<-Mapping|-m> mapping_name

[<-Wait|-w> true|false]

[<-ParameterFile|-pf> parameter_file_path]

[<-ParameterSet|-ps> parameter_set_name]
```

```
[<-OperatingSystemProfile|-osp> operating_system_profile_name]

[<-NodeName|-nn> node_name]

[<-OptimizationLevel|-ol> optimization_level]

[<-PushdownType|-pt> pushdown_type]

[<-CustomProperties|-cp> custom_properties]
```

Der Befehl gibt die Job-ID für die Zuordnungsausführung zurück.

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ms RunMapping“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch. Optional. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Bei der Sicherheitsdomäne wird die Groß-/Kleinschreibung beachtet. Standardwert ist „Nativ“.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	application_name	Erforderlich. Name der Anwendung, die die Zuordnung enthält.
-Mapping -m	mapping_name	Erforderlich. Name der auszuführenden Zuordnung.
-Wait -w	true|false	Optional. Gibt an, ob infacmd bis zum Abschluss der Zuordnung wartet, bevor eine Rückkehr zur Shell oder Eingabeaufforderung erfolgt. Ist die Option auf TRUE festgelegt, kehrt infacmd nach Abschluss der Zuordnung zur Shell oder Eingabeaufforderung zurück. Sie können keine nachfolgenden Befehle ausführen, wenn die Zuordnung noch nicht abgeschlossen ist. Ist die Option auf FALSE festgelegt, kehrt infacmd sofort zur Shell oder Eingabeaufforderung zurück. Sie müssen nicht auf den Abschluss der Zuordnung warten, bevor Sie den nächsten Befehl ausführen. Standardwert ist „false“.
-ParameterFile -pf	parameter_file_path	Optional. Name und Pfad der Parameterdatei. Geben Sie weder eine Parameterdatei noch einen Parametersatz ein.

Option	Argument	Beschreibung
-ParameterSet -ps	parameter_set_name	Optional. Name eines zur Laufzeit zu verwendenden Parametersatzes. Die Parametersatzoption überschreibt alle mit einer Anwendung bereitgestellten Parametersätze. Geben Sie weder einen Parametersatz noch eine Parameterdatei ein.
-OperatingSystemProfile -osp	operating_system_profile_name	Optional. Name des Betriebssystemprofils, das die Zuordnung ausführt. Wenn Sie diese Option nicht verwenden, wenn der Datenintegrationsdienst zur Verwendung von Betriebssystemprofilen eingerichtet ist, führt der Datenintegrationsdienst die Zuordnung mit dem Standardprofil aus.
-NodeName -nn	node_name	Optional. Name des Knotens in einem Datenintegrationsdienstgitter, an den der Zuordnungsjob gesendet werden soll. Ein Datenintegrationsdienstprozess muss auf dem Knoten ausgeführt werden. Wenn Sie diese Option nicht verwenden, wird der Zuordnungsjob an den Knoten gesendet, auf dem der Master-Prozess des Datenintegrationsdiensts ausgeführt wird.
-OptimizationLevel -ol	optimization_level	Optional. Steuert die Optimierungsmethoden, die der Datenintegrationsdienst auf die Zuordnung anwendet. Geben Sie den numerischen Wert ein, der mit der Optimierungsebene verbunden ist, die Sie konfigurieren möchten. Geben Sie einen der folgenden numerischen Werte ein: - 0 (Keine). Der Datenintegrationsdienst wendet keine Optimierung an. - 1 (Minimal). Der Datenintegrationsdienst wendet die Optimierungsmethode der frühen Projektion an. - 2 (Normal). Der Datenintegrationsdienst wendet folgende Optimierungsmethoden an: frühe Projektion, frühe Auswahl, Verzweigungsbereinigung, Push-Into, Pushdown und Prädikat. Normal ist die Standardoptimierungsebene. - 3 (Vollständig). Der Datenintegrationsdienst wendet folgende Optimierungsmethoden an: kostenbasiert, frühe Projektion, frühe Auswahl, Verzweigungsbereinigung, Prädikat, Push-Into, Pushdown und Semi-Join. Wenn Sie diese Option nicht verwenden, wendet der Datenintegrationsdienst die Optimierungsebene an, die in den Zuordnungseigenschaften für die bereitgestellte Anwendung im Administrator Tool konfiguriert wurde.

Option	Argument	Beschreibung
-PushdownType -pt	pushdown_type	Optional. Steuert den Pushdown-Typ, den der Datenintegrationsdienst auf eine Zuordnung anwendet. Geben Sie einen der folgenden Werte ein: - Keine. Wählt keinen Pushdown-Typ für die Zuordnung aus. - Quelle. Der Datenintegrationsdienst versucht, möglichst viel Umwandlungslogik in die Quelldatenbank zu übertragen. - Vollständig. Der Datenintegrationsdienst überträgt die vollständige Umwandlungslogik in die Quelldatenbank. Diese Option überschreibt den Pushdown-Typ, der in den Laufzeiteigenschaften der Zuordnung oder in einer Parameterdatei oder einem -satz festgelegt wurde. Wenn Sie diese Option nicht verwenden, wendet der Datenintegrationsdienst den Pushdown-Typ an, der in den Laufzeiteigenschaften der Zuordnung oder in einer Parameterdatei oder einem -satz festgelegt wurde.
-CustomProperties -cp	custom_properties	Optional. Definieren Sie benutzerdefinierte Eigenschaften für eine Zuordnung auf Anfrage des globalen Kundensupports von Informatica. Geben Sie benutzerdefinierte Eigenschaften als durch Semikola getrennte Namen-Wert-Paare ein. Beispiel: `... -cp custom_property_name=value` Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

UpgradeMappingParameterFile

Wandelt eine in einer vorherigen Informatica-Version erstellte Parameterdatei in ein Parameterdateiformat um, das für Informatica Version 10.0 gültig ist.

In Informatica Version 10.0 kann eine Parameterdatei Zuordnungs- und Arbeitsablaufparameter, aber keine Umwandlungsparameter mehr enthalten. Wenn Sie eine Zuordnung oder einen Arbeitsablauf in der mit einer früheren Version erstellten Parameterdatei ausführen, muss der Datenintegrationsdienst die Parameterdatei zur Laufzeit in die Informatica Version 10.0 konvertieren. Sie können die Leistung steigern, indem Sie Parameterdateien in das Informatica 10.0-Format konvertieren.

Der infacmd ms upgradeMappingParameterFile-Befehl verwendet die folgende Syntax:

```
UpgradeMappingParameterFile

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]
```

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

<-Application|-a> application_name

<-Mapping|-m> mapping_name

[<-OutputFile|-o> output file_to_write_to]

<-ParameterFile|-pf> parameter_file_to_upgrade
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ms upgradeMappingParameterFile“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch. Optional. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Bei der Sicherheitsdomäne wird die Groß-/Kleinschreibung beachtet. Standardwert ist „Nativ“.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	application_name	Erforderlich. Name der Anwendung, die die Zuordnung enthält.
-Mapping -m	mapping_name	Erforderlich. Name der Zuordnung.
- OutputFile - o	output file_to_write_to	Optional. Pfad und Dateiname der zu erstellenden Parameterdatei. Wenn Sie keine Datei angeben, zeigt der Befehl die Parameter in der Eingabeaufforderung an.
-ParameterFile -pf	parameter_file_to_upgrade	Erforderlich. Der Name der zu aktualisierenden Parameterdatei.

KAPITEL 18

Infacmd oie-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- DeployApplication, 748
- ExportObjects, 749
- exportResources, 753
- ImportObjects, 755

DeployApplication

Stellt eine Anwendung in einer .iar-Datei bereit.

Stellen Sie eine Anwendung in einer Datei bereit, wenn die Anwendung eine große Anzahl von Objekten enthält. Nachdem Sie den Befehl „infacmd oie deployApplication“ ausgeführt haben, führen Sie den Befehl „infacmd dis DeployApplication“ aus, um die Anwendung für einen Datenintegrationsdienst bereitzustellen.

Der Befehl „infacmd oie DeployApplication“ verwendet die folgende Syntax:

```
DeployApplication

<-DomainName|-dn> Domain name

<-UserName|-un> User name

<-Password|-pd> Password

<-ModelRepositoryService|-rs> Model Repository Service

<-OutputDirectory|-od> Output directory

<-ApplicationPath|-ap> Application path
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd oie DeployApplication“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	Domänenname	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	Benutzername	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ModelRepositoryService -rs	Modellrepository-Dienst	Erforderlich. Name des Modellrepository-Diensts.
- OutputDirectory -od	Ausgabeverzeichnis	Erforderlich. Verzeichnis, in das Sie die .iar-Datei schreiben möchten.
- ApplicationPath -ap	Anwendungspfad	Erforderlich. Der Anwendungspfad, beginnend mit den Projektnamen, Ordnernamen und gefolgt vom Namen der Anwendung. Trennen Sie den Projektnamen, Ordnernamen und den Namen der Anwendung mit einem Schrägstrich (/). Beispiel: „Projekt/Ordner1/Ordner2/Anwendung“.

ExportObjects

Exportiert Objekte aus einem Projekt im Modellrepository in eine XML-Datei.

Wenn Sie nicht alle Objekte im Projekt exportieren möchten, verwenden Sie eine infacmd-Exportsteuerdatei zum Filtern der Objekte im Modellrepository, die Sie exportieren möchten.

Wenn das zu exportierende Projekt Referenztabellen enthält, müssen Sie den Befehl über das Informatica-Dienste-Installationsverzeichnis ausführen. Der Befehl exportiert die Referenztabellenmetadaten aus dem Modellrepository in die XML-Datei. Der Befehl exportiert die Referenztabellendaten in eine ZIP-Datei. Wenn Sie den Befehl ausführen, geben Sie den Pfad und Dateinamen der zu erstellenden XML- und ZIP-Dateien an.

Der Befehl exportiert keine leeren Ordner.

Wenn der Befehl mit einem Java-Speicherfehler fehlschlägt, erhöhen Sie den verfügbaren Speicher für „infacmd“. Um den Systemspeicher zu erhöhen, legen Sie den Wert -Xmx in der Umgebungsvariable ICMD_JAVA_OPTS fest.

Der Befehl „infacmd oie ExportObjects“ verwendet die folgende Syntax:

```
ExportObjects

<-DomainName|-dn> Domain name

<-UserName|-un> User name

<-Password|-pd> Password

[<-SecurityDomain|-sdn> Security domain]

<-ProjectName|-pn> Project name

<-RepositoryService|-rs> Model Repository Service name

<-ExportFilePath|-fp> Path of file to export to

[<-OverwriteExportFile|-ow> Set to "true" to overwrite export file if it exists.]

[<-ControlFilePath|-cp> Path of export control file]

[<-OtherOptions|-oo>]
```


```
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]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd oie ExportObjects“ beschrieben:

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

Option	Argument	Beschreibung
-ExportFilePath -fp	Pfad der Datei zum Exportieren in	Erforderlich. Pfad und XML-Datei Name der zu erstellenden Exportdatei. Sie können einen absoluten Pfad oder einen relativen Pfad zum Dateinamen angeben. Verwenden Sie einen einfach zu unterscheidenden Namen für die Datei. Verwenden Sie beispielsweise die folgende vorgeschlagene Namenskonvention: `exp_<project_name>.xml`
-OverwriteExportFile -ow	Setzen Sie die Option auf „true“, um gegebenenfalls eine Exportdatei zu überschreiben.	Optional. Legen Sie die Option auf TRUE fest, um eine vorhandene Exportdatei zu überschreiben. Wenn eine Exportdatei vorhanden und diese Option auf FALSE festgelegt ist, schlägt der Export fehl. Standardwert ist „false“.
-ControlFilePath -cp	Pfad der Exportsteuerungsdatei	Optional. Pfad und Dateiname der Exportsteuerdatei, die die zu exportierenden Objekte filtert. Sie können einen absoluten Pfad oder einen relativen Pfad zu dem Dateinamen angeben.

-OtherOptions
-oo
	-	Erforderlich, wenn das zu exportierende Projekt Referenztabellen enthält. Zusätzliche Optionen zum Exportieren von Referenztabellendaten in eine ZIP-Datei. Geben Sie die Optionen im folgenden Format ein:
		`rtm:<option_name>=<value>,<option_name>=<value>`
		Erforderliche Optionsnamen enthalten:
		- disName. Name des Datenintegrationsdienst.
		- codePage. Codepage der Referenzdaten.
		- refDataFile. Pfad und Dateiname der ZIP-Datei, in die Sie die Referenztabellendaten exportieren möchten.
		Beispiel:
		`rtm:disName=ds,codePage=UTF-8,refDataFile=/folder1/data.zip`

Option	Argument	Beschreibung
-DomainName -dn	Domänenname	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	Benutzername	Erforderlich. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.
-Password -pd	Passwort	Erforderlich. Passwort für den Benutzernamen. Beim Passwort muss die Groß-/Kleinschreibung beachtet werden.
-SecurityDomain -sdn	Sicherheitsdomäne	Optional. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Bei der Sicherheitsdomäne wird die Groß-/Kleinschreibung beachtet. Standardwert ist „Native“.

Option	Argument	Beschreibung
-ProjectName -pn	Projektname	Erforderlich. Name des Projekts, aus dem die Objekte exportiert werden.
-RepositoryService -rs	Name des Modellrepository-Diensts	Erforderlich. Name des Modellrepository-Diensts.
-ExportFilePath -fp	Pfad der Datei zum Exportieren in	Erforderlich. Pfad und XML-Datei Name der zu erstellenden Exportdatei. Sie können einen absoluten Pfad oder einen relativen Pfad zum Dateinamen angeben. Verwenden Sie einen einfach zu unterscheidenden Namen für die Datei. Verwenden Sie beispielsweise die folgende vorgeschlagene Namenskonvention: `exp_<project_name>.xml`
-OverwriteExportFile -ow	Setzen Sie die Option auf „true“, um gegebenenfalls eine Exportdatei zu überschreiben.	Optional. Legen Sie die Option auf TRUE fest, um eine vorhandene Exportdatei zu überschreiben. Wenn eine Exportdatei vorhanden und diese Option auf FALSE festgelegt ist, schlägt der Export fehl. Standardwert ist „false“.
-ControlFilePath -cp	Pfad der Exportsteuerungsdate i	Optional. Pfad und Dateiname der Exportsteuerdatei, die die zu exportierenden Objekte filtert. Sie können einen absoluten Pfad oder einen relativen Pfad zu dem Dateinamen angeben.

exportResources

Exportiert die Scorecard-Objekte und Herkunftsinformationen in einem Projekt oder Ordner in eine XML-Datei, die Sie in Metadata Manager verwenden.

Wenn Sie nicht alle Objekte im Projekt exportieren möchten, verwenden Sie eine infacmd-Exportsteuerdatei zum Filtern der zu exportierenden Objekte. Der Befehl exportiert keine leeren Ordner.

Wenn der Befehl mit einem Java-Speicherfehler fehlschlägt, erhöhen Sie den verfügbaren Speicher für „infacmd“. Um den Systemspeicher zu erhöhen, legen Sie den Wert `-Xmx` in der Umgebungsvariable `ICMD_JAVA_OPTS` fest.

Der Befehl „infacmd oie exportResources“ verwendet die folgende Syntax:

```
exportResources

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

<-ProjectName|-pn> project_name

<-RepositoryService|-rs> model_repository_service_name
```

```
<-ExportFilePath|-fp> export_file_path

[<-OverwriteExportFile|-ow> overwrite_export_file]

[<-ControlFilePath|-cp> control_file_path]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd oie exportResources“ beschrieben:

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

Option	Argument	Beschreibung
-RepositoryService -rs	model_repository_service_name	Erforderlich. Name des Modellrepository-Diensts.
-ExportFilePath -fp	export_file_path	Erforderlich. Pfad und XML-Dateiname der Exportdatei, die beim Ausführen des Befehls vom Befehlszeilenprogramm erstellt wird. Sie können einen absoluten Pfad oder einen relativen Pfad zu dem Dateinamen angeben. Verwenden Sie für die Datei einen Namen, der leicht zu unterscheiden ist. Verwenden Sie beispielsweise die folgende vorgeschlagene Namenskonvention: `exp_<project_name>.xml`
-OverwriteExportFile -ow	overwrite_export_file	Optional. Legen Sie die Option auf TRUE fest, um eine vorhandene Exportdatei zu überschreiben. Wenn eine Exportdatei vorhanden ist und Sie diese Option auf FALSE festlegen, schlägt der Export fehl. Standardwert ist „false“.
-ControlFilePath -cp	control_file_path	Optional. Pfad und Dateiname der Exportsteuerdatei, die die vom Befehlszeilenprogramm exportierten Objekte filtert. Sie können einen absoluten Pfad oder einen relativen Pfad zu dem Dateinamen angeben.

ImportObjects

Importiert Objekte aus einer XML-Datei in ein vorhandenes Projekt im Modellrepository.

Wenn Sie nicht alle Objekte in der Datei importieren möchten, verwenden Sie eine infacmd-Importsteuerdatei zum Filtern der Objekte im Modellrepository, die Sie importieren möchten.

Wenn die zu importierende Datei Referenztabellen enthält, müssen Sie den Befehl über das Informatica-Dienste-Installationsverzeichnis ausführen. Der Befehl importiert die Referenztabellenmetadaten aus der XML-Datei in das Modellrepository. Der Befehl importiert die Referenztabellendaten aus einer ZIP-Datei. Wenn Sie den Befehl ausführen, geben Sie den Pfad und Dateinamen der zu importierenden XML- und ZIP-Dateien an.

Wenn der Befehl mit einem Java-Speicherfehler fehlschlägt, erhöhen Sie den verfügbaren Speicher für „infacmd“. Um den Systemspeicher zu erhöhen, legen Sie den Wert „-Xmx“ in der Umgebungsvariable ICMD_JAVA_OPTS fest.

Der Befehl „infacmd oie ImportObjects“ verwendet die folgende Syntax:

```
ImportObjects

<-DomainName|-dn> Domain name

<-UserName|-un> User name

<-Password|-pd> Password

[<-SecurityDomain|-sdn> Security domain]

[<-TargetProject|-tp> Target project name <ignored if control file is specified>]

<-RepositoryService|-rs> Model Repository Service name
```

```
<-ImportFilePath|-fp> import_file_path

[<-SourceProject|-sp> Source project name in import file <ignored if control file is
specified>]

[<-TargetFolder|-tf> Target folder to import to <omit for root, ignored if control file
is specified>]

[<-SkipCRC|-sc> Set to "true" to skip CRC check on imported file.]

[<-ConflictResolution|-cr> Resolution type]

[<-ControlFilePath|-cp> Path of import control file]

[<-SkipCnxValidation|-scv> Set to "true" to skip connection validation.]

[<-OtherOptions|-oo>]


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.]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd oie ImportObjects“ beschrieben:

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

Option	Argument	Beschreibung
-TargetProject -tp	Zielprojektname <wird ignoriert, wenn Steuerungsdatei angegeben wurde>	Optional. Name des Projekts, in das die Objekte importiert werden sollen. Das Projekt muss im Repository vorhanden sein, bevor Sie die Objekte importieren. Die Option wird ignoriert, wenn Sie eine Importsteuerungsdatei verwenden.
-RepositoryService - rs	Name des Modellrepository-Diensts	Erforderlich. Name des Modellrepository-Diensts.
-ImportFilePath -fp	import_file_path	Erforderlich. Pfad und Dateiname der XML-Datei, aus der die Objekte importiert werden sollen. Sie können einen absoluten Pfad oder einen relativen Pfad für den Dateinamen angeben.
-SourceProject -sp	Name des Quellprojekts in Importdatei <wird ignoriert, wenn Steuerungsdatei angegeben wurde>	Optional. Name des Quellprojekts in der zu importierenden Datei. Die Option wird ignoriert, wenn Sie eine Importsteuerungsdatei verwenden.
-TargetFolder -tf	Zielordner zum Importieren in <für Root weglassen, wird ignoriert, wenn Steuerungsdatei angegeben wurde>	Optional. Zielordner, in den Sie die Objekte importieren möchten. Wenn Sie keinen Zielordner angeben, werden die Objekte in das Zielprojekt importiert. Der Ordner muss im Repository vorhanden sein, bevor Sie die Objekte importieren. Die Option wird ignoriert, wenn Sie eine Importsteuerungsdatei verwenden.
-SkipCRC -sc	Legen Sie diese Option auf TRUE fest, um die CRC-Prüfung für die importierte Datei zu überspringen.	Gibt an, ob die zyklische Redundanzprüfung (Cyclic Redundancy Check, CRC) übersprungen werden soll, mit der festgestellt wird, ob die zu importierende Datei geändert wurde. Legen Sie die Option auf TRUE fest, um die Prüfung zu überspringen. Standardwert ist „false“.
-ConflictResolution -cr	Angegebener Lösungstyp	Optional. Konfliktlösungsstrategie. Sie können eine der folgenden Optionen für alle zu importierenden Objekte angeben: - umbenennen - ersetzen - erneut verwenden - none Die Option wird ignoriert, wenn Sie eine Importsteuerungsdatei verwenden. Wenn die Konfliktlösungsstrategie auf KEINE festgelegt ist und ein Konflikt auftritt, schlägt der Import fehl. Standardwert ist „Keine“.
-ControlFilePath -cp	Pfad der Importsteuerungsdatei	Optional. Pfad und Dateiname der Importsteuerungsdatei, die die zu importierenden Objekte filtert. Sie können einen absoluten Pfad oder einen relativen Pfad angeben.

Option	Argument	Beschreibung
-SkipCnxValidation -scv	Legen Sie die Option auf TRUE fest, um die Verbindungsvalidierung zu überspringen.	Optional. Gibt an, ob die Validierung der Zielverbindung während des Imports übersprungen werden soll. Der Importprozess stellt standardmäßig sicher, dass die von den importierten Objekten verwendeten Verbindungen im Zielrepository vorhanden sind. Wenn die Verbindungen nicht vorhanden sind, schlägt der Import fehl. Um die Validierung der Zielverbindung zu überspringen und mit dem Import fortzufahren, legen Sie diese Option auf TRUE fest. Wenn die importierten Objekte Verbindungen verwenden, die im Zielrepository nicht vorhanden sind, importiert der Importprozess die Objekte mit einer nicht angegebenen Verbindung. Verwenden Sie das Developer Tool, um nach Abschluss des Importprozesses die richtige Verbindung auszuwählen. Standardwert ist „false“. **Hinweis:** Wenn eine Import-Steuerdatei eine Quellverbindung angibt, die in der Datei, die Sie importieren, nicht vorhanden ist, schlägt der Importprozess unabhängig vom Wert dieser Option fehl. Um den Fehler zu korrigieren, stellen Sie sicher, dass das rebind-Element für die Verbindung in der Import-Steuerdatei Quellverbindungen enthält, die in der von Ihnen importierten Datei vorhanden sind.

-OtherOptions
-oo
	-	Erforderlich, wenn die Importdatei Referenztabellen enthält. Zusätzliche Optionen für den Import von Referenztabellendaten aus einer ZIP-Datei. Geben Sie die Optionen in folgendem Format ein:
		`rtm:<option_name>=<value>,<option_name>=<value>`
		Zu den erforderlichen Optionsnamen gehören:
		- disName. Name des Datenintegrationsdiensts.
		- codePage. Codepage der Referenzdaten.
		- refDataFile. Pfad und Dateiname der ZIP-Datei, aus der Sie die Referenztabellendaten importieren möchten.
		Beispiel:
		`rtm:disName=ds,codePage=UTF-8,refDataFile=/folder1/data.zip`

Option	Argument	Beschreibung
-DomainName -dn	Domänenname	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen

Option	Argument	Beschreibung
		Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	Benutzername	Erforderlich. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.
-Password -pd	Password	Erforderlich. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet.
-SecurityDomain -sdn	Sicherheitsdomäne	Optional. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Bei der Sicherheitsdomäne wird die Groß-/Kleinschreibung beachtet. Standardwert ist „Nativ“.
-TargetProject -tp	Zielprojektname <wird ignoriert, wenn Steuerungsdatei angegeben wurde>	Optional. Name des Projekts, in das die Objekte importiert werden sollen. Das Projekt muss im Repository vorhanden sein, bevor Sie die Objekte importieren. Die Option wird ignoriert, wenn Sie eine Importsteuerungsdatei verwenden.
-RepositoryService - rs	Name des Modellrepository-Diensts	Erforderlich. Name des Modellrepository-Diensts.
-ImportFilePath -fp	import_file_path	Erforderlich. Pfad und Dateiname der XML-Datei, aus der die Objekte importiert werden sollen. Sie können einen absoluten Pfad oder einen relativen Pfad für den Dateinamen angeben.
-SourceProject -sp	Name des Quellprojekts in Importdatei <wird ignoriert, wenn Steuerungsdatei angegeben wurde>	Optional. Name des Quellprojekts in der zu importierenden Datei. Die Option wird ignoriert, wenn Sie eine Importsteuerungsdatei verwenden.
-TargetFolder -tf	Zielordner zum Importieren in <für Root weglassen, wird ignoriert, wenn Steuerungsdatei angegeben wurde>	Optional. Zielordner, in den Sie die Objekte importieren möchten. Wenn Sie keinen Zielordner angeben, werden die Objekte in das Zielprojekt importiert. Der Ordner muss im Repository vorhanden sein, bevor Sie die Objekte importieren. Die Option wird ignoriert, wenn Sie eine Importsteuerungsdatei verwenden.
-SkipCRC -sc	Legen Sie diese Option auf TRUE fest, um die CRC-Prüfung für die importierte Datei zu überspringen.	Gibt an, ob die zyklische Redundanzprüfung (Cyclic Redundancy Check, CRC) übersprungen werden soll, mit der festgestellt wird, ob die zu importierende Datei geändert wurde. Legen Sie die Option auf TRUE fest, um die Prüfung zu überspringen. Standardwert ist „false“.

Option	Argument	Beschreibung
-ConflictResolution -cr	Angegebener Lösungstyp	Optional. Konfliktlösungsstrategie. Sie können eine der folgenden Optionen für alle zu importierenden Objekte angeben: - umbenennen - ersetzen - erneut verwenden - none Die Option wird ignoriert, wenn Sie eine Importsteuerungsdatei verwenden. Wenn die Konfliktlösungsstrategie auf KEINE festgelegt ist und ein Konflikt auftritt, schlägt der Import fehl. Standardwert ist „Keine“.
-ControlFilePath -cp	Pfad der Importsteuerungsdatei	Optional. Pfad und Dateiname der Importsteuerungsdatei, die die zu importierenden Objekte filtert. Sie können einen absoluten Pfad oder einen relativen Pfad angeben.
-SkipCnxValidation -scv	Legen Sie die Option auf TRUE fest, um die Verbindungsvalidierung zu überspringen.	Optional. Gibt an, ob die Validierung der Zielverbindung während des Imports übersprungen werden soll. Der Importprozess stellt standardmäßig sicher, dass die von den importierten Objekten verwendeten Verbindungen im Zielrepository vorhanden sind. Wenn die Verbindungen nicht vorhanden sind, schlägt der Import fehl. Um die Validierung der Zielverbindung zu überspringen und mit dem Import fortzufahren, legen Sie diese Option auf TRUE fest. Wenn die importierten Objekte Verbindungen verwenden, die im Zielrepository nicht vorhanden sind, importiert der Importprozess die Objekte mit einer nicht angegebenen Verbindung. Verwenden Sie das Developer Tool, um nach Abschluss des Importprozesses die richtige Verbindung auszuwählen. Standardwert ist „false“. **Hinweis:** Wenn eine Import-Steuerdatei eine Quellverbindung angibt, die in der Datei, die Sie importieren, nicht vorhanden ist, schlägt der Importprozess unabhängig vom Wert dieser Option fehl. Um den Fehler zu korrigieren, stellen Sie sicher, dass das rebind-Element für die Verbindung in der Import-Steuerdatei Quellverbindungen enthält, die in der von Ihnen importierten Datei vorhanden sind.

KAPITEL 19

infacmd ps-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- cancelProfileExecution, 762
- CreateWH, 764
- DropWH, 766
- Execute, 767
- executeProfile, 770
- getExecutionStatus, 772
- getProfileExecutionStatus, 773
- List, 775
- migrateProfileResults, 777
- migrateScorecards, 779
- Purge, 780
- synchronizeProfile, 783

cancelProfileExecution

Stoppt alle Profilausführungen, einschließlich der Profile sowie des Enterprise-Erkennungsprofils.

Der Befehl „infacmd ps cancelProfileExecution“ verwendet die folgende Syntax:

```
cancelProfileExecution
<-DomainName|-dn> domain_name
[<-Gateway|-hp> gateway_name]
[<-NodeName|-nn> node_name]
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-MrsServiceName|-msn> MRS_name
<-DsServiceName|-dsn> data_integration_service_name
<-ObjectPathAndName|-opn> MRS_object_path
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd ps cancelProfileExecution“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-NodeName -nn	node_name	Optional. Name des Knotens, auf dem der Datenintegrationsdienst ausgeführt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-MrsServiceName -msn	MRS_name	Erforderlich. Name des Modellrepository-Diensts.
-DsServiceName -dsn	data_integration_service_name	Erforderlich. Name des Datenintegrationsdiensts.
-ObjectPathAndName -opn	MRS_object_path	Erforderlich. Verwenden Sie folgende Syntax: `ProjectName/FolderName/.../SubFolder_Name/{ObjectName|ProjectName/ObjectName}`

CreateWH

Erstellt den Inhalt des Profiling Warehouse.

Der Befehl „infacmd ps CreateWH“ verwendet die folgende Syntax:

```
CreateWH

<-DomainName|-dn> domain_name

[<-Gateway|-hp>] gateway_name]

<-UserName|-un> user_name

<-Password|-pd> Password

[<-SecurityDomain|-sdn> security_domain]

<-DsServiceName|-dsn> data_integration_service_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ps CreateWH“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-Gateway -hp	gateway_name	Optional. Verwenden Sie diese Option, wenn die Gateway-Konnektivitätsinformationen in der Datei „domains.infa“ veraltet sind. Geben Sie den Hostnamen und die Portnummer für den Gateway-Knoten in der Domäne ein. Verwenden Sie die folgende Syntax: gateway_hostname:port.

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

DropWH

Entfernt den Inhalt des Profiling Warehouse.

Der Befehl „infacmd ps DropWH“ verwendet die folgende Syntax:

```
DropWH

<-DomainName|-dn> domain_name

[<-Gateway|-hp>] gateway_name]

<-UserName|-un> user_name

<-Password|-pd> Password

[<-SecurityDomain|-sdn> security_domain]

<-DsServiceName|-dsn> data_integration_service_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ps DropWH“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-Gateway -hp	gateway_name	Optional. Verwenden Sie diese Option, wenn die Gateway-Konnektivitätsinformationen in der Datei „domains.infa“ veraltet sind. Geben Sie den Hostnamen und die Portnummer für den Gateway-Knoten in der Domäne ein. Verwenden Sie die folgende Syntax: gateway_hostname:port.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang. Erforderlich. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch. Optional. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Bei der Sicherheitsdomäne wird die Groß-/Kleinschreibung beachtet. Standardwert ist „Native“.
-DsServiceName -dsn	data_integration_service_name	Erforderlich. Name des Datenintegrationsdiensts.

.

Execute

Führt ein Profil oder eine Scorecard aus.

Der Befehl „infacmd ps Execute“ verwendet die folgende Syntax:

```
Execute

<-DomainName|-dn> domain_name

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-NodeName|-nn> node_name]

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

<-MrsServiceName|-msn> MRS_name

<-DsServiceName|-dsn> data_integration_service_name

<-ObjectType|-ot> object_type

<-ObjectPathAndName|-opn> MRS_object_path

[<-ProfileName|-pt> profile_task_name]
```

```
[<-wait|-w> true|false]

[<-ospn|-OsProfileName> os_profile_name]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ps Execute“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-NodeName -nn	node_name	Optional. Name des Knotens, auf dem der Datenintegrationsdienst ausgeführt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-MrsServiceName -msn	MRS_name	Erforderlich. Name des Modellrepository-Diensts.
-DsServiceName -dsn	data_inetgration_service_name	Erforderlich. Name des Datenintegrationsdiensts.
-ObjectType -ot	object_type	Erforderlich. Geben Sie ein Profil oder eine Scorecard ein.
-ObjectPathandName -opn	MRS_object_path	Erforderlich. Verwenden Sie folgende Syntax: `ProjectName/FolderName/.../SubFolder_Name/{ObjectName|ProjectName/ObjectName}`
-ProfileName -pt	profile_task_name	Optional. Name einer Profilaufgabe im Enterprise-Erkennungsprofil.
-Wait -w	true|false	Optional. Wenn TRUE, wird vor der Rückkehr zur Eingabeaufforderung gewartet, bis der Befehl abgeschlossen ist. Wenn FALSE, wird zur Eingabeaufforderung zurückgekehrt, bevor der Befehl abgeschlossen ist. Standardwert ist „False“.
-ospn -OsProfileName	os_profile_name	Optional. Der Name des Betriebssystemprofils, wenn der Datenintegrationsdienst für die Verwendung von Betriebssystemprofilen eingerichtet ist.

executeProfile

Führt ein Enterprise-Erkennungsprofil aus.

Der Befehl „infacmd ps executeProfile“ verwendet die folgende Syntax:

```
executeProfile

<-DomainName|-dn> domain_name

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-NodeName|-nn> node_name]

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

<-MrsServiceName|-msn> MRS_name

<-DsServiceName|-dsn> data_integration_service_name

<-ObjectPathAndName|-opn> MRS_object_path

[<-WaitForModelExecToFinish|-w> true|false]

[<-ospn|-OsProfileName> os_profile_name]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ps executeProfile“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-NodeName -nn	node_name	Optional. Name des Knotens, auf dem der Datenintegrationsdienst ausgeführt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-MrsServiceName -msn	MRS_name	Erforderlich. Name des Modellrepository-Diensts.
-DsServiceName -dsn	data_inetgration_service_name	Erforderlich. Name des Datenintegrationsdiensts.
-ObjectPathandName -opn	MRS_object_path	Erforderlich. Verwenden Sie folgende Syntax: `ProjectName/FolderName/.../SubFolder_Name/{ObjectName|ProjectName/ObjectName}`
-WaitForModelExecToFinish -w	true|false	Optional. Wenn TRUE, wird vor der Rückkehr zur Eingabeaufforderung gewartet, bis der Befehl abgeschlossen ist. Wenn FALSE, wird zur Eingabeaufforderung zurückgekehrt, bevor der Befehl abgeschlossen ist. Standardwert ist „False“.
-ospn -OsProfileName	os_profile_name	Optional. Der Name des Betriebssystemprofils, wenn der Datenintegrationsdienst für die Verwendung von Betriebssystemprofilen eingerichtet ist.

getExecutionStatus

Ruft den Laufzeitstatus von Profilaufgaben in einem Enterprise-Erkennungsprofil ab.

Der Befehl „infacmd ps getExecutionStatus“ verwendet die folgende Syntax:

```
getExecutionStatus

<-DomainName|-dn> domain_name

[<-Gateway|-hp> gateway_name]

[<-NodeName|-nn> node_name]

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

<-MrsServiceName|-msn> MRS_name

<-DsServiceName|-dsn> data_integration_service_name

<-ObjectType|-ot> object_type

<-ObjectPathAndName|-opn> MRS_object_path

<-ProfileTaskName|-pt> profile_task_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ps getExecutionStatus“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-NodeName -nn	node_name	Optional. Name des Knotens, auf dem der Datenintegrationsdienst ausgeführt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-MrsServiceName -msn	MRS_name	Erforderlich. Name des Modellrepository-Diensts.
-DsServiceName -dsn	data_integration_service_name	Erforderlich. Name des Datenintegrationsdiensts.
-ObjectType -ot	object_type	Erforderlich. Geben Sie ein Profil oder eine Scorecard ein.
-ObjectPathAndName -opn	MRS_object_path	Erforderlich. Verwenden Sie folgende Syntax: `ProjectName/FolderName/.../SubFolder_Name/{ObjectName|ProjectName/ObjectName}`
-ProfileTaskName -pt	profile_task_name	Optional. Name einer Profilaufgabe im Enterprise-Erkennungsprofil.

getProfileExecutionStatus

Ruft den Laufzeitstatus eines Enterprise-Erkennungsprofils ab. Der Befehl listet auch alle Profilaufgaben im Enterprise-Erkennungsprofil sowie deren Laufzeitstatusangaben ab.

Der Befehl „infacmd ps getProfileExecutionStatus“ verwendet die folgende Syntax:

```
getProfileExecutionStatus
```

```
<-DomainName|-dn> domain_name

[<-Gateway|-hp> gateway_name]

[<-NodeName|-nn> node_name]

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

<-MrsServiceName|-msn> MRS_name

<-DsServiceName|-dsn> data_integration_service_name

<-ObjectPathAndName|-opn> MRS_object_path
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ps getProfileExecutionStatus“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-NodeName -nn	node_name	Optional. Name des Knotens, auf dem der Datenintegrationsdienst ausgeführt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-MrsServiceName -msn	MRS_name	Erforderlich. Name des Modellrepository-Diensts.
-DsServiceName -dsn	data_integration_service_name	Erforderlich. Name des Datenintegrationsdiensts.
-ObjectPathAndName -opn	MRS_object_path	Erforderlich. Verwenden Sie folgende Syntax: `ProjectName/FolderName/.../SubFolder_Name/{ObjectName|ProjectName/ObjectName}`

List

Listet Profile und Scorecards auf.

Der Befehl „infacmd ps List“ verwendet die folgende Syntax:

```
List

<-DomainName|-dn> domain_name

[<-Gateway|-hp> gateway_name]

[<-NodeName|-nn>] node_name

<-MrsServiceName|-msn> MRS_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

<-ObjectType|-ot>

<-FolderPath|-fp> full_folder_path

[<-Recursive|-r>]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ps List“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-NodeName -nn	node_name	Optional. Name des Knotens, auf dem der Datenintegrationsdienst ausgeführt wird.
-MrsServiceName -msn	MRS_name	Erforderlich. Name des Modellrepository-Diensts.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-ObjectType -ot	-	Erforderlich. Geben Sie ein Profil oder eine Scorecard ein.
-FolderPath -fp	full_folder_path	Erforderlich. Geben Sie den Pfad des Ordners ein, der die aufzulistenden Objekte enthält. Verwenden Sie folgende Syntax: `Project_name/folder_name/../SubFolderName`
-Recursive -r	-	Optional. Wendet den Befehl auf Objekte in dem von Ihnen angegebenen Ordner und seinen Unterordnern an.

migrateProfileResults

Migriert Spaltenprofilergebnisse und Ergebnisse der Datendomänenerkennung aus Version 9.1.0, 9.5.0 oder 9.5.1.

Der Befehl „infacmd ps migrateProfileResults“ verwendet die folgende Syntax:

```
migrateProfileResults

<-DomainName|-dn> domain_name

[<-Gateway|-hp> gateway_name]

[<-NodeName|-nn> node_name]

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

<-MrsServiceName|-msn> MRS_name

<-DsServiceName|-dsn> data_integration_service_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ps migrateProfileResults“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-NodeName -nn	node_name	Optional. Name des Knotens, auf dem der Datenintegrationsdienst ausgeführt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-MrsServiceName -msn	MRS_name	Erforderlich. Name des Modellrepository-Diensts.
-DsServiceName -dsn	data_integration_service_name	Erforderlich. Name des Datenintegrationsdiensts.

migrateScorecards

Migriert Scorecard-Ergebnisse aus Informatica 9.1.0 oder 9.5.0 bis 9.5.1.

Der Befehl „infacmd ps migrateScorecards“ verwendet die folgende Syntax:

```
migrateScorecards
<-DomainName|-dn> domain_name
[<-Gateway|-hp> gateway_name]
[<-NodeName|-nn> node_name]
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-MrsServiceName|-msn> MRS_name
<-DsServiceName|-dsn> data_integration_service_name
<-migrateFrom|-mfr> migrate_from_release
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ps migrateScorecards“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-NodeName -nn	node_name	Optional. Name des Knotens, auf dem der Datenintegrationsdienst ausgeführt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.

Option	Argument	Beschreibung
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-MrsServiceName -msn	MRS_name	Erforderlich. Name des Modellrepository-Diensts.
-DsServiceName -dsn	data_integration_service_name	Erforderlich. Name des Datenintegrationsdiensts.
-migrateFrom -mfr	migrate_from_release	Erforderlich. Version von Daten-Explorer, von der die Migration erfolgt. Die Version kann entweder 9.1.0 oder 9.5.0 sein.

Purge

Bereinigt Profil- oder Scorecard-Ergebnisse aus dem Profiling Warehouse.

Der Befehl „infacmd ps Purge“ verwendet die folgende Syntax:

```
Purge

<-DomainName|-dn> domain_name

[<-Gateway|-hp> gateway_name]

[<-NodeName|-nn>] node_name

<-UserName|-un> user_name

<-Password|-pd> Password
```

```
[<-SecurityDomain|-sdn> security_domain]

<-MrsServiceName|-msn> MRS_name

<-DsServiceName|-dsn> data_integration_service_name

<-ObjectType|-ot> object_type

<-ObjectPathAndName|-opn> MRS_object_path

[<-RetainDays|-rd> results_retain_days]

[<-ProjectFolderPath|-pf> project_folder_path]

[<-ProfileName|-pt> profile_task_name]

[<-Recursive|-r> recursive]

[<-PurgeAllResults|-pa> purge_all_results]
```

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

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Der Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-Gateway -hp	gateway_name	Optional, wenn Sie den Befehl aus dem Informatica-Installationsverzeichnis \bin ausführen. Erforderlich, wenn Sie den Befehl von einem anderen Speicherort aus ausführen. Der Name des Gateway-Knotens. Verwenden Sie folgende Syntax: `[Domain_Host]:[HTTP_Port]`
-NodeName -nn	node_name	Erforderlich. Der Name des Knotens, auf dem der Datenintegrationsdienst ausgeführt wird.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-MrsServiceName -msn	MRS_name	Erforderlich. Der Modellrepository-Dienstname.
-DsServiceName -dsn	data_integration_service_name	Erforderlich. Der Datenintegrationsdienst-Name.
-ObjectType -ot	-	Erforderlich. Geben Sie ein Profil oder eine Scorecard ein.
-ObjectPathAndName -opn *	MRS_object_path	Optional. Nicht mit ProjectFolderPath oder Recursive verwenden. Der Pfad zum Profil oder zur Scorecard im Modellrepository. Verwenden Sie folgende Syntax: `ProjectName/FolderName/.../{SubFolder_Name/ObjectName|ProjectName/ObjectName}`
-RetainDays -rd	results_retain_days	Optional. Die Anzahl an Tagen, die das Profiling Warehouse Profil- oder Scorecard-Ergebnisse speichert, bevor diese bereinigt werden.
-ProjectFolderPath -pf *	project_folder_path	Optional. Nicht mit ObjectPathAndName oder ProfileTaskName verwenden. Die Namen des Projekts und Ordners, in denen das Profil oder die Scorecard gespeichert ist. Verwenden Sie folgende Syntax: `ProjectName/FolderName`
-ProfileName -pt *	profile_task_name	Optional. Der Name der Profilaufgabe, die Sie löschen möchten. Wenn Sie ProjectFolderPath angeben, müssen Sie diese Option nicht angeben, da ProjectFolderPath den Namen des Enterprise-Erkennungsprofils enthält, das die Profilaufgabe enthält.
-Recursive -r	recursive	Optional. Nicht mit ObjectPathAndName verwenden. Wendet den Befehl auf Objekte in dem angegebenen Ordner und seinen Unterordnern an.

Option	Argument	Beschreibung
-PurgeAllResults -pa	purge_all_results	Optional. Legen Sie diese Option fest, um alle Ergebnisse für das Profil- oder Scorecard-Objekt zu bereinigen. Verwenden Sie die -recursive-Option, um den Befehl auf Profil- und Scorecard-Ergebnisse in dem angegebenen Ordner und seinen Unterordnern anzuwenden.
* Um den Befehl auszuführen, müssen Sie ObjectPathAndName oder ProjectFolderPath oder ProfileTaskName angeben.		

synchronizeProfile

Migriert dokumentierte, benutzerdefinierte und übernommene Primär- und Fremdschlüssel für alle Profile in einem Projekt der Version 9.1.0, 9.5.0 oder 9.5.1.

Der Befehl „infacmd ps synchronizeProfile“ verwendet die folgende Syntax:

```
synchronizeProfile

<-DomainName|-dn> domain_name

[<-Gateway|-hp> gateway_name]

[<-NodeName|-nn> node_name]

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

<-MrsServiceName|-msn> MRS_name

<-DsServiceName|-dsn> data_integration_service_name

<-ProjectName|-pn> project_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ps synchronizeProfile“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-NodeName -nn	node_name	Optional. Name des Knotens, auf dem der Datenintegrationsdienst ausgeführt wird.

Option	Argument	Beschreibung
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-MrsServiceName -msn	MRS_name	Erforderlich. Name des Modellrepository-Diensts.
-DsServiceName -dsn	data_integration_service_name	Erforderlich. Name des Datenintegrationsdiensts.
-ProjectName -pn	project_name	Erforderlich. Projektname.

KAPITEL 20

infacmd pwx-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- CloseForceListener, 785
- CloseListener, 788
- CondenseLogger, 791
- createdatamaps, 794
- CreateListenerService, 797
- CreateLoggerService, 799
- DisplayAllLogger, 804
- DisplayCPULogger, 807
- DisplayEventsLogger, 810
- DisplayMemoryLogger, 813
- DisplayRecordsLogger, 816
- displayStatsListener, 819
- DisplayStatusLogger, 822
- FileSwitchLogger, 825
- ListTaskListener, 828
- ShutDownLogger, 831
- StopTaskListener, 834
- UpgradeModels, 837
- UpdateListenerService, 840
- UpdateLoggerService, 844

CloseForceListener

Erzwingt den Abbruch lang andauernder Unteraufgaben auf dem PowerExchange-Listenerdienst und stoppt den Listenerdienst.

Wenn Sie den Befehl infacmd pwx CloseForceListener verwenden, schließt PowerExchange die folgenden Aktionen ab:

1. Prüfen, ob alle Unteraufgaben im Listenerdienst aktiv sind.

2. Sind aktive Unteraufgaben vorhanden, wird die Anzahl der Unteraufgaben über einen Zeitraum von 30 Sekunden im Sekundentakt abgefragt.
3. Während dieses Zeitraums wird jede Unteraufgabe angehalten, die auf eine TCP/IP-Netzwerkeingabe wartet.
4. Abbrechen aller verbleibenden aktiven Unteraufgaben.
5. Anhalten des Listenerdiensts.

Der Befehl „infacmd pwx CloseForceListener“ verwendet die folgende Syntax:

```
CloseForceListener

[<-DomainName|-dn> domain_name]

[<-UserName|-un> user_name]

[<-Password|-pd> password]

<-ServiceName|-sn> service_name

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-OSUser|-oun> OS_user_name]

[<-OSPassword|-oup> OS_password]

[<-OSEPassword|-ouep> OS_epassword]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx CloseForceListener“ beschrieben:

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

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Listenerdiensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-OSUser -oun	OS_user_name	Erforderlich, wenn Sie Betriebssystemsicherheit aktiviert haben. Benutzername für das Betriebssystem. Aktivieren Sie Betriebssystemsicherheit wie folgt: - Damit Benutzer eine gültige Benutzer-ID und ein gültiges Passwort für das Betriebssystem im Befehl eingeben, legen Sie 1 oder 2 für den ersten Parameter der SECURITY-Anweisung in der DBMOVER-Konfigurationsdatei auf jedem Linux-, UNIX- oder Windows-System fest, das als Target des Befehls fungiert. PowerExchange verwendet Betriebssystemfunktionen auf dem Target-System, um die Benutzer-ID und das Passwort für die Verwendung des infacmd pwx-Programms zu authentifizieren. - Um Benutzer für die Ausführung bestimmter infacmd pwx-Befehle zu authentifizieren, legen Sie 2 für den ersten Parameter der SECURITY-Anweisung fest und definieren Sie die AUTHGROUP- und USER-Anweisungen in der PowerExchange-Anmeldedatei auf jedem Linux-, UNIX- oder Windows-System, das als Target des Befehls fungiert. PowerExchange überprüft die Anmeldedatei, um zu bestimmen, ob der im infacmd pwx-Programm bereitgestellten Benutzer-ID die Ausführung von Befehlen gewährt werden soll. Weitere Informationen finden Sie im *PowerExchange-Referenzhandbuch*.
-OSPassword -oup	OS_password	Erforderlich, wenn Sie einen Benutzernamen ohne verschlüsseltes Passwort festlegen. Passwort für das Betriebssystem. Sie können ein Klartextpasswort mit der Option -p oder der Umgebungsvariable INFA_DEFAULT_PWX_OSPASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -p festgelegte Passwort Vorrang.
-OSEPassword -ouep	OS_epassword	Erforderlich, wenn Sie einen Benutzernamen ohne Klartextpasswort festlegen. Verschlüsseltes Passwort für das Betriebssystem. Sie können ein verschlüsseltes Passwort mit der Option -e oder der Umgebungsvariable INFA_DEFAULT_PWX_OSEPASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -e festgelegte Passwort Vorrang.

CloseListener

Hält den PowerExchange-Listenerdienst an, wenn alle ausstehenden Unteraufgaben im Listenerdienst abgeschlossen sind.

Hinweis: Befinden sich im Listenerdienst lang andauernde Unteraufgaben, verwenden Sie den Befehl „infacmd pwx closeforceListener“, um den Abbruch aller Unteraufgaben zu erzwingen und den Listenerdienst anzuhalten.

Der Befehl „infacmd pwx CloseListener“ verwendet die folgende Syntax:

```
CloseListener
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-OSUser|-oun> OS_user_name]
[<-OSPassword|-oup> OS_password]
[<-OSEPassword|-ouep> OS_epassword]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx CloseListener“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-OSUser -oun	OS_user_name	Erforderlich, wenn Sie Betriebssystemsicherheit aktiviert haben. Benutzername für das Betriebssystem. Aktivieren Sie Betriebssystemsicherheit wie folgt: - Damit Benutzer eine gültige Benutzer-ID und ein gültiges Passwort für das Betriebssystem im Befehl eingeben, legen Sie 1 oder 2 für den ersten Parameter der SECURITY-Anweisung in der DBMOVER-Konfigurationsdatei auf jedem Linux-, UNIX- oder Windows-System fest, das als Target des Befehls fungiert. PowerExchange verwendet Betriebssystemfunktionen auf dem Target-System, um die Benutzer-ID und das Passwort für die Verwendung des infacmd pwx-Programms zu authentifizieren. - Um Benutzer für die Ausführung bestimmter infacmd pwx-Befehle zu authentifizieren, legen Sie 2 für den ersten Parameter der SECURITY-Anweisung fest und definieren Sie die AUTHGROUP- und USER-Anweisungen in der PowerExchange-Anmeldedatei auf jedem Linux-, UNIX- oder Windows-System, das als Target des Befehls fungiert. PowerExchange überprüft die Anmeldedatei, um zu bestimmen, ob der im infacmd pwx-Programm bereitgestellten Benutzer-ID die Ausführung von Befehlen gewährt werden soll.

Option	Argument	Beschreibung
-OSPassword -oup	OS_password	Erforderlich, wenn Sie einen Benutzernamen ohne verschlüsseltes Passwort festlegen. Passwort für das Betriebssystem. Sie können ein Klartextpasswort mit der Option -p oder der Umgebungsvariable INFA_DEFAULT_PWX_OSPASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -p festgelegte Passwort Vorrang.
-OSEPassword -ouep	OS_epassword	Erforderlich, wenn Sie einen Benutzernamen ohne Klartextpasswort festlegen. Verschlüsseltes Passwort für das Betriebssystem. Sie können ein verschlüsseltes Passwort mit der Option -e oder der Umgebungsvariable INFA_DEFAULT_PWX_OSEPASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -e festgelegte Passwort Vorrang.

CondenseLogger

Startet einen weiteren Logging-Zyklus, bevor die Wartezeit für das Starten eines anderen Zyklus verstrichen ist, wenn der PowerExchange-Protokollierungsdienst im fortlaufenden Modus ausgeführt wird. Legen Sie die Wartezeit im Parameter NO_DATA_WAIT der Konfigurationsdatei „pwxccl.cfg“ fest.

Der Befehl „infacmd pwx CondenseLogger“ verwendet die folgende Syntax:

```
CondenseLogger

[<-DomainName|-dn> domain_name]

[<-UserName|-un> user_name]

[<-Password|-pd> password]

<-ServiceName|-sn> service_name

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-OSUser|-oun> OS_user_name]

[<-OSPassword|-oup> OS_password]

[<-OSEPassword|-ouep> OS_epassword]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx CondenseLogger“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-OSUser -oun	OS_user_name	Erforderlich, wenn Sie Betriebssystemsicherheit aktiviert haben. Benutzername für das Betriebssystem. Aktivieren Sie Betriebssystemsicherheit wie folgt: - Damit Benutzer eine gültige Benutzer-ID und ein gültiges Passwort für das Betriebssystem im Befehl eingeben, legen Sie 1 oder 2 für den ersten Parameter der SECURITY-Anweisung in der DBMOVER-Konfigurationsdatei auf jedem Linux-, UNIX- oder Windows-System fest, das als Target des Befehls fungiert. PowerExchange verwendet Betriebssystemfunktionen auf dem Target-System, um die Benutzer-ID und das Passwort für die Verwendung des infacmd pwx-Programms zu authentifizieren. - Um Benutzer für die Ausführung bestimmter infacmd pwx-Befehle zu authentifizieren, legen Sie 2 für den ersten Parameter der SECURITY-Anweisung fest und definieren Sie die AUTHGROUP- und USER-Anweisungen in der PowerExchange-Anmeldedatei auf jedem Linux-, UNIX- oder Windows-System, das als Target des Befehls fungiert. PowerExchange überprüft die Anmeldedatei, um zu bestimmen, ob der im infacmd pwx-Programm bereitgestellten Benutzer-ID die Ausführung von Befehlen gewährt werden soll.

Option	Argument	Beschreibung
-OSPassword -oup	OS_password	Erforderlich, wenn Sie einen Benutzernamen ohne verschlüsseltes Passwort festlegen. Passwort für das Betriebssystem. Sie können ein Klartextpasswort mit der Option -p oder der Umgebungsvariable INFA_DEFAULT_PWX_OSPASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -p festgelegte Passwort Vorrang.
-OSEPassword -ouep	OS_epassword	Erforderlich, wenn Sie einen Benutzernamen ohne Klartextpasswort festlegen. Verschlüsseltes Passwort für das Betriebssystem. Sie können ein verschlüsseltes Passwort mit der Option -e oder der Umgebungsvariable INFA_DEFAULT_PWX_OSEPASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -e festgelegte Passwort Vorrang.

createdatamaps

Erstellt Datenzuordnungen für Massendatenbewegungsoperationen.

Verwenden Sie den Befehl createdatamaps zum Generieren von Datenzuordnungen für IMS-, SEQ- und VSAM-Datenquellen über die Befehlszeile. Dieser Befehl bietet in bestimmten Fällen eine Alternative zur Verwendung des PowerExchange Navigator und ermöglicht Ihnen, Datenzuordnungen nicht interaktiv zu generieren oder neu zu generieren.

Wenn der Befehl mit einem Java-Speicherfehler fehlschlägt, erhöhen Sie den verfügbaren Speicher für „infacmd“. Um den Systemspeicher zu erhöhen, legen Sie den Wert „-Xmx“ in der Umgebungsvariable ICMD_JAVA_OPTS fest. Weitere Informationen hierzu finden Sie unter “ICMD_JAVA_OPTS” auf Seite 41.

Der Befehl „infacmd pwx createdatamaps“ verwendet die folgende Syntax:

```
createdatamaps

[<-pwxLocation|-loc> pwx_location]

[<-pwxUserName|-pun> pwx_user_name]

[<-pwxPassword|-ppd> pwx_password]

[<-pwxEncryptedPassword|-epwd> pwx_encrypted_password]

[<-datamapOutputDir|-dod> datamap_output_directory]

[<-replace|-r> replace_existing_datamaps

<-controlFile|-cf> file_path_for_control_file

[<-logFile|-lf> file_path_for_log_file]

[<-verbosity|-v> logging_verbosity]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx createdatamaps“ beschrieben:

Option	Argument	Beschreibung
-pwxLocation -loc	pwx_location	Optional. Der Speicherort der Datenquelle, wie in einer NODE-Anweisung in der dbmover-Konfigurationsdatei von PowerExchange angegeben. Wenn pwxLocation nicht angegeben ist, greift das Dienstprogramm createdatamaps auf das Copybook und die DBD-Metadaten im lokalen Dateisystem zu. Wenn Sie die Steuerungsdatei zum Auffinden von Datensatz-IDs konfigurieren, ist pwxLocation erforderlich.
-pwxUserName -pun	pwx_user_name	Optional. Die Benutzer-ID für die Verbindung zum PowerExchange Listener, wenn pwxLocation angegeben ist.
-pwxPassword -ppd	pwx_password	Optional. Passwort für eine Verbindung zum PowerExchange Listener, wenn pwxLocation angegeben ist. Anstelle eines Passworts können Sie eine gültige PowerExchange Passphrase eingeben. Passphrasen für den Zugriff auf einen PowerExchange Listener unter z/OS kann von 9 bis 128 Zeichen lang sein und folgende Zeichen enthalten: - Groß- und Kleinbuchstaben - Die Zahlen 0 bis 9 - Leerzeichen - Die folgenden Sonderzeichen: `' - ; # \ , . / ! % & * ( ) _ + { } : @ | < > ?` **Hinweis:** Das erste Zeichen ist ein Apostroph. Passphrasen dürfen keine einfachen Anführungszeichen (‘), doppelten Anführungszeichen (") oder Währungssymbole enthalten. Wenn eine Passphrase Leerzeichen enthält, müssen Sie sie in doppelte Anführungszeichen setzen. Beispiel: `„Das ist eine Beispiel-Passphrase“`. Wenn eine Passphrase Sonderzeichen enthält, müssen Sie sie in dreifache doppelte Anführungszeichen (""") setzen. Beispiel: `"""Diese Passphrase enthält Sonderzeichen. % & *."""`. Wenn eine Passphrase nur alphanumerische Zeichen ohne Leerzeichen enthält, können Sie sie ohne Delimiter eingeben. **Hinweis:** Auf z/OS kann eine gültige RACF-Passphrase bis zu 100 Zeichen umfassen. PowerExchange schneidet Passphrases mit mehr als 100 Zeichen ab, wenn diese zur Validierung an RACF übergeben werden. Stellen Sie vor der Verwendung von Passphrasen sicher, dass der PowerExchange-Listenerdienst im DBMOVER-Mitglied mit der Sicherheitseinstellung SECURITY=(1,N) oder höher ausgeführt wird. Weitere Informationen finden Sie unter „SECURITY-Anweisung“ im *PowerExchange-Referenzhandbuch*.

Option	Argument	Beschreibung
-pwxEncryptedPassword -epwd	pwx_encrypted_password	Optional. Verschlüsseltes Passwort für eine Verbindung zum PowerExchange Listener, wenn pwxLocation angegeben ist. Wenn der PowerExchange Listener auf einem z/OS- oder i5/OS-System ausgeführt wird, können Sie eine verschlüsselte PowerExchange-Passphrase anstelle eines verschlüsselten Passworts eingeben. Verschlüsseln Sie keine Passphrase, die ungültige Zeichen wie z. B. doppelte Anführungszeichen, einzelne Anführungszeichen oder Währungssymbole enthält.
-datamapOutputDir -dod	datamap_output_directory	Optional. Das lokale Dateiverzeichnis, in das die Ausgabe-Datenzuordnungen geschrieben werden sollen. Standardwert ist das aktuelle Arbeitsverzeichnis.
-replace -r	replace_existing_datamaps	Optional. Gibt an, ob vorhandene Datenzuordnungen ersetzt werden sollen. Im Fall von replace=Y werden alle Datenzuordnungen in datamap_output_directory ersetzt, die denselben Namen als Datenzuordnungen haben, die Sie erstellen. Im Fall von replace=N wird die Erstellung einer Datenzuordnung bersprungen, falls eine Datenzuordnung mit demselben Namen bereits in datamap_output_directory existiert. Standardwert ist „N“.
-controlFile -cf	file_path_for_control_file	Erforderlich. Pfad und Dateiname der Steuerdatei, die die Datenzuordnungs-Erzeugung steuert.
-logFile -lf	file_path_for_log_file	Optional. Pfad und Dateiname der Ausgabeprotokolldatei. Standardwert ist „STDOUT“.
-verbosity -v	logging_verbosity	Optional. Ausführlichkeit für Protokolldateien. Standardwert ist „INFO“. Gültige Werte: - DEBUG. Detailliertere Protokollierung. Zeigt möglicherweise Stapelüberwachungen an. - INFO. Informationsmeldungen. - WARN. Gibt ein potenzielles Problem an. - ERROR. Gibt einen Fehler an. Die Verarbeitung wird fortgesetzt. - FATAL. Gibt eine schwerwiegende Fehlerbedingung an. Der Prozess wird beendet.

Der PowerExchange-Knotenname und die Anmeldedaten sind optional. Wenn Sie die Option „pwxLocation“ nicht einbeziehen, greift der Befehl direkt auf das lokale Dateisystem zu, um Metadaten zu lesen. In diesem Fall muss PowerExchange nicht auf dem Computer installiert sein, auf dem Sie createdatamaps ausführen.

Weitere Informationen zum Befehl „createdatamaps“ finden Sie im *PowerExchange Utilities-Handbuch*.

CreateListenerService

Erstellt einen PowerExchange-Listenerdienst in einer Domäne. Standardmäßig wird der Listenerdienst bei seiner Erstellung deaktiviert. Führen Sie den Befehl „infacmd isp EnableService“ aus, um den Dienst zu aktivieren.

Der Befehl „infacmd pwx CreateListenerService“ verwendet die folgende Syntax:

```
CreateListenerService

[<-DomainName|-dn> domain_name]

[<-UserName|-un> user_name]

[<-Password|-pd> password]

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-NodeName|-nn> node_name

[<-LicenseName|-ln> license_name]

[<-BackupNode|-bn> backup_node]

<-StartParameters|-sp> start_parameters

<-SvcPort|-sp> service_port
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx CreateListenerService“ beschrieben:

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

Option	Argument	Beschreibung
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn -DomainName nicht angegeben wurde. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Listenerdiensts. Bei diesem Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden. Der Name darf nicht länger als 128 Zeichen sein und keine Wagenrückläufe, Tabulatoren, Leerzeichen oder die folgenden Zeichen enthalten: `/ * ? < > " |`
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Listenerdienst ausgeführt werden soll.
-LicenseName -ln	license_name	Optional. Lizenz zur Zuweisung zum Dienst. Wenn Sie jetzt keine Lizenz auswählen, können Sie dem Dienst später eine Lizenz zuweisen. Dies ist erforderlich, bevor Sie den Dienst aktivieren können.
-BackupNode -bn	backup_node	Optional. Wenn die PowerCenter-Umgebung für hohe Verfügbarkeit konfiguriert ist, wird mit dieser Option der Name des Backup-Knotens angegeben.

Option	Argument	Beschreibung
-StartParameters -sp	start_parameters	Parameter, die beim Starten des Listenerdiensts einbezogen werden müssen. Trennen Sie die Parameter durch Leerzeichen. Der Parameter *node_name* ist erforderlich. Sie können die folgenden Parameter einbeziehen: - *node_name* Erforderlich. Knotenname, der den Listenerdienst identifiziert. Dieser Name muss mit dem Namen in der LISTENER-Anweisung in der Konfigurationsdatei DBMOVER übereinstimmen. - config=*directory* Optional. Gibt den vollständigen Pfad und Dateinamen für die Konfigurationsdatei „dbmover.cfg“ an, die Sie anstelle der Standarddatei „dbmover.cfg“ verwenden möchten. Diese alternative Konfigurationsdatei hat Vorrang vor jeder anderen alternativen Konfigurationsdatei, die Sie in der Umgebungsvariable PWX_CONFIG angeben. - license=*directory/license_key_file* Optional. Gibt den vollständigen Pfad und Dateinamen für eine Lizenzschlüsseldatei an, die Sie anstelle der Standarddatei license.key verwenden möchten. Diese alternative Lizenzschlüsseldatei und die Standarddatei dürfen nicht denselben Namen und denselben Pfad haben. Entweder Name oder Pfad muss unterschiedlich sein. Diese alternative Lizenzschlüsseldatei hat Vorrang vor jeder anderen alternativen Lizenzschlüsseldatei, die Sie in der Umgebungsvariable PWX_LICENSE angeben. **Hinweis:** In den Konfigurations- und Lizenzparametern müssen Sie den vollständigen Pfad nur dann angeben, wenn die Datei sich *nicht* im Installationsverzeichnis befindet. Schließen Sie Pfad- und Dateinamen, die Leerzeichen enthalten, in Anführungszeichen ein.
-SvcPort -sp	service_port	Erforderlich. Port des Listenerdiensts für die Reaktion auf Befehle vom Dienstmanager.

CreateLoggerService

Erstellt einen PowerExchange-Protokollierungsdienst in einer Domäne. Standardmäßig wird der Protokollierungsdienst bei seiner Erstellung deaktiviert. Führen Sie den Befehl „infacmd isp EnableService“ aus, um den Dienst zu aktivieren.

Der Befehl „infacmd pwx CreateLoggerService“ verwendet die folgende Syntax:

```
CreateLoggerService

[<-DomainName|-dn> domain_name]

[<-UserName|-un> user_name]

[<-Password|-pd> password]

[<-SecurityDomain|-sdn> security_domain]
```

```
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-NodeName|-nn> node_name

[<-LicenseName|-ln> license_name]

[<-BackupNode|-bn> backup_node]

[<-StartParameters|-sp> start_parameters>]

<-SvcPort|-sp> service_port
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx CreateLoggerService“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Optional. Wenn -DomainName nicht angegeben wurde. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Protokollierungsdiensts. Bei diesem Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden. Der Name darf nicht länger als 128 Zeichen sein und keine Wagenrückläufe, Tabulatoren, Leerzeichen oder die folgenden Zeichen enthalten: `/ * ? < > " |`
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Protokollierungsdienst ausgeführt werden soll.
-LicenseName -ln	license_name	Optional. Lizenz zur Zuweisung zum Dienst. Wenn Sie jetzt keine Lizenz auswählen, können Sie dem Dienst später eine Lizenz zuweisen. Dies ist erforderlich, bevor Sie den Dienst aktivieren können.
-BackupNode -bn	backup_node	Optional. Wenn die PowerCenter-Umgebung für hohe Verfügbarkeit konfiguriert ist, wird mit dieser Option der Name des Backup-Knotens angegeben.

Option	Argument	Beschreibung
-StartParameters -sp	start_parameters	Optional. Parameter, die beim Starten des Protokollierungsdiensts einbezogen werden müssen. Trennen Sie die Parameter durch Leerzeichen. Sie können die folgenden Parameter einbeziehen: - coldstart={Y|N} Gibt an, ob der Protokollierungsdienst kalt oder warm gestartet wird. Geben Sie Y für einen Kaltstart des Protokollierungsdiensts ein. Wenn die CDCT-Datei Protokolldatensätze enthält, löscht der Protokollierungsdienst diese Datensätze. Geben Sie N ein, um den Protokollierungsdienst ab dem Neustartpunkt warm zu starten, der in der CDCT-Datei angegeben ist. Standardwert ist „N“. - config=*directory/pwx_config_file* Gibt den vollständigen Pfad und Dateinamen für die Konfigurationsdatei „dbmover.cfg“ an, die Sie anstelle der Standarddatei „dbmover.cfg“ verwenden möchten. Diese alternative Konfigurationsdatei hat Vorrang vor jeder anderen alternativen Konfigurationsdatei, die Sie in der Umgebungsvariable PWX_CONFIG angeben. - cs=*directory/pwxlogger_config_file* Gibt den Pfad und Dateinamen für die Konfigurationsdatei des Protokollierungsdiensts an. Sie können auch den cs-Parameter verwenden, um eine Protokollierungsdienst-Konfigurationsdatei anzugeben, die die Standarddatei pwxccl.cfg überschreibt. Diese Überschreibungsdatei und die Standarddatei dürfen nicht denselben Namen und denselben Pfad haben. Entweder Name oder Pfad muss unterschiedlich sein. - encryptepwd=*encrypted_password* Ein Passwort im verschlüsselten Format zum Aktivieren der Verschlüsselung von Protokolldateien der PowerExchange-Protokollierung. Mit diesem Passwort kann die PowerExchange-Protokollierung einen eindeutigen Verschlüsselungsschlüssel für jede Protokolldatei der Protokollierung erzeugen. Das Passwort wird in der CDCT-Datei im verschlüsselten Format gespeichert. Aus Sicherheitsgründen wird das Passwort weder in CDCT-Sicherungsdateien gespeichert noch in den CDCT-Berichten angezeigt, die mit dem PowerExchange-Dienstprogramm PWXUCDCT erzeugt werden können. Bei Angabe dieses Parameters müssen Sie auch coldstart=y angeben. Wenn Sie diesen Parameter und den Parameter ENCRYPTEPWD in der Konfigurationsdatei (pwxccl.cfg) der PowerExchange-Protokollierung angeben, hat der Parameter in der Konfigurationsdatei Vorrang. Wenn Sie diesen Parameter und den Parameter ENCRYPTPWD in der Konfigurationsdatei der PowerExchange-Protokollierung angeben, tritt ein Fehler auf. Sie können den AES-Algorithmus festlegen, um ihn zum Verschlüsseln der Protokolldatei im Parameter ENCRYPTOPT der Datei „pwxccl.cfg“ zu verwenden. Standardwert ist AES128.

Option	Argument	Beschreibung
		Tipp: Zur Sicherheitsoptimierung empfiehlt Informatica, das Verschlüsselungspasswort beim Kaltstart der PowerExchange-Protokollierung und nicht in der Konfigurationsdatei „pwxccl.cfg“ anzugeben. Mit dieser Vorgehensweise verringern Sie aus folgenden Gründen das Risiko eines böswilligen Zugriffs auf das Verschlüsselungspasswort: 1) Das Verschlüsselungspasswort ist nicht in der Datei „pwxccl.cfg“ gespeichert. 2) Sie können das Passwort nach einem erfolgreichen Kaltstart aus der Befehlszeile löschen. Wenn Sie das Verschlüsselungspasswort für einen Kaltstart angeben und die CDCT-Datei dann zu einem späteren Zeitpunkt wiederherstellen müssen, müssen Sie dasselbe Verschlüsselungspasswort im Befehl RESTORE_CDCT des Dienstprogramms PWXUCDCT eingeben. Um die Protokolldateien der PowerExchange-Protokollierung *nicht* zu verschlüsseln, geben Sie kein Verschlüsselungspasswort ein. - license=*directory/license_key_file* Gibt den vollständigen Pfad und Dateinamen für eine Lizenzschlüsseldatei an, die Sie anstelle der Standarddatei license.key verwenden möchten. Diese alternative Lizenzschlüsseldatei und die Standarddatei dürfen nicht denselben Namen und denselben Pfad haben. Entweder Name oder Pfad muss unterschiedlich sein. Diese alternative Lizenzschlüsseldatei hat Vorrang vor jeder anderen alternativen Lizenzschlüsseldatei, die Sie in der Umgebungsvariable PWX_LICENSE angeben. - specialstart={Y|N} Gibt an, ob ein Sonderstart der PowerExchange-Protokollierung durchgeführt werden soll. Ein Sonderstart startet die Verarbeitung der PowerExchange-Erfassung an dem Punkt im Änderungsstrom, den Sie in der Datei „pwxccl.cfg“ angeben. Dieser Startpunkt überschreibt den Neustartpunkt aus der CDCT-Datei für die PowerExchange-Protokollierungsausführung. Bei einem Sonderstart wird kein Inhalt aus der CDCT-Datei gelöscht. Verwenden Sie diesen Parameter zum Überspringen problematischer Stellen in den Quellprotokollen, ohne dabei erfasste Daten zu verlieren. Verwenden Sie einen Sonderstart beispielsweise in folgenden Situationen: - Sie möchten nicht, dass die PowerExchange-Protokollierung eine Aktualisierung eines Oracle-Katalogs erfasst. Stoppen Sie in diesem Fall die PowerExchange-Protokollierung vor der Aktualisierung. Erzeugen Sie nach Abschluss der Aktualisierung eine neue Sequenz und starten Sie Token für die PowerExchange-Protokollierung basierend auf dem Post-Upgrade-SCN neu. Geben Sie diese Token-Werte in den Parametern SEQUENCE_TOKEN und RESTART_TOKEN in der Datei „pwxccl.cfg“ ein und führen Sie dann einen Sonderstart der PowerExchange-Protokollierung durch. - Sie möchten nicht, dass von der PowerExchange-Protokollierung alte, nicht verfügbare Protokolle erneut verarbeitet werden, die durch ausstehende Arbeitseinheiten verursacht wurden, die nicht zu CDC gehören. Stoppen Sie in diesem Fall die PowerExchange-

Option	Argument	Beschreibung
		Protokollierung. Bearbeiten Sie den Wert RESTART_TOKEN, um den SCN des frühesten verfügbaren Protokolls widerzuspiegeln, und führen Sie dann einen Sonderstart durch. Wenn alle ausstehenden Arbeitseinheiten, die vor diesem Neustartpunkt gestartet wurden, zu CDC gehören, gehen unter Umständen Daten verloren. Gültige Werte: - Y. Führen Sie einen Sonderstart der PowerExchange-Protokollierung ab dem Punkt im Änderungsstrom durch, der von den Parameterwerten SEQUENCE_TOKEN und RESTART_TOKEN in der Konfigurationsdatei „pwxccl.cfg“ definiert wird. Sie müssen gültige Token-Werte in der Datei „pwxccl.cfg“ angegeben, um einen Sonderstart durchzuführen. Diese Token-Werte überschreiben die Token-Werte aus der CDCT-Datei. Stellen Sie sicher, dass der Wert SEQUENCE_TOKEN in der Datei „pwxccl.cfg“ größer oder gleich dem aktuellen Sequenz-Token in der CDCT-Datei ist. Geben Sie den Parameter coldstart=Y nicht noch zusätzlich an. Wenn Sie den Parameter coldstart=Y angeben, hat dieser Parameter Vorrang. - N. Führen Sie keinen Sonderstart durch. Führen Sie einen Kalt- oder Warmstart, wie vom coldstart-Parameter angegeben, durch. Standardwert ist „N“. **Hinweis:** Der vollständige Pfad muss in den Konfigurations-, cs- und Lizenzparametern nur angegeben werden, wenn sich die Datei *nicht* im Installationsverzeichnis befindet. Schließen Sie Pfad- und Dateinamen, die Leerzeichen enthalten, in Anführungszeichen ein.
-SvcPort -sp	service_port	Optional. Port des Protokollierungsdiensts für die Reaktion auf Befehle vom Dienstmanager.

DisplayAllLogger

Zeigt sortiert nach Befehl alle Nachrichten an, die von den Anzeigebefehlen des anderen PowerExchange-Protokollierungsdiensts erzeugt werden können.

Der Befehl „infacmd pwx DisplayAllLogger“ zeigt die konsolidierte Ausgabe für die folgenden Befehle an:

- DisplayCPULogger
- DisplayEventsLogger
- DisplayMemoryLogger
- DisplayRecordsLogger
- DisplayStatusLogger

Der Befehl „infacmd pwx DisplayAllLogger“ verwendet die folgende Syntax:

```
DisplayAllLogger
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-OSUser|-oun> OS_user_name]
[<-OSPassword|-oup> OS_password]
[<-OSEPassword|-ouep> OS_epassword]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx DisplayAllLogger“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-OSUser -oun	OS_user_name	Erforderlich, wenn Sie Betriebssystemsicherheit aktiviert haben. Benutzername für das Betriebssystem. Aktivieren Sie Betriebssystemsicherheit wie folgt: - Damit Benutzer eine gültige Benutzer-ID und ein gültiges Passwort für das Betriebssystem im Befehl eingeben, legen Sie 1 oder 2 für den ersten Parameter der SECURITY-Anweisung in der DBMOVER-Konfigurationsdatei auf jedem Linux-, UNIX- oder Windows-System fest, das als Target des Befehls fungiert. PowerExchange verwendet Betriebssystemfunktionen auf dem Target-System, um die Benutzer-ID und das Passwort für die Verwendung des infacmd pwx-Programms zu authentifizieren. - Um Benutzer für die Ausführung bestimmter infacmd pwx-Befehle zu authentifizieren, legen Sie 2 für den ersten Parameter der SECURITY-Anweisung fest und definieren Sie die AUTHGROUP- und USER-Anweisungen in der PowerExchange-Anmeldedatei auf jedem Linux-, UNIX- oder Windows-System, das als Target des Befehls fungiert. PowerExchange überprüft die Anmeldedatei, um zu bestimmen, ob der im infacmd pwx-Programm bereitgestellten Benutzer-ID die Ausführung von Befehlen gewährt werden soll.

Option	Argument	Beschreibung
-OSPassword -oup	OS_password	Erforderlich, wenn Sie einen Benutzernamen ohne verschlüsseltes Passwort festlegen. Passwort für das Betriebssystem. Sie können ein Klartextpasswort mit der Option -p oder der Umgebungsvariable INFA_DEFAULT_PWX_OSPASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -p festgelegte Passwort Vorrang.
-OSEPassword -ouep	OS_epassword	Erforderlich, wenn Sie einen Benutzernamen ohne Klartextpasswort festlegen. Verschlüsseltes Passwort für das Betriebssystem. Sie können ein verschlüsseltes Passwort mit der Option -e oder der Umgebungsvariable INFA_DEFAULT_PWX_OSEPASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -e festgelegte Passwort Vorrang.

DisplayCPULogger

Zeigt die CPU-Zeit in Mikrosekunden an, die vom PowerExchange-Protokollierungsdienst für jede Phase der Verarbeitung während des aktuellen Logging-Zyklus benötigt wird. Enthält außerdem die CPU-Gesamtzeit für die gesamte Protokollierungsdienst-Verarbeitung.

Mit dem Befehl „infacmd pwx DisplayCPULogger“ kann beispielsweise die CPU-Zeit angegeben werden, die vom Protokollierungsdienst zum Abschließen der folgenden Aktionen benötigt wird:

- Lesen von Quelldaten
- Schreiben von Daten in die Protokolldateien des Protokollierungsdiensts
- Durchführen von Dateiwechseln
- Durchführen weiterer Verarbeitungsaufgaben, wie z. B. das Initialisieren und Verarbeiten von Befehlen

Der Befehl „infacmd pwx DisplayCPULogger“ verwendet die folgende Syntax:

```
DisplayCPULogger

[<-DomainName|-dn> domain_name]

[<-UserName|-un> user_name]

[<-Password|-pd> password]

<-ServiceName|-sn> service_name

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-OSUser|-oun> OS_user_name]

[<-OSPassword|-oup> OS_password]

[<-OSEPassword|-ouep> OS_epassword]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx DisplayCPULogger“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-OSUser -oun	OS_user_name	Erforderlich, wenn Sie Betriebssystemsicherheit aktiviert haben. Benutzername für das Betriebssystem. Aktivieren Sie Betriebssystemsicherheit wie folgt: - Damit Benutzer eine gültige Benutzer-ID und ein gültiges Passwort für das Betriebssystem im Befehl eingeben, legen Sie 1 oder 2 für den ersten Parameter der SECURITY-Anweisung in der DBMOVER-Konfigurationsdatei auf jedem Linux-, UNIX- oder Windows-System fest, das als Target des Befehls fungiert. PowerExchange verwendet Betriebssystemfunktionen auf dem Target-System, um die Benutzer-ID und das Passwort für die Verwendung des infacmd pwx-Programms zu authentifizieren. - Um Benutzer für die Ausführung bestimmter infacmd pwx-Befehle zu authentifizieren, legen Sie 2 für den ersten Parameter der SECURITY-Anweisung fest und definieren Sie die AUTHGROUP- und USER-Anweisungen in der PowerExchange-Anmeldedatei auf jedem Linux-, UNIX- oder Windows-System, das als Target des Befehls fungiert. PowerExchange überprüft die Anmeldedatei, um zu bestimmen, ob der im infacmd pwx-Programm bereitgestellten Benutzer-ID die Ausführung von Befehlen gewährt werden soll.

Option	Argument	Beschreibung
-OSPassword -oup	OS_password	Erforderlich, wenn Sie einen Benutzernamen ohne verschlüsseltes Passwort festlegen. Passwort für das Betriebssystem. Sie können ein Klartextpasswort mit der Option -p oder der Umgebungsvariable INFA_DEFAULT_PWX_OSPASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -p festgelegte Passwort Vorrang.
-OSEPassword -ouep	OS_epassword	Erforderlich, wenn Sie einen Benutzernamen ohne Klartextpasswort festlegen. Verschlüsseltes Passwort für das Betriebssystem. Sie können ein verschlüsseltes Passwort mit der Option -e oder der Umgebungsvariable INFA_DEFAULT_PWX_OSEPASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -e festgelegte Passwort Vorrang.

DisplayEventsLogger

Zeigt Ereignisse an, auf die die Controller-, Command Handler- und Writer-Aufgaben für den PowerExchange-Protokollierungsdienst warten. Gibt außerdem an, ob der Writer Daten verarbeitet oder im Ruhemodus ausgeführt wird und auf das Auftreten eines Ereignisses oder Timeouts wartet.

Der Befehl „infacmd pwx DisplayEventsLogger“ verwendet die folgende Syntax:

```
DisplayEventsLogger

[<-DomainName|-dn> domain_name]

[<-UserName|-un> user_name]

[<-Password|-pd> password]

<-ServiceName|-sn> service_name

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-OSUser|-oun> OS_user_name]

[<-OSPassword|-oup> OS_password]

[<-OSEPassword|-ouep> OS_epassword]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx DisplayEventsLogger“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-OSUser -oun	OS_user_name	Erforderlich, wenn Sie Betriebssystemsicherheit aktiviert haben. Benutzername für das Betriebssystem. Aktivieren Sie Betriebssystemsicherheit wie folgt: - Damit Benutzer eine gültige Benutzer-ID und ein gültiges Passwort für das Betriebssystem im Befehl eingeben, legen Sie 1 oder 2 für den ersten Parameter der SECURITY-Anweisung in der DBMOVER-Konfigurationsdatei auf jedem Linux-, UNIX- oder Windows-System fest, das als Target des Befehls fungiert. PowerExchange verwendet Betriebssystemfunktionen auf dem Target-System, um die Benutzer-ID und das Passwort für die Verwendung des infacmd pwx-Programms zu authentifizieren. - Um Benutzer für die Ausführung bestimmter infacmd pwx-Befehle zu authentifizieren, legen Sie 2 für den ersten Parameter der SECURITY-Anweisung fest und definieren Sie die AUTHGROUP- und USER-Anweisungen in der PowerExchange-Anmeldedatei auf jedem Linux-, UNIX- oder Windows-System, das als Target des Befehls fungiert. PowerExchange überprüft die Anmeldedatei, um zu bestimmen, ob der im infacmd pwx-Programm bereitgestellten Benutzer-ID die Ausführung von Befehlen gewährt werden soll.

Option	Argument	Beschreibung
-OSPassword -oup	OS_password	Erforderlich, wenn Sie einen Benutzernamen ohne verschlüsseltes Passwort festlegen. Passwort für das Betriebssystem. Sie können ein Klartextpasswort mit der Option -p oder der Umgebungsvariable INFA_DEFAULT_PWX_OSPASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -p festgelegte Passwort Vorrang.
-OSEPassword -ouep	OS_epassword	Erforderlich, wenn Sie einen Benutzernamen ohne Klartextpasswort festlegen. Verschlüsseltes Passwort für das Betriebssystem. Sie können ein verschlüsseltes Passwort mit der Option -e oder der Umgebungsvariable INFA_DEFAULT_PWX_OSEPASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -e festgelegte Passwort Vorrang.

DisplayMemoryLogger

Zeigt die Speichernutzung (in Byte) für jede Aufgabe und Unteraufgabe im PowerExchange-Protokollierungsdienst mit Gesamtsummen für den gesamten Protokollierungsdienst-Prozess an.

PowerExchange gibt die Speichernutzung für folgende Kategorien an:

- Application Speicher, der von der Protokollierungsdienst-Anwendung zur eigenen Nutzung benötigt wird.
- Gesamt. Gesamter für die Protokollierungsdienst-Anwendung und den zugehörigen Header-Overhead verwendeter Speicher. Dieser Wert variiert, da PowerExchange während der Protokollierungsdienst-Verarbeitung Speicher zuweist und freigibt.
- Maximal. Die größte für die Kategorie „Gesamt“ aufgezeichnete Speichermenge bis zu dem Zeitpunkt, an dem dieser Befehl ausgeführt wird.

Der Befehl „infacmd pwx DisplayMemoryLogger“ verwendet die folgende Syntax:

```
DisplayMemoryLogger

[<-DomainName|-dn> domain_name]

[<-UserName|-un> user_name]

[<-Password|-pd> password]

<-ServiceName|-sn> service_name

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-OSUser|-oun> OS_user_name]

[<-OSPassword|-oup> OS_password]

[<-OSEPassword|-ouep> OS_epassword]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx DisplayMemoryLogger“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-OSUser -oun	OS_user_name	Erforderlich, wenn Sie Betriebssystemsicherheit aktiviert haben. Benutzername für das Betriebssystem. Aktivieren Sie Betriebssystemsicherheit wie folgt: - Damit Benutzer eine gültige Benutzer-ID und ein gültiges Passwort für das Betriebssystem im Befehl eingeben, legen Sie 1 oder 2 für den ersten Parameter der SECURITY-Anweisung in der DBMOVER-Konfigurationsdatei auf jedem Linux-, UNIX- oder Windows-System fest, das als Target des Befehls fungiert. PowerExchange verwendet Betriebssystemfunktionen auf dem Target-System, um die Benutzer-ID und das Passwort für die Verwendung des infacmd pwx-Programms zu authentifizieren. - Um Benutzer für die Ausführung bestimmter infacmd pwx-Befehle zu authentifizieren, legen Sie 2 für den ersten Parameter der SECURITY-Anweisung fest und definieren Sie die AUTHGROUP- und USER-Anweisungen in der PowerExchange-Anmeldedatei auf jedem Linux-, UNIX- oder Windows-System, das als Target des Befehls fungiert. PowerExchange überprüft die Anmeldedatei, um zu bestimmen, ob der im infacmd pwx-Programm bereitgestellten Benutzer-ID die Ausführung von Befehlen gewährt werden soll.

Option	Argument	Beschreibung
-OSPassword -oup	OS_password	Erforderlich, wenn Sie einen Benutzernamen ohne verschlüsseltes Passwort festlegen. Passwort für das Betriebssystem. Sie können ein Klartextpasswort mit der Option -p oder der Umgebungsvariable INFA_DEFAULT_PWX_OSPASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -p festgelegte Passwort Vorrang.
-OSEPassword -ouep	OS_epassword	Erforderlich, wenn Sie einen Benutzernamen ohne Klartextpasswort festlegen. Verschlüsseltes Passwort für das Betriebssystem. Sie können ein verschlüsseltes Passwort mit der Option -e oder der Umgebungsvariable INFA_DEFAULT_PWX_OSEPASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -e festgelegte Passwort Vorrang.

DisplayRecordsLogger

Zeigt die Anzahl der Änderungsdatensätze an, die vom PowerExchange-Protokollierungsdienst während des aktuellen Verarbeitungszyklus verarbeitet wurden. Wenn der Protokollierungsdienst während des aktuellen Zyklus keine Änderungen erhalten hat, wird die Anzahl der Änderungsdatensätze für den aktuellen Satz an Protokolldateien des Protokollierungsdiensts angezeigt.

Der Befehl „infacmd pwx DisplayRecordsLogger“ zeigt die Anzahl an Datensätzen für jeden verarbeiteten Typ der Änderungsdatensätze sowie für die Gesamtzahl der verarbeiteten Datensätze an. Zu den Änderungsdatensatztypen gehören: Delete, Insert, Update und Commit.

Je nachdem, ob der Befehl Zähler für den aktuellen Zyklus oder die aktuellen Logdateien anzeigt, enthält die Ausgabe alle oder bestimmte der folgenden Informationstypen:

- Zyklus. Anzahl der Änderungsdatensätze für den aktuellen Protokollierungsdienst-Verarbeitungszyklus. Der Protokollierungsdienst setzt diese Anzahl auf „null“ zurück, wenn der im Parameter NO_DATA_WAIT2 der Datei „pwxccl.cfg“ angegebene Wartezeitraum abläuft oder wenn keine Änderungsdaten empfangen wurden.
- Datei. Anzahl der Änderungsdatensätze für den aktuellen Satz an PowerExchange-Logdateien. Der Protokollierungsdienst setzt diese Anzahl auf „null“ zurück, wenn ein Dateiwechsel stattfindet.
- Gesamt. Anzahl der Änderungsdatensätze, die der Protokollierungsdienst seit seinem Start erhalten hat. PowerExchange setzt diese Anzahl nicht auf Null zurück.

Der Befehl „infacmd pwx DisplayRecordsLogger“ verwendet die folgende Syntax:

```
DisplayRecordsLogger

[<-DomainName|-dn> domain_name]

[<-UserName|-un> user_name]

[<-Password|-pd> password]

<-ServiceName|-sn> service_name
```

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

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-OSUser|-oun> OS_user_name]

[<-OSPassword|-oup> OS_password]

[<-OSEPassword|-ouep> OS_epassword]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx DisplayRecordsLogger“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-OSUser -oun	OS_user_name	Erforderlich, wenn Sie Betriebssystemsicherheit aktiviert haben. Benutzername für das Betriebssystem. Aktivieren Sie Betriebssystemsicherheit wie folgt: - Damit Benutzer eine gültige Benutzer-ID und ein gültiges Passwort für das Betriebssystem im Befehl eingeben, legen Sie 1 oder 2 für den ersten Parameter der SECURITY-Anweisung in der DBMOVER-Konfigurationsdatei auf jedem Linux-, UNIX- oder Windows-System fest, das als Target des Befehls fungiert. PowerExchange verwendet Betriebssystemfunktionen auf dem Target-System, um die Benutzer-ID und das Passwort für die Verwendung des infacmd pwx-Programms zu authentifizieren. - Um Benutzer für die Ausführung bestimmter infacmd pwx-Befehle zu authentifizieren, legen Sie 2 für den ersten Parameter der SECURITY-Anweisung fest und definieren Sie die AUTHGROUP- und USER-Anweisungen in der PowerExchange-Anmeldedatei auf jedem Linux-, UNIX- oder Windows-System, das als Target des Befehls fungiert. PowerExchange überprüft die Anmeldedatei, um zu bestimmen, ob der im infacmd pwx-Programm bereitgestellten Benutzer-ID die Ausführung von Befehlen gewährt werden soll.

Option	Argument	Beschreibung
-OSPassword -oup	OS_password	Erforderlich, wenn Sie einen Benutzernamen ohne verschlüsseltes Passwort festlegen. Passwort für das Betriebssystem. Sie können ein Klartextpasswort mit der Option -p oder der Umgebungsvariable INFA_DEFAULT_PWX_OSPASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -p festgelegte Passwort Vorrang.
-OSEPassword -ouep	OS_epassword	Erforderlich, wenn Sie einen Benutzernamen ohne Klartextpasswort festlegen. Verschlüsseltes Passwort für das Betriebssystem. Sie können ein verschlüsseltes Passwort mit der Option -e oder der Umgebungsvariable INFA_DEFAULT_PWX_OSEPASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -e festgelegte Passwort Vorrang.

displayStatsListener

Zeigt die Überwachungsstatistik für einen PowerExchange-Listener unter Linux, UNIX oder Windows an, den der PowerExchange-Listenerdienst verwaltet. Zeigt außerdem Statistiken für die Client-Aufgaben und Quell- oder Zielverbindungen, die dem Listener zugeordnet sind.

Der Befehl kann die folgenden Arten von Statistiken drucken, je nachdem, welche Option Sie für „-type“ angeben:

- Zusammenfassung der PowerExchange-Listener-Statistiken über Arbeitsspeichernutzung, CPU-Verarbeitungszeit und Aktivität für Clientanfragen. Diese Statistiken enthalten die Anzahl von Client-Aufgaben, Verbindungen, gesendeten und empfangenen Nachrichten sowie gesendeten und empfangenen Datenbytes.
- Nachrichten- und Datenmengen, die Client-Aufgaben für Client-Anfragen gesendet und empfangen haben, nach Aufgaben-ID und Zugriffsmethode. Die Nachrichten- und Datenmengen sind Summen zu dem Zeitpunkt, zu dem die Statistiken generiert werden.
- Informationen über die aktiven Aufgaben, die unter dem Listener zur Verarbeitung von Client-Anfragen ausgeführt werden. Diese Statistiken enthalten die Aufgaben-Startzeit, die CPU-Verarbeitungszeit, die Zugriffsmethode, den Lese- oder Schreibmodus und zugeordnete Prozess- und Sitzungs-IDs. Enthält außerdem die Portnummer und die IP-Adresse des Clients, der die Anfrage an den PowerExchange-Listener ausgegeben hat.

Wichtig: Damit PowerExchange die Überwachungsstatistiken vom PowerExchange-Listener erfassen kann, müssen Sie den Parameter MONITOR in der Anweisung STATS in der DBMOVER-Konfigurationsdatei angeben, in der der Listener ausgeführt wird.

Der Befehl „infacmd pwx displayStatsListener“ verwendet die folgende Syntax:

```
displayStatsListener

[<-DomainName|-dn> domain_name]

[<-UserName|-un> user_name]
```

```
[<-Password|-pd> password]

<-ServiceName|-sn> service_name

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> domain_host1:port domain_host2:port...]

[<-OSUser|-oun> OS_user_name]

[<-OSPassword|-oup> OS_password]

[<-OSEPassword|-ouep> OS_epassword]

[<-Type|-tp> report_type]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx displayStatsListener“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-OSUser -oun	OS_user_name	Erforderlich, wenn Sie Betriebssystemsicherheit aktiviert haben. Benutzername für das Betriebssystem. Aktivieren Sie Betriebssystemsicherheit wie folgt: - Damit Benutzer eine gültige Benutzer-ID und ein gültiges Passwort für das Betriebssystem im Befehl eingeben, legen Sie 1 oder 2 für den ersten Parameter der SECURITY-Anweisung in der DBMOVER-Konfigurationsdatei auf jedem Linux-, UNIX- oder Windows-System fest, das als Target des Befehls fungiert. PowerExchange verwendet Betriebssystemfunktionen auf dem Target-System, um die Benutzer-ID und das Passwort für die Verwendung des infacmd pwx-Programms zu authentifizieren. - Um Benutzer für die Ausführung bestimmter infacmd pwx-Befehle zu authentifizieren, legen Sie 2 für den ersten Parameter der SECURITY-Anweisung fest und definieren Sie die AUTHGROUP- und USER-Anweisungen in der PowerExchange-Anmeldedatei auf jedem Linux-, UNIX- oder Windows-System, das als Target des Befehls fungiert. PowerExchange überprüft die Anmeldedatei, um zu bestimmen, ob der im infacmd pwx-Programm bereitgestellten Benutzer-ID die Ausführung von Befehlen gewährt werden soll.
-OSPassword -oup	OS_password	Erforderlich, wenn Sie einen Benutzernamen ohne verschlüsseltes Passwort festlegen. Passwort für das Betriebssystem. Sie können ein Klartextpasswort mit der Option -p oder der Umgebungsvariable INFA_DEFAULT_PWX_OSPASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -p festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-OSEPassword -ouep	OS_epassword	Erforderlich, wenn Sie einen Benutzernamen ohne Klartextpasswort festlegen. Verschlüsseltes Passwort für das Betriebssystem. Sie können ein verschlüsseltes Passwort mit der Option -e oder der Umgebungsvariable INFA_DEFAULT_PWX_OSEPASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -e festgelegte Passwort Vorrang.
-type -tp	report_type	Optional. Der Typ von Überwachungsstatistiken zum Berichten für den PowerExchange-Listener und dessen Client-Aufgaben und Verbindungen. Für report_type muss einer der folgenden Werte angegeben werden: - Listener. Berichtet für einen bestimmten PowerExchange-Listener über Speichernutzung, CPU-Verarbeitungszeit, die Gesamtanzahl der Client-Aufgaben, aktive Aufgaben, High-Watermark-Aufgaben, die maximal zulässigen Aufgaben, die Gesamtanzahl der Verbindungsversuche, die akzeptierten Verbindungen, die aktiven Verbindungen, die Anzahl der gesendeten und empfangenen Nachrichten sowie die Anzahl der gesendeten und empfangenen Datenbytes. - Zugriffsmethoden. Berichtet für jede Zugriffsmethode für jede aktive Aufgabe über die Anzahl der gelesenen und geschriebenen Zeilen, die Anzahl der gelesenen und geschriebenen Datenbytes, den Quell- oder Zieldateinamen oder den Daten-Mapping-Dateinamen je nach der Zugriffsmethode sowie über die CPU-Verarbeitungszeit. - Clients. Berichtet für jede aktive Aufgabe über die Aufgaben-ID, den Status, die Zugriffsmethode, den Lese- oder Schreibmodus, die Prozess- und Sitzungs-IDs (sofern verfügbar), die CPU-Verarbeitungszeit und Startdatum und -uhrzeit. Berichtet auch die Portnummer und IP-Adresse des Clients, der die Anfrage ausgegeben hat, für welche die Aufgabe erstellt wurde. Berichtet die PowerCenter-Sitzungs-ID und den Anwendungsnamen für CDC, wenn der Client PowerCenter ist. Der Standardwert lautet „Listener“. **Hinweis:** In diesen Berichten kann eine Zugriffsmethode ein Quelltyp sein, z. B. NRDB. Eine Client-Aufgabe kann möglicherweise mehreren Zugriffsmethoden zugeordnet sein: einer Methode für das Lesen der Quelldaten und einer Methode für das Zuordnen von nicht-relationalen Daten zu einem relationalen Format.

DisplayStatusLogger

Zeigt den Status der Writer-Unteraufgabe für einen PowerExchange-Protokollierungsdienst an.

Mit dem Befehl infacmd pwx DisplayStatusLogger kann beispielsweise angegeben werden, wann der Writer die folgenden Aktionen abschließt:

- Initialisieren

- Lesen von oder Warten auf Quelldaten
- Schreiben von Quelldaten in eine Protokolldatei des Protokollierungsdiensts
- Schreiben von CDCT-Datensätzen während eines Dateiwechsels
- Löschen abgelaufener CDCT-Datensätze
- Herunterfahren

Der Befehl „infacmd pwx DisplayStatusLogger“ verwendet die folgende Syntax:

```
DisplayStatusLogger
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-OSUser|-oun> OS_user_name]
[<-OSPassword|-oup> OS_password]
[<-OSEPassword|-ouep> OS_epassword]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx DisplayStatusLogger“ beschrieben:

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

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Protokollierungsdiensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-OSUser -oun	OS_user_name	Erforderlich, wenn Sie Betriebssystemsicherheit aktiviert haben. Benutzername für das Betriebssystem. Aktivieren Sie Betriebssystemsicherheit wie folgt: - Damit Benutzer eine gültige Benutzer-ID und ein gültiges Passwort für das Betriebssystem im Befehl eingeben, legen Sie 1 oder 2 für den ersten Parameter der SECURITY-Anweisung in der DBMOVER-Konfigurationsdatei auf jedem Linux-, UNIX- oder Windows-System fest, das als Target des Befehls fungiert. PowerExchange verwendet Betriebssystemfunktionen auf dem Target-System, um die Benutzer-ID und das Passwort für die Verwendung des infacmd pwx-Programms zu authentifizieren. - Um Benutzer für die Ausführung bestimmter infacmd pwx-Befehle zu authentifizieren, legen Sie 2 für den ersten Parameter der SECURITY-Anweisung fest und definieren Sie die AUTHGROUP- und USER-Anweisungen in der PowerExchange-Anmeldedatei auf jedem Linux-, UNIX- oder Windows-System, das als Target des Befehls fungiert. PowerExchange überprüft die Anmeldedatei, um zu bestimmen, ob der im infacmd pwx-Programm bereitgestellten Benutzer-ID die Ausführung von Befehlen gewährt werden soll.
-OSPassword -oup	OS_password	Erforderlich, wenn Sie einen Benutzernamen ohne verschlüsseltes Passwort festlegen. Passwort für das Betriebssystem. Sie können ein Klartextpasswort mit der Option -p oder der Umgebungsvariable INFA_DEFAULT_PWX_OSPASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -p festgelegte Passwort Vorrang.
-OSEPassword -ouep	OS_epassword	Erforderlich, wenn Sie einen Benutzernamen ohne Klartextpasswort festlegen. Verschlüsseltes Passwort für das Betriebssystem. Sie können ein verschlüsseltes Passwort mit der Option -e oder der Umgebungsvariable INFA_DEFAULT_PWX_OSEPASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -e festgelegte Passwort Vorrang.

FileSwitchLogger

Schließt geöffnete Protokolldateien für den PowerExchange-Protokollierungsdienst und wechselt dann zu einem neuen Satz an Protokolldateien. Wenn die geöffneten Logdateien keine Daten enthalten, findet kein Dateiwechsel statt.

Hinweis: Wenn Sie den fortlaufenden Extraktionsmodus verwenden, müssen Sie die Dateiwechsel in der Regel nicht manuell abschließen.

Der Befehl „infacmd pwx FileSwitchLogger“ verwendet die folgende Syntax:

```
FileSwitchLogger
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-OSUser|-oun> OS_user_name]
[<-OSPassword|-oup> OS_password]
[<-OSEPassword|-ouep> OS_epassword]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx FileSwitchLogger“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-OSUser -oun	OS_user_name	Erforderlich, wenn Sie Betriebssystemsicherheit aktiviert haben. Benutzername für das Betriebssystem. Aktivieren Sie Betriebssystemsicherheit wie folgt: - Damit Benutzer eine gültige Benutzer-ID und ein gültiges Passwort für das Betriebssystem im Befehl eingeben, legen Sie 1 oder 2 für den ersten Parameter der SECURITY-Anweisung in der DBMOVER-Konfigurationsdatei auf jedem Linux-, UNIX- oder Windows-System fest, das als Target des Befehls fungiert. PowerExchange verwendet Betriebssystemfunktionen auf dem Target-System, um die Benutzer-ID und das Passwort für die Verwendung des infacmd pwx-Programms zu authentifizieren. - Um Benutzer für die Ausführung bestimmter infacmd pwx-Befehle zu authentifizieren, legen Sie 2 für den ersten Parameter der SECURITY-Anweisung fest und definieren Sie die AUTHGROUP- und USER-Anweisungen in der PowerExchange-Anmeldedatei auf jedem Linux-, UNIX- oder Windows-System, das als Target des Befehls fungiert. PowerExchange überprüft die Anmeldedatei, um zu bestimmen, ob der im infacmd pwx-Programm bereitgestellten Benutzer-ID die Ausführung von Befehlen gewährt werden soll.

Option	Argument	Beschreibung
-OSPassword -oup	OS_password	Erforderlich, wenn Sie einen Benutzernamen ohne verschlüsseltes Passwort festlegen. Passwort für das Betriebssystem. Sie können ein Klartextpasswort mit der Option -p oder der Umgebungsvariable INFA_DEFAULT_PWX_OSPASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -p festgelegte Passwort Vorrang.
-OSEPassword -ouep	OS_epassword	Erforderlich, wenn Sie einen Benutzernamen ohne Klartextpasswort festlegen. Verschlüsseltes Passwort für das Betriebssystem. Sie können ein verschlüsseltes Passwort mit der Option -e oder der Umgebungsvariable INFA_DEFAULT_PWX_OSEPASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -e festgelegte Passwort Vorrang.

ListTaskListener

Zeigt Informationen zu jeder aktiven Aufgabe für den PowerExchange-Listenerdienst an, einschließlich TCP/IP-Adresse, Portnummer, Anwendungsname, Zugriffstyp und Status.

Der Befehl „infacmd pwx ListTaskListener“ verwendet die folgende Syntax:

```
ListTaskListener

[<-DomainName|-dn> domain_name]

[<-UserName|-un> user_name]

[<-Password|-pd> password]

<-ServiceName|-sn> service_name

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-OSUser|-oun> OS_user_name]

[<-OSPassword|-oup> OS_password]

[<-OSEPassword|-ouep> OS_epassword]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx ListTaskListener“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-OSUser -oun	OS_user_name	Erforderlich, wenn Sie Betriebssystemsicherheit aktiviert haben. Benutzername für das Betriebssystem. Aktivieren Sie Betriebssystemsicherheit wie folgt: - Damit Benutzer eine gültige Benutzer-ID und ein gültiges Passwort für das Betriebssystem im Befehl eingeben, legen Sie 1 oder 2 für den ersten Parameter der SECURITY-Anweisung in der DBMOVER-Konfigurationsdatei auf jedem Linux-, UNIX- oder Windows-System fest, das als Target des Befehls fungiert. PowerExchange verwendet Betriebssystemfunktionen auf dem Target-System, um die Benutzer-ID und das Passwort für die Verwendung des infacmd pwx-Programms zu authentifizieren. - Um Benutzer für die Ausführung bestimmter infacmd pwx-Befehle zu authentifizieren, legen Sie 2 für den ersten Parameter der SECURITY-Anweisung fest und definieren Sie die AUTHGROUP- und USER-Anweisungen in der PowerExchange-Anmeldedatei auf jedem Linux-, UNIX- oder Windows-System, das als Target des Befehls fungiert. PowerExchange überprüft die Anmeldedatei, um zu bestimmen, ob der im infacmd pwx-Programm bereitgestellten Benutzer-ID die Ausführung von Befehlen gewährt werden soll.

Option	Argument	Beschreibung
-OSPassword -oup	OS_password	Erforderlich, wenn Sie einen Benutzernamen ohne verschlüsseltes Passwort festlegen. Passwort für das Betriebssystem. Sie können ein Klartextpasswort mit der Option -p oder der Umgebungsvariable INFA_DEFAULT_PWX_OSPASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -p festgelegte Passwort Vorrang.
-OSEPassword -ouep	OS_epassword	Erforderlich, wenn Sie einen Benutzernamen ohne Klartextpasswort festlegen. Verschlüsseltes Passwort für das Betriebssystem. Sie können ein verschlüsseltes Passwort mit der Option -e oder der Umgebungsvariable INFA_DEFAULT_PWX_OSEPASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -e festgelegte Passwort Vorrang.

ShutDownLogger

Hält den PowerExchange-Protokollierungsdienst in kontrollierter Weise an. Der Befehl schließt die Protokolldateien des Protokollierungsdiensts und schreibt die aktuelle Neustartposition dann in die CDCT-Datei.

Verwenden Sie diesen Befehl zum Anhalten eines PowerExchange-Protokollierungsdiensts, der im fortlaufenden Modus ausgeführt wird.

Beim Herunterfahren schließt der Protokollierungsdienst die folgenden Aktionen ab:

- Schließen aller geöffneten Logdateien
- Schreibt aktualisierte Informationen in die CDCT-Datei, einschließlich Neustart- und Sequenztoken
- Schließen der CAPI
- Anhalten der Writer- und Command Handler-Unteraufgaben
- Beenden des pwxccl-Programms
- Aufzeichnen der CPU-Nutzung

Der Befehl „infacmd pwx ShutDownLogger“ verwendet die folgende Syntax:

```
ShutDownLogger

[<-DomainName|-dn> domain_name]

[<-UserName|-un> user_name]

[<-Password|-pd> password]

<-ServiceName|-sn> service_name

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
```

```
[<-OSUser|-oun> OS_user_name]

[<-OSPassword|-oup> OS_password]

[<-OSEPassword|-ouep> OS_epassword]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx ShutDownLogger“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-OSUser -oun	OS_user_name	Erforderlich, wenn Sie Betriebssystemsicherheit aktiviert haben. Benutzername für das Betriebssystem. Aktivieren Sie Betriebssystemsicherheit wie folgt: - Damit Benutzer eine gültige Benutzer-ID und ein gültiges Passwort für das Betriebssystem im Befehl eingeben, legen Sie 1 oder 2 für den ersten Parameter der SECURITY-Anweisung in der DBMOVER-Konfigurationsdatei auf jedem Linux-, UNIX- oder Windows-System fest, das als Target des Befehls fungiert. PowerExchange verwendet Betriebssystemfunktionen auf dem Target-System, um die Benutzer-ID und das Passwort für die Verwendung des infacmd pwx-Programms zu authentifizieren. - Um Benutzer für die Ausführung bestimmter infacmd pwx-Befehle zu authentifizieren, legen Sie 2 für den ersten Parameter der SECURITY-Anweisung fest und definieren Sie die AUTHGROUP- und USER-Anweisungen in der PowerExchange-Anmeldedatei auf jedem Linux-, UNIX- oder Windows-System, das als Target des Befehls fungiert. PowerExchange überprüft die Anmeldedatei, um zu bestimmen, ob der im infacmd pwx-Programm bereitgestellten Benutzer-ID die Ausführung von Befehlen gewährt werden soll.

Option	Argument	Beschreibung
-OSPassword -oup	OS_password	Erforderlich, wenn Sie einen Benutzernamen ohne verschlüsseltes Passwort festlegen. Passwort für das Betriebssystem. Sie können ein Klartextpasswort mit der Option -p oder der Umgebungsvariable INFA_DEFAULT_PWX_OSPASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -p festgelegte Passwort Vorrang.
-OSEPassword -ouep	OS_epassword	Erforderlich, wenn Sie einen Benutzernamen ohne Klartextpasswort festlegen. Verschlüsseltes Passwort für das Betriebssystem. Sie können ein verschlüsseltes Passwort mit der Option -e oder der Umgebungsvariable INFA_DEFAULT_PWX_OSEPASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -e festgelegte Passwort Vorrang.

StopTaskListener

Hält eine PowerExchange-Listenerdienst-Aufgabe basierend auf einem Anwendungsnamen oder einer Aufgaben-ID an, die vom Benutzer angegeben wurde. Bei der Extraktion geänderter Daten wartet der Befehl „infacmd pwx StopTaskListener“ mit dem Anhalten der Aufgabe, bis entweder das UOW-Ende oder der Commit-Schwellenwert erreicht ist.

Der Befehl „infacmd pwx StopTaskListener“ verwendet die folgende Syntax:

```
StopTaskListener

[<-DomainName|-dn> domain_name]

[<-UserName|-un> user_name]

[<-Password|-pd> password]

<-ServiceName|-sn> service_name

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-OSUser|-oun> OS_user_name]

[<-OSPassword|-oup> OS_password]

[<-OSEPassword|-ouep> OS_epassword]

[<-applicationid|-a> appname]

[<-taskid|-t> taskid]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx StopTaskListener“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-OSUser -oun	OS_user_name	Erforderlich, wenn Sie Betriebssystemsicherheit aktiviert haben. Benutzername für das Betriebssystem. Aktivieren Sie Betriebssystemsicherheit wie folgt: - Damit Benutzer eine gültige Benutzer-ID und ein gültiges Passwort für das Betriebssystem im Befehl eingeben, legen Sie 1 oder 2 für den ersten Parameter der SECURITY-Anweisung in der DBMOVER-Konfigurationsdatei auf jedem Linux-, UNIX- oder Windows-System fest, das als Target des Befehls fungiert. PowerExchange verwendet Betriebssystemfunktionen auf dem Target-System, um die Benutzer-ID und das Passwort für die Verwendung des infacmd pwx-Programms zu authentifizieren. - Um Benutzer für die Ausführung bestimmter infacmd pwx-Befehle zu authentifizieren, legen Sie 2 für den ersten Parameter der SECURITY-Anweisung fest und definieren Sie die AUTHGROUP- und USER-Anweisungen in der PowerExchange-Anmeldedatei auf jedem Linux-, UNIX- oder Windows-System, das als Target des Befehls fungiert. PowerExchange überprüft die Anmeldedatei, um zu bestimmen, ob der im infacmd pwx-Programm bereitgestellten Benutzer-ID die Ausführung von Befehlen gewährt werden soll.
-OSPassword -oup	OS_password	Erforderlich, wenn Sie einen Benutzernamen ohne verschlüsseltes Passwort festlegen. Passwort für das Betriebssystem. Sie können ein Klartextpasswort mit der Option -p oder der Umgebungsvariable INFA_DEFAULT_PWX_OSPASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -p festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-OSEPassword -ouep	OS_epassword	Erforderlich, wenn Sie einen Benutzernamen ohne Klartextpasswort festlegen. Verschlüsseltes Passwort für das Betriebssystem. Sie können ein verschlüsseltes Passwort mit der Option -e oder der Umgebungsvariable INFA_DEFAULT_PWX_OSEPASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -e festgelegte Passwort Vorrang.
-applicationid -a	appname	Erforderlich, wenn Sie -taskid nicht angeben. Anwendungsname. Der Name des aktiven Extraktionsvorgangs, der angehalten werden soll. Die PWX-00712-Meldung der infacmd pwx listtaskListener-Befehlsausgabe zeigt diesen Namen an.
-taskid -t	taskid	Erforderlich, wenn Sie -application nicht angeben. Aufgaben-ID des Listenerdiensts. Die numerische ID für die Listenerdienstsaufgabe, die angehalten werden soll. **Tipp:** Um den Namen der aktiven Aufgabe zu bestimmen, verwenden Sie den Befehl infacmd pwx listtaskListener. In der Befehlsausgabe zeigt der Namenwert in der PWX-00712-Meldung die Aufgaben-ID an.

UpgradeModels

Aktualisiert nichtrelationale Datenobjekte von PowerExchange 9.0.1. Sie müssen die Datenobjekte upgraden, bevor Sie sie verwenden können.

Der Befehl zeigt die Ergebnisse des Upgrades sortiert nach Verbindungsname, Schema und Map-Name an. Sie können den UpgradeModels-Befehl mehrmals ausführen, wenn bestimmte Objekte nicht beim ersten Mal aktualisiert werden.

Der Befehl überprüft, ob das Daten-Mapping mit den nichtrelationalen Operationen übereinstimmt, die dafür beim Importieren des nichtrelationalen Objekts definiert wurden. Wenn Abweichungen bestehen, werden die nichtrelationalen Operationen gelöscht und neu erstellt, um mit dem Daten-Mapping übereinzustimmen. Sie müssen alle betroffenen Mappings oder Mapplets ändern, um die neu erstellten nichtrelationalen Operationen zu verwenden.

Der Befehl „infacmd pwx UpgradeModels“ verwendet die folgende Syntax:

```
UpgradeModels

[<-DomainName|-dn> domain_name]

[<-UserName|-un> user_name]

[<-Password|-pd> password]

<-MrsServiceName|-msn> mrs_service_name

<-ConnectionName|-cn> connection_name

<-DataObjectSchemaName|ds> data_object_schema_name

<-DataObjectName|do> data_object_name
```

```
<-Preview|pr> preview

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-ServiceName|-sn> service_name]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx UpgradeModels“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-MrsServiceName -msn	mrs_service_name	Erforderlich. Name des Modellrepository-Dienst. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositorys kompatibel sein. Der Name darf nicht länger als 230 Zeichen sein und keine führenden oder abschließenden Leerzeichen, Wagenrückläufe, Tabulatoren oder die folgenden Zeichen enthalten: `/ * ? < > " |`
-ConnectionName -cn	connection_name	Erforderlich. Name der Verbindung, die die nichtrelationalen Datenobjekte enthält, die aktualisiert werden sollen. Um alle Verbindungen oder alle Verbindungen mit dem gleichen Anfangsnamensmuster anzugeben, setzen Sie das Platzhalterzeichen Sternchen (*) in doppelte Anführungszeichen, z. B. "*" oder ABC"*".
-DataObjectSchemaName -ds	data_object_schema_name	Erforderlich. Name des Schemas, das die Datenzuordnungen der nichtrelationalen Datenobjekte enthält, die aktualisiert werden sollen. Um alle Schemas oder alle Schemas mit dem gleichen Anfangsnamensmuster anzugeben, setzen Sie das Platzhalterzeichen Sternchen (*) in doppelte Anführungszeichen, z. B. "*" oder ABC"*".

Option	Argument	Beschreibung
-DataObjectName -do	data_object_name	Erforderlich. Name der Datenzuordnung des nichtrelationalen Datenobjekts, das aktualisiert werden soll. Um alle Datenzuordnungen oder alle Datenzuordnungen mit dem gleichen Anfangsnamensmuster anzugeben, setzen Sie das Platzhalterzeichen Sternchen (*) in doppelte Anführungszeichen, z. B. "*" oder ABC"*".
-Preview -pr	Vorschau	Erforderlich. Geben Sie „Y“ an, um eine Vorschau der Upgrade-Ergebnisse anzuzeigen, ohne diese zu bestätigen. Geben Sie „N“ an, um ein Upgrade der Objekte durchzuführen. Um eine erfolgreiche Ausführung des Befehls sicherzustellen, legen Sie „Preview“ auf „Y“ fest und führen den UpgradeModels-Befehl aus, bevor Sie das tatsächliche Upgrade durchführen.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Optional. Name des Listenerdiensts. Der Befehl verwendet zuerst den Verbindungsnamen zum Abrufen der angegebenen Daten-Mappings. Wenn der Versuch fehlschlägt, verwendet der Befehl den Namen des Listenerdiensts zum Abrufen von Daten-Mappings. Bei diesem Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden. Der Name darf nicht länger als 128 Zeichen sein und keine Wagenrückläufe, Tabulatoren, Leerzeichen oder die folgenden Zeichen enthalten: `/ * ? < > " |`

UpdateListenerService

Aktualisiert die Eigenschaften eines PowerExchange-Listenerdiensts.

Der Befehl „infacmd pwx UpdateListenerService“ verwendet die folgende Syntax:

```
UpdateListenerService

[<-DomainName|-dn> domain_name]

[<-UserName|-un> user_name]

[<-Password|-pd> password]

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

[<-LicenseName|-ln> license_name]

[<-NodeName|-nn> node_name]

[<-BackupNode|-bn> backup_node]

[<-StartParameters|-sp> start_parameters>]

[<-SvcPort|-sp> service_port]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx UpdateListenerService“ beschrieben:

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

Option	Argument	Beschreibung
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Listenerdiensts.

Option	Argument	Beschreibung
-LicenseName -ln	license_name	Optional. Lizenz zur Zuweisung zum Dienst. Wenn nicht bereits bereitgestellt, erforderlich, bevor Sie den Dienst aktivieren können.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Listenerdienst ausgeführt werden soll.
-BackupNode -bn	backup_node	Optional. Wenn die PowerCenter-Umgebung für hohe Verfügbarkeit konfiguriert ist, wird mit dieser Option der Name des Backup-Knotens angegeben.

Option	Argument	Beschreibung
-StartParameters -sp	start_parameters	Optional. Parameter, die beim Starten des Listenerdiensts einbezogen werden müssen. Trennen Sie die Parameter durch Leerzeichen. Sie können die folgenden Parameter einbeziehen: - *node_name* Knotenname, der den Listenerdienst identifiziert. Dieser Name muss mit dem Namen in der LISTENER-Anweisung in der Konfigurationsdatei DBMOVER übereinstimmen. - config=*directory* Gibt den vollständigen Pfad und Dateinamen für die Konfigurationsdatei „dbmover.cfg“ an, die Sie anstelle der Standarddatei „dbmover.cfg“ verwenden möchten. Diese alternative Konfigurationsdatei hat Vorrang vor jeder anderen alternativen Konfigurationsdatei, die Sie in der Umgebungsvariable PWX_CONFIG angeben. - license=*directory/license_key_file* Gibt den vollständigen Pfad und Dateinamen für eine Lizenzschlüsseldatei an, die Sie anstelle der Standarddatei license.key verwenden möchten. Diese alternative Lizenzschlüsseldatei und die Standarddatei dürfen nicht denselben Namen und denselben Pfad haben. Entweder Name oder Pfad muss unterschiedlich sein. Diese alternative Lizenzschlüsseldatei hat Vorrang vor jeder anderen alternativen Lizenzschlüsseldatei, die Sie in der Umgebungsvariable PWX_LICENSE angeben. **Hinweis:** In den Konfigurations- und Lizenzparametern müssen Sie den vollständigen Pfad nur dann angeben, wenn die Datei sich *nicht* im Installationsverzeichnis befindet. Schließen Sie Pfad- und Dateinamen, die Leerzeichen enthalten, in Anführungszeichen ein.
-SvcPort -sp	service_port	Optional. Port des Listenerdiensts für die Reaktion auf Befehle vom Dienstmanager.

UpdateLoggerService

Aktualisiert die Eigenschaften eines PowerExchange-Protokollierungsdiensts.

Der Befehl „infacmd pwx UpdateLoggerService“ verwendet die folgende Syntax:

```
UpdateLoggerService

[<-DomainName|-dn> domain_name]

[<-UserName|-un> user_name]

[<-Password|-pd> password]

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-NodeName|-nn> node_name

[<-LicenseName|-ln> license_name]

[<-BackupNode|-bn> backup_node]

[<-StartParameters|-sp> start_parameters>]

[<-SvcPort|-sp> service_port]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd pwx UpdateLoggerService“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie den Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Protokollierungsdiensts.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Protokollierungsdienst ausgeführt werden soll.
-LicenseName -ln	license_name	Lizenz zur Zuweisung zum Dienst. Wenn nicht bereits bereitgestellt, erforderlich, bevor Sie den Dienst aktivieren können.
-BackupNode -bn	backup_node	Optional. Wenn die PowerCenter-Umgebung für hohe Verfügbarkeit konfiguriert ist, wird mit dieser Option der Name des Backup-Knotens angegeben.

Option	Argument	Beschreibung
-StartParameters -sp	start_parameters	Optional. Parameter, die beim Starten des Protokollierungsdiensts einbezogen werden müssen. Trennen Sie die Parameter durch Leerzeichen. Sie können die folgenden Parameter einbeziehen: - coldstart={Y|N} Gibt an, ob der Protokollierungsdienst kalt oder warm gestartet wird. Geben Sie Y für einen Kaltstart des Protokollierungsdiensts ein. Wenn die CDCT-Datei Protokolldatensätze enthält, löscht der Protokollierungsdienst diese Datensätze. Geben Sie N ein, um den Protokollierungsdienst ab dem Neustartpunkt warm zu starten, der in der CDCT-Datei angegeben ist. Standardwert ist „N“. - config=*directory/pwx_config_file* Gibt den vollständigen Pfad und Dateinamen für die Konfigurationsdatei „dbmover.cfg“ an, die Sie anstelle der Standarddatei „dbmover.cfg“ verwenden möchten. Diese alternative Konfigurationsdatei hat Vorrang vor jeder anderen alternativen Konfigurationsdatei, die Sie in der Umgebungsvariable PWX_CONFIG angeben. - cs=*directory/pwxlogger_config_file* Gibt den Pfad und Dateinamen für die Konfigurationsdatei des Protokollierungsdiensts an. Sie können auch den cs-Parameter verwenden, um eine Protokollierungsdienst-Konfigurationsdatei anzugeben, die die Standarddatei pwxccl.cfg überschreibt. Diese Überschreibungsdatei und die Standarddatei dürfen nicht denselben Namen und denselben Pfad haben. Entweder Name oder Pfad muss unterschiedlich sein. - encryptepwd=*encrypted_password* Ein Passwort im verschlüsselten Format zum Aktivieren der Verschlüsselung von Protokolldateien der PowerExchange-Protokollierung. Mit diesem Passwort kann die PowerExchange-Protokollierung einen eindeutigen Verschlüsselungsschlüssel für jede Protokolldatei der Protokollierung erzeugen. Das Passwort wird in der CDCT-Datei im verschlüsselten Format gespeichert. Aus Sicherheitsgründen wird das Passwort weder in CDCT-Sicherungsdateien gespeichert noch in den CDCT-Berichten angezeigt, die mit dem PowerExchange-Dienstprogramm PWXUCDCT erzeugt werden können. Bei Angabe dieses Parameters müssen Sie auch coldstart=y angeben. Wenn Sie diesen Parameter und den Parameter ENCRYPTEPWD in der Konfigurationsdatei (pwxccl.cfg) der PowerExchange-Protokollierung angeben, hat der Parameter in der Konfigurationsdatei Vorrang. Wenn Sie diesen Parameter und den Parameter ENCRYPTPWD in der Konfigurationsdatei der PowerExchange-Protokollierung angeben, tritt ein Fehler auf. Sie können den AES-Algorithmus festlegen, um ihn zum Verschlüsseln der Protokolldatei im Parameter ENCRYPTOPT der Datei „pwxccl.cfg“ zu verwenden. Standardwert ist AES128.

Option	Argument	Beschreibung
		Tipp: Zur Sicherheitsoptimierung empfiehlt Informatica, das Verschlüsselungspasswort beim Kaltstart der PowerExchange-Protokollierung und nicht in der Konfigurationsdatei „pwxccl.cfg“ anzugeben. Mit dieser Vorgehensweise verringern Sie aus folgenden Gründen das Risiko eines böswilligen Zugriffs auf das Verschlüsselungspasswort: 1) Das Verschlüsselungspasswort ist nicht in der Datei „pwxccl.cfg“ gespeichert. 2) Sie können das Passwort nach einem erfolgreichen Kaltstart aus der Befehlszeile löschen. Wenn Sie das Verschlüsselungspasswort für einen Kaltstart angeben und die CDCT-Datei dann zu einem späteren Zeitpunkt wiederherstellen müssen, müssen Sie dasselbe Verschlüsselungspasswort im Befehl RESTORE_CDCT des Dienstprogramms PWXUCDCT eingeben. Um die Protokolldateien der PowerExchange-Protokollierung *nicht* zu verschlüsseln, geben Sie kein Verschlüsselungspasswort ein. - license=*directory/license_key_file* Gibt den vollständigen Pfad und Dateinamen für eine Lizenzschlüsseldatei an, die Sie anstelle der Standarddatei license.key verwenden möchten. Diese alternative Lizenzschlüsseldatei und die Standarddatei dürfen nicht denselben Namen und denselben Pfad haben. Entweder Name oder Pfad muss unterschiedlich sein. Diese alternative Lizenzschlüsseldatei hat Vorrang vor jeder anderen alternativen Lizenzschlüsseldatei, die Sie in der Umgebungsvariable PWX_LICENSE angeben. - specialstart={Y|N} Gibt an, ob ein Sonderstart der PowerExchange-Protokollierung durchgeführt werden soll. Ein Sonderstart startet die Verarbeitung der PowerExchange-Erfassung an dem Punkt im Änderungsstrom, den Sie in der Datei „pwxccl.cfg“ angeben. Dieser Startpunkt überschreibt den Neustartpunkt aus der CDCT-Datei für die PowerExchange-Protokollierungsausführung. Bei einem Sonderstart wird kein Inhalt aus der CDCT-Datei gelöscht. Verwenden Sie diesen Parameter zum Überspringen problematischer Stellen in den Quellprotokollen, ohne dabei erfasste Daten zu verlieren. Verwenden Sie einen Sonderstart beispielsweise in folgenden Situationen: - Sie möchten nicht, dass die PowerExchange-Protokollierung eine Aktualisierung eines Oracle-Katalogs erfasst. Stoppen Sie in diesem Fall die PowerExchange-Protokollierung vor der Aktualisierung. Erzeugen Sie nach Abschluss der Aktualisierung eine neue Sequenz und starten Sie Token für die PowerExchange-Protokollierung basierend auf dem Post-Upgrade-SCN neu. Geben Sie diese Token-Werte in den Parametern SEQUENCE_TOKEN und RESTART_TOKEN in der Datei „pwxccl.cfg“ ein und führen Sie dann einen Sonderstart der PowerExchange-Protokollierung durch. - Sie möchten nicht, dass von der PowerExchange-Protokollierung alte, nicht verfügbare Protokolle erneut verarbeitet werden, die durch ausstehende Arbeitseinheiten verursacht wurden, die nicht zu CDC gehören. Stoppen Sie in diesem Fall die PowerExchange-

Option	Argument	Beschreibung
		Protokollierung. Bearbeiten Sie den Wert RESTART_TOKEN, um den SCN des frühesten verfügbaren Protokolls widerzuspiegeln, und führen Sie dann einen Sonderstart durch. Wenn alle ausstehenden Arbeitseinheiten, die vor diesem Neustartpunkt gestartet wurden, zu CDC gehören, gehen unter Umständen Daten verloren. Gültige Werte: - Y. Führen Sie einen Sonderstart der PowerExchange-Protokollierung ab dem Punkt im Änderungsstrom durch, der von den Parameterwerten SEQUENCE_TOKEN und RESTART_TOKEN in der Konfigurationsdatei „pwxccl.cfg“ definiert wird. Sie müssen gültige Token-Werte in der Datei „pwxccl.cfg“ angegeben, um einen Sonderstart durchzuführen. Diese Token-Werte überschreiben die Token-Werte aus der CDCT-Datei. Stellen Sie sicher, dass der Wert SEQUENCE_TOKEN in der Datei „pwxccl.cfg“ größer oder gleich dem aktuellen Sequenz-Token in der CDCT-Datei ist. Geben Sie den Parameter coldstart=Y nicht noch zusätzlich an. Wenn Sie den Parameter coldstart=Y angeben, hat dieser Parameter Vorrang. - N. Führen Sie keinen Sonderstart durch. Führen Sie einen Kalt- oder Warmstart, wie vom coldstart-Parameter angegeben, durch. Standardwert ist „N“. **Hinweis:** In den Konfigurations-, cs- und Lizenzparametern müssen Sie den vollständigen Pfad nur dann angeben, wenn die Datei sich *nicht* im Installationsverzeichnis befindet. Schließen Sie Pfad- und Dateinamen, die Leerzeichen enthalten, in Anführungszeichen ein.
-SvcPort -sp	service_port	Port des Protokollierungsdiensts für die Reaktion auf Befehle vom Dienstmanager.

KAPITEL 21

infacmd rms-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- ListComputeNodeAttributes, 849
- ListServiceOptions, 851
- SetComputeNodeAttributes, 852
- UpdateServiceOptions, 854

ListComputeNodeAttributes

Listet die Attribute des Berechnungsknotens auf, die für den angegebenen oder für alle Knoten übersprungen wurden. Verwenden Sie den infacmd rms SetComputeNodeAttributes-Befehl, um die Attribute des Berechnungsknotens zu überspringen.

Bei den Standardwerten für die Attribute handelt es sich um die tatsächliche Anzahl der Kerne und den auf dem Computer verfügbaren Speicher. Wenn der infacmd rms ListComputeNodeAttributes-Befehl keinen Wert für ein Attribut auflistet, verwendet der Ressourcenmanager-Dienst die Standardwerte.

Der infacmd rms ListComputeNodeAttributes-Befehl verwendet die folgende Syntax:

```
ListComputeNodeAttributes

<-DomainName|-dn> domain_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password

[<-NodeName|-nn> node_name]

[<-ServiceName|-sn> service_name]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd rms ListComputeNodeAttributes“ beschrieben:

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

ListServiceOptions

Listet die Eigenschaften für den Ressourcenmanager-Dienst auf.

Der infacmd rms ListServiceOptions-Befehl verwendet die folgende Syntax:

```
ListServiceOptions

<-DomainName|-dn> domain_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password

[<-ServiceName|-sn> service_name]

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd rms ListServiceOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Optional. Geben Sie Resource_Manager_Service ein.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

SetComputeNodeAttributes

Überschreibt die Berechnungsknotenattribute für den angegebenen Knoten.

Bei den Standardwerten für die Attribute handelt es sich um die tatsächliche Anzahl der Kerne und den auf dem Computer verfügbaren Speicher. Zum Zurücksetzen einer Option auf ihren Standardwert geben Sie -1 als Wert ein.

Der infacmd rms SetComputeNodeAttributes-Befehl verwendet die folgende Syntax:

```
SetComputeNodeAttributes

<-DomainName|-dn> domain_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password

<-NodeName|-nn> node_name
```

```
[<-MaxCores|-mc> max_number_of_cores_to_allocate]

[<-MaxMem|-mm> max_memory_in_mb_to_allocate]

[<-ServiceName|-sn> service_name]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd rms SetComputeNodeAttributes“ beschrieben:

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

Option	Argument	Beschreibung
-MaxCores -mc	max_number_of_cores_to_allocate	Optional. Maximale Anzahl der Kerne, die der Ressourcenmanager-Dienst für Jobs zuweisen kann, die auf dem Berechnungsknoten ausgeführt werden. Ein Berechnungsknoten benötigt mindestens fünf verfügbare Knoten, um einen Container zum Starten eines DTM-Prozesses zu initialisieren. Wenn ein beliebiger dem Gitter zugewiesener Berechnungsknoten weniger als fünf Kerne aufweist, wird diese Anzahl als Mindestanzahl der Kerne verwendet, die zum Initialisieren eines Containers notwendig sind. Standardmäßig stellt die maximale Anzahl der Kerne die tatsächliche Anzahl der auf dem Computer verfügbaren Kerne dar.
-MaxMem -mm	max_memory_in_mb_to_allocate	Optional. Maximale Speichermenge in Megabyte, die vom Ressourcenmanager-Dienst für Jobs zugwiesen werden kann, die auf dem Berechnungsknoten ausgeführt werden. Ein Berechnungsknoten benötigt mindestens 2,5 GB Speicher, um einen Container zum Starten eines DTM-Prozesses zu initialisieren. Standardmäßig stellt die maximale Speichermenge die tatsächlich auf dem Computer verfügbare Speichermenge dar.
-ServiceName -sn	service_name	Optional. Geben Sie Resource_Manager_Service ein.

UpdateServiceOptions

Aktualisiert die Eigenschaften des Ressourcenmanager-Diensts. Führen Sie diesen Befehl aus, um den primären und den Backup-Knoten für den Ressourcenmanager-Dienst zu konfigurieren.

Sie können die Eigenschaften ändern, während der Dienst ausgeführt wird, aber Sie müssen den Dienst neu starten, damit die geänderten Eigenschaften wirksam werden.

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

```
UpdateServiceOptions

<-DomainName|-dn> domain_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password

[<-ServiceName|-sn> service_name]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-Options|-o> options]

[<-NodeName|-nn> primary_node_name]

[<-BackupNodes|-bn> backup_node_name1,backup_node_name2,...]
```

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

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Options -o	options	Optional. Geben Sie jede Option durch ein Leerzeichen getrennt ein.
-NodeName -nn	primary_node_name	Optional. Primärer Knoten, auf dem der Ressourcenmanager-Dienst ausgeführt wird.
-BackupNodes -bn	backup_node_name1,backup_node_name2,...	Optional. Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist.

Optionen des Ressourcenmanager-Diensts

Verwenden Sie die Optionen des Ressourcenmanager-Diensts mit dem infacmd rms UpdateServiceOptions-Befehl.

Geben Sie die Optionen des Ressourcenmanager-Diensts in folgendem Format ein:

```
... -o option_type.option_name=value
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Optionen des Ressourcenmanager-Diensts beschrieben:

Option	Beschreibung
ResourceManagerServiceOptions.Log_Level	Ebene der Fehlermeldungen, die der Ressourcenmanager-Dienst in das Dienstprotokoll schreibt. Wählen Sie eine der folgenden Meldungsebenen aus: Fatal, Error, Warning, Info, Trace oder Debug.

KAPITEL 22

infacmd rtm-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- DeployImport, 857
- Export, 859
- Import, 862

DeployImport

Importiert den Inhalt aus einer Anwendungsdatei in der Datenbank, die vom Modellrepository gelesen wird.

Der Befehl „infacmd rtm DeployImport“ verwendet die folgende Syntax:

```
DeployImport

<-DomainName|-dn> Domain name

<-UserName|-un> User name

<-Password|-pd> Password

<-securityDomain|-sdn> Security domain

[<-Gateway|-hp> Domain gateway host:port]

[<-NodeName|-nn> Node name]

<-DataIntegrationService|-ds> Data Integration Service name

<-CodePage|-cp> Code page

<-Folder|-f> The folder to import from

<-MetadataFile|-mf> Metadata file
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd rtm DeployImport“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	Domänenname	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	Benutzername	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-securityDomain -sdn	Sicherheitsdomäne	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	Host des Domänen-Gateways:Port	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Geben Sie den Hostnamen und die Portnummer für den Gateway-Knoten in der Domäne ein. Verwenden Sie folgende Syntax: `gateway_hostname:HttpPort`
-NodeName -nn	Knotenname	Optional. Name des Gateway-Knotens für den Modellrepository-Dienst.

Option	Argument	Beschreibung
-DataIntegrationService -ds	Name des Datenintegrationsdiensts	Erforderlich. Name des Datenintegrationsdiensts.
-CodePage -cp	Codepage	Erforderlich. Codepage für die zu importierenden Referenzdaten.
-Folder -f	Der Ordner, aus dem importiert wird	Erforderlich. Pfad des Ordners, der die zu importierenden Dateien enthält. Sie führen den Befehl DeployImport auf dem Computer aus, auf dem der Ordner gespeichert ist. Die Ordneroption beschreibt einen Pfad auf dem Computer, auf dem der Befehl ausgeführt wird.
-MetadataFile -mf	Metadatendatei	Erforderlich. Vollständiger Name und Pfad für die Anwendungsdatei, auf die der Befehl angewendet wird.

Export

Exportieren von Daten aus Referenztabellen. Sie können Referenztabellenobjekte oder nur die Daten exportieren. Sie können Daten aus verwalteten und nicht verwalteten Referenztabellen exportieren.

Definieren Sie die Exportdaten mit einer der folgenden Optionen:

- ProjectFolder. Name des Projekts oder Ordners, der exportiert werden soll.
- MetadataFile. Name einer metadata.xml-Datei, die auf die zu exportierenden Referenztabellen verweist.
- ObjectList. Vollständiger Pfad zu einer Textdatei, die eine Liste der zu exportierenden Dateien enthält.

Wenn Sie eine Objektliste konfigurieren, erstellen Sie eine Textdatei, die eine Liste von Objekten mit der folgenden Syntax enthält:

```
ProjectName/FolderName/reference_table_object1
ProjectName/FolderName/reference_table_object2
ProjectName/FolderName/reference_table_object3
```

Hinweis: Sie müssen jeden Pfad in der Objektliste mit Schrägstrichen konfigurieren. Verwenden Sie keine umgekehrten Schrägstriche im Pfad.

Der Befehl „infacmd rtm Export“ verwendet die folgende Syntax:

```
Export

<-DomainName|-dn> Domain name

<-UserName|-un> User name

<-Password|-pd> Password

<-SecurityDomain|-sdn> Security domain

[<-Gateway|-hp> Domain gateway host:port]

[<-NodeName|-nn> Node name]

<-RepositoryService|-rs> Model Repository Service name
```

```
<-CodePage|-cp> Code Page

<-Folder|-f> The folder to export to

[<-ObjectList|-ol> List of Obects to export]

[<-ProjectFolder|-pf> Name of the project folder to export]

[<-metadataFile|-mf> Metadata file]

[<-Recursive|-r> Include subfolders when exporting project folder]

[<-SkipDatGeneration|-sdg> Skip Data Generation]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd rtm Export“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	Sicherheitsdomäne	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	Hostname des Domänen-Gateways:Portnummer	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Geben Sie den Hostnamen und die Portnummer für den Gateway-Knoten in der Domäne ein. Verwenden Sie folgende Syntax: `gateway_hostname:HttpPort`
-NodeName -nn	Knotenname	Optional. Name des Gateway-Knotens für den Modellrepository-Dienst.
-RepositoryService -rs	Name des Modellrepository-Diensts	Name des Modellrepository-Diensts.
-CodePage -cp	Codepage	Erforderlich. Codepage für die Referenzdaten.
-Folder -f	Der Ordner, in den exportiert wird	Erforderlich. Zielspeicherort für die Exportdatei.
-ObjectList -ol	Liste der zu exportierenden Objekte	Vollständig qualifizierter Dateiname, der eine Liste der Referenztabellenobjekte enthält. Konfigurieren Sie diese Option nicht mit der Option ProjectFolder oder metadataFile.
-ProjectFolder -pf	Name des zu exportierenden Projektordners	Name des Projekts und Ordners, die exportiert werden sollen. Verwenden Sie folgende Syntax: `ProjectName/FolderName` Verwenden Sie zur Konfiguration weder die Option metadataFile noch die Option ObjectList.
-metadataFile -mf	Metadatendatei	Erforderlich für den Export von Objekten. Vollständiger Pfad und Name für eine metadata.xml-Datei, auf die der Befehl angewendet werden soll. Exportiert alle Referenztabellen, die in der Datei „metadata. xml“·enthalten sind. Konfigurieren Sie diese Option nicht mit der Option ProjectFolder oder ObjectList.

Option	Argument	Beschreibung
-Recursive -r	Beim Exportieren des Projektordners Unterordner berücksichtigen	Optional. Verwenden Sie diese Option mit der Option ProjectFolder. Exportieren Sie mehr als eine Ebene des Objekts. Standardwert ist „nicht rekursiv“.
-SkipDatGeneration -sdg	Datenerzeugung überspringen	Optional. Schreibt eine DAT-Datei, die die Struktur der Referenztabelle beschreibt, in den Verzeichnissatz in der Ordnereigenschaft. Beim Importieren der Referenztabelle wird diese Datei nicht verwendet. Standardwert ist „False“.

Import

Führt einen Metadaten- und Datenimport aus Objektexportdateien durch. Importiert Referenztabellen-Metadaten in das Modellrepository und importiert die Daten in die Referenzdaten-Datenbank. Importiert auch Referenzdaten ohne die Metadaten.

Bevor Sie Referenztabellendaten importieren, muss das Projekt im Modellrepository vorhanden sein.

Der Befehl „infacmd rtm Import“ verwendet die folgende Syntax:

```
Import

<-DomainName|-dn> Domain name

<-UserName|-un> User name

<-Password|-pd> Password

<-securityDomain|-sdn> Security domain

[<-Gateway|-hp> Domain gateway host:port]

[<-NodeName|-nn> Node name]

<-RepositoryService|-rs> Model Repository Service name

<-CodePage|-cp> Code page

<-ConflictResolution|-cr> Conflict resolution

<-ImportType|-it> Import type

<-Folder|-f> The folder to import from

[<-FileName|-fn> Required only for importing a single dictionary]

[<-MetadataFile|-mf> Required only for Object import]

[<-ProjectFolder|-pf> Name of the project folder to import into]

[<-NotRecursive|-nr> Don't include subfolders]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd rtm Import“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	Domänenname	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable *INFA_DEFAULT_DOMAIN* festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	Benutzername	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-securityDomain -sdn	Sicherheitsdomäne	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	Host des Domänen-Gateways:Port	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Name und Portnummer für den Gateway-Knoten in der Domäne. Verwenden Sie folgende Syntax: `gateway_hostname:HttpPort`
-NodeName -nn	Knotenname	Optional. Name des Gateway-Knotens für den Modellrepository-Dienst.

Option	Argument	Beschreibung
-RepositoryService -rs	Name des Modellrepository -Diensts	Erforderlich. Name des Modellrepository-Diensts.
-CodePage -cp	Codepage	Erforderlich. Codepage für die Referenzdaten.
-ConflictResolution -cr	Konfliktlösung	Erforderlich. Definiert das Verhalten bei Auftreten eines Namenskonflikts. Geben Sie eines der folgenden Argumente ein: - Replace. Entfernen Sie die bestehende Referenztabelle aus der Datenbank und erstellen Sie eine neue Referenztabelle. - Rename. Erstellen Sie eine neue Referenztabelle mit einem anderen Namen. - Skip. Importieren Sie die Referenztabelle nicht.
-ImportType -it	Importtyp	Erforderlich. Der Typ des zu importierenden Inhalts. Geben Sie MetadataAndData für den Metadaten- und Datenimport ein.
-Folder -f	Der Ordner, aus dem importiert wird	Erforderlich für den Metadaten- und Datenimport. Vollständiger Pfad zu dem Ordner, der die zu importierende Referenzdatendatei enthält.
-FileName -fn	Nur für den Import eines einzelnen Wörterbuchs erforderlich	Erforderlich für den Import von Metadaten und Daten, wenn Sie Daten aus einer einzelnen Datei importieren. Name der Datei, die die gewünschten Referenzdaten zum Importieren enthält. Der Dateiname ist relativ zum Ordnerpfad.
-MetadataFile -mf	Nur für den Import von Objekten erforderlich	Erforderlich, wenn Sie nur Referenzdatenwerte importieren. Vollständiger Pfad und Name für die metadata.xml-Datei, auf die der Befehl angewendet werden soll. Die Datei „metadata.xml“ enthält die Metadaten, die mit den Referenzdatenwerten verknüpft sind. Nicht mit der Option ProjectFolder verwenden.
-ProjectFolder -pf	Name des Projektordners zum Importieren in	Erforderlich, wenn Sie Referenzdaten und Metadaten importieren. Name des Modellrepository-Projekts, in das Sie importieren möchten. Nicht mit der Option MetadataFile verwenden.
-NotRecursive -nr	- Unterordner nicht einbeziehen	Optional. Verwendung mit Metadaten- und Datenimport. Nur eine Objektebene importieren. Standardwert ist „rekursiv“.

KAPITEL 23

infacmd sch-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- CreateSchedule, 865
- DeleteSchedule, 873
- ListSchedule, 875
- ListServiceOptions, 877
- ListServiceProcessOptions, 879
- PauseAll, 881
- PauseSchedule, 882
- ResumeAll, 884
- ResumeSchedule, 885
- UpdateSchedule, 887
- UpdateServiceOptions, 891
- UpdateServiceProcessOptions, 894
- Upgrade, 896

CreateSchedule

Erstellt einen Zeitplan für bereitgestellte Mappings, bereitgestellte Arbeitsabläufe, Profile und Scorecards.

Der infacmd sch CreateSchedule-Befehl verwendet die folgende Syntax:

```
CreateSchedule
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ScheduleName|-scn> schedule_name
[<-ScheduleDescription|-scd> schedule_description]
<-Recurrence|-r> once|daily|weekly|monthly
```

```
<-StartTime|-st> yyyy-MM-dd HH:mm

[<-EndTime|-et> yyyy-MM-dd HH:mm]

[<-TimeZone|-tz> time_zone]

[<-DailyRunEvery|-dre> daily_run_every]

[<-RunDaysOfWeek|-rdw> mon|tue|wed|thu|fri|sat|sun]

[<-RunDayOfWeekMonth|-rdwm> monday|tuesday|wednesday|thursday|friday|saturday|sunday]

[<-RunDayOfMonth|-rdm> 1-30|LAST_DAY_OF_MONTH]

[<-RepeatCount|-rc> repeat_count]

[<-RunnableObjects|-ro> runnable_objects]

[<-Status|-ss> SCHEDULED|SUSPENDED]

[<-RunNow|-rn> true|false]
```

Zum Konfigurieren mehrerer Werte für ein Argument trennen Sie die Werte durch Kommas.

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sch CreateSchedule“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ScheduleName -scn	schedule_name	Erforderlich. Name des Zeitplans. Beim Namen des Zeitplans wird die Groß-/Kleinschreibung beachtet.
-Description -scd	schedule_description	Optional. Beschreibung des Zeitplans.
-Recurrence -r	once|daily|weekly|monthly	Erforderlich. Geben Sie an, ob der Zeitplan einmal oder mehrmals ausgeführt wird.
-StartTime -st	yyyy-MM-dd HH:mm	Erforderlich. Datum und Uhrzeit des Beginns der Wiederholung.
-EndTime -et	yyyy-MM-dd HH:mm	Optional. Datum und Uhrzeit des Endes der Wiederholung.
-TimeZone -tz	Zeitzone	Optional. Zeitzone für den Anfangszeitpunkt des Zeitplans. Zum Konfigurieren der Zeitzone können Sie die ID-Nummer der Zeitzone oder die Olson-Datenbank-ID eingeben. Standardwert ist das Gebietsschema des Client-Computers.

Option	Argument	Beschreibung
-DailyRunEvery -dre	daily_run_every	Optional. Führen Sie den Zeitplan intervallweise aus. In der folgenden Liste werden die Optionen beschrieben, die Sie konfigurieren können: - Minute(n). Führen Sie den Zeitplan täglich alle n Minuten aus. - Stunde(n). Führen Sie den Zeitplan täglich alle n Stunden aus. - Tag(e). Führen Sie den Zeitplan alle n Tage aus. - Woche(n). Führen Sie den Zeitplan alle n Wochen aus. - Monat(e). Führen Sie den Zeitplan alle n Monate aus. - Jahr(e). Führen Sie den Zeitplan alle n Jahre aus. - ERSTER. Führen Sie den Zeitplan an jedem ersten n-ten Tag des Monats aus. Verwenden Sie die Option -rdwm, um den Wochentag oder die Wochentage anzugeben. - ZWEITER. Führen Sie den Zeitplan an jedem zweiten n-ten Tag des Monats aus. Verwenden Sie die Option -rdwm, um den Wochentag oder die Wochentage anzugeben. - DRITTER. Führen Sie den Zeitplan an jedem dritten n-ten Tag des Monats aus. Verwenden Sie die Option -rdwm, um den Wochentag oder die Wochentage anzugeben. - VIERTER. Führen Sie den Zeitplan an jedem vierten n-ten Tag des Monats aus. Verwenden Sie die Option -rdwm, um den Wochentag oder die Wochentage anzugeben. - LETZTER. Führen Sie den Zeitplan an jedem letzten n-ten Tag des Monats aus. Verwenden Sie die Option -rdwm, um den Wochentag oder die Wochentage anzugeben.
-RunDaysOfWeek -rdw	mon|tue|wed|thu|fri|sat|sun	Optional. Führen Sie den Zeitplan an bestimmten Wochentagen aus.
-RunDayOfWeekMonth -rdwm	monday|tuesday| wednesday|thursday|friday| saturday|sunday	Optional. Führen Sie den Zeitplan monatlich an bestimmten Wochentagen aus. Verwenden Sie die Optionen -dre, um den Zeitplan alle ersten, zweiten, dritten, vierten oder letzten n-ten Tage des Monats auszuführen.
-RunDayofMonth -rdm	1-30| LAST_DAY_OF_MONTH	Optional. Führen Sie den Zeitplan an Tag n des Monats aus.
-RepeatCount -rc	repeat_count	Optional. Beenden Sie die Wiederholung nach einer bestimmten Anzahl an Ausführungen statt an einem bestimmten Datum.

Option	Argument	Beschreibung

-RunnableObjects
-ro
	runnableObjects	Optional. Objekte, die geplant werden sollen. Geben Sie den Objekttyp und dann den Pfad des Objekts im Datenintegrationsdienst an. Beispiel:
		`"mapping:DIS_1234/Application_mapping/Mapping_abc"`
		Optional können Sie die folgenden Argumente verwenden, um eine Parameterdatei, einen Parametersatz, das Ausführen als Benutzer oder ein Betriebssystemprofil für das Objekt zu konfigurieren:
		- parameterFilePath=PATH_TO_PARAMETER_FILE
		- parameterSet=PARAMETER_SET_NAME
		- runAsUser=USER_NAME
		&runAsUserSecurityDomain=SECURITY_DOMAIN
		&runAsUserPassword=PASSWORD
		- osProfileName=OS_PROFILE_NAME
		Beispiel:
		`"workflow:DIS_1234/Application_workflow/Workflow_abc?`
		`parameterFilePath=C://Informatica/Parameter Files/Parameter.xml`
		`&runAsUser=Administrator`
		`&runAsUserSecurityDomain=Native`
		`&runAsUserPassword=Administrator"`

-Status -ss	SCHEDULED|PAUSED	Optional. Erstellen Sie den Zeitplan mit dem Status „Geplant“ oder „Angehalten“.
-RunNow -rn	true|false	Führen Sie den Zeitplan sofort aus.

Gültige Zeitzonenparameter

Wenn Sie den Zeitzonenparameter eingeben, können Sie eine Zeitzonen-ID oder die Olson-Datenbank-ID eingeben.

In der folgenden Tabelle werden die Werte aufgelistet, die Sie für die Zeitzone eingeben können:

ID	Olson-Datenbank-ID	Name
0	Etc/GMT+12	(UTC-12:00) Internationale Datumsgrenze (Westen)
110	Etc/GMT+11	(UTC-11:00) Koordinierte Weltzeit-11
200	Pazifik/Honolulu	(UTC-10:00) Hawaii
300	Amerika/Anchorage	(UTC-09:00) Alaska
410	Amerika/Santa_Isabel	(UTC-08:00) Baja California
400	Amerika/Los_Angeles	(UTC-08:00) PST (Pacific Standard Time – USA, Kanada)

ID	Olson-Datenbank-ID	Name
520	Amerika/Phoenix	(UTC-07:00) Arizona
510	Amerika/Chihuahua	(UTC-07:00) Chihuahua, La Paz, Mazatlán
500	Amerika/Denver	(UTC-07:00) MST (Mountain Standard Time – USA, Kanada)
610	Amerika/Guatemala	(UTC-06:00) Mittelamerika
620	Amerika/Chicago	(UTC-06:00) CST (Central Standard Time – USA, Kanada)
630	Amerika/Mexico_City	(UTC-06:00) Guadalajara, Mexiko-Stadt, Monterrey
600	Amerika/Regina	(UTC-06:00) Saskatchewan
710	Amerika/Bogotá	(UTC-05:00) Bogotá, Lima, Quito, Rio Branco
700	Amerika/New_York	(UTC-05:00) EST (Eastern Standard Time – USA, Kanada)
720	Amerika/Indianapolis	(UTC-05:00) Indiana (Ost)
840	Amerika/Caracas	(UTC-04:30) Caracas
850	Amerika/Asunción	(UTC-04:00) Asunción
800	Amerika/Halifax	(UTC-04:00) AST (Atlantic Standard Time – Kanada)
810	Amerika/Cuiabá	(UTC-04:00) Cuiabá
830	Amerika/La_Paz	(UTC-04:00) Georgetown, La Paz, Manaus, San Juan
900	Amerika/St_Johns	(UTC-03:30) Neufundland
910	Amerika/Sao_Paulo	(UTC-03:00) Brasília
940	Amerika/Cayenne	(UTC-03:00) Cayenne, Fortaleza
950	Amerika/Buenos_Aires	(UTC-03:00) Buenos Aires Stadt
920	Amerika/Godthåb	(UTC-03:00) Grönland
930	Amerika/Montevideo	(UTC-03:00) Montevideo
820	Amerika/Santiago	(UTC-03:00) Santiago
1010	Etc/GMT+2	(UTC-02:00) Koordinierte Weltzeit-02
1100	Atlantik/Azoren	(UTC-01:00) Azoren
1110	Atlantik/Cape_Verde	(UTC-01:00) Kapverdische Inseln
1220	Afrika/Casablanca	(UTC) Casablanca

ID	Olson-Datenbank-ID	Name
1230	Etc/GMT	(UTC) Koordinierte Weltzeit
1200	Europa/London	(UTC) Dublin, Edinburgh, Lissabon, London
1210	Atlantik/Reykjavik	(UTC) Monrovia, Reykjavik
1340	Europa/Berlin	(UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
1300	Europa/Budapest	(UTC+01:00) Belgrad, Bratislava, Budapest, Ljubljana, Prag
1320	Europa/Paris	(UTC+01:00) Brüssel, Kopenhagen, Madrid, Paris
1310	Europa/Warschau	(UTC+01:00) Sarajevo, Skopje, Warschau, Zagreb
1330	Afrika/Lagos	(UTC+01:00) West-Zentralafrika
1350	Afrika/Windhuk	(UTC+01:00) Windhuk
1450	Asien/Amman	(UTC+02:00) Amman
1430	Europa/Bukarest	(UTC+02:00) Athen, Bukarest
1460	Asien/Beirut	(UTC+02:00) Beirut
1410	Afrika/Kairo	(UTC+02:00) Kairo
1480	Asien/Damaskus	(UTC+02:00) Damaskus
1470	Afrika/Johannesburg	(UTC+02:00) Harare, Pretoria
1420	Europa/Kiew	(UTC+02:00) Helsinki, Kiew, Riga, Sofia, Tallinn, Vilnius
1490	Europa/Istanbul	(UTC+02:00) Istanbul
1440	Asien/Jerusalem	(UTC+02:00) Jerusalem
1530	Europa/Kaliningrad	(UTC+02:00) Kaliningrad (RTZ 1)
1510	Asien/Bagdad	(UTC+03:00) Bagdad
1500	Asien/Riad	(UTC+03:00) Kuwait, Riad
1400	Europa/Minsk	(UTC+03:00) Minsk
1540	Europa/Moskau	(UTC+03:00) Moskau, St. Petersburg, Wolgograd (RTZ 2)
1520	Afrika/Nairobi	(UTC+03:00) Nairobi
1550	Asien/Teheran	(UTC+03:30) Teheran
1600	Asien/Dubai	(UTC+04:00) Abu Dhabi, Muskat

ID	Olson-Datenbank-ID	Name
1610	Asien/Baku	(UTC+04:00) Baku
1650	Indik/Mauritius	(UTC+04:00) Port Louis
1640	Asien/Tiflis	(UTC+04:00) Tiflis
1620	Asien/Eriwan	(UTC+04:00) Eriwan
1630	Asien/Kabul	(UTC+04:30) Kabul
1710	Asien/Taschkent	(UTC+05:00) Aschgabat, Taschkent
1700	Asien/Jekaterinburg	(UTC+05:00) Jekaterinburg (RTZ 4)
1750	Asien/Karatschi	(UTC+05:00) Islamabad, Karatschi
1720	Asien/Kalkutta	(UTC+05:30) Chennai, Kolkata, Mumbai, Neu-Delhi
1730	Asien/Colombo	(UTC+05:30) Sri Jayewardenepura
1740	Asien/Kathmandu	(UTC+05:45) Kathmandu
1800	Asien/Almaty	(UTC+06:00) Astana
1830	Asien/Dhaka	(UTC+06:00) Astana
1810	Asien/Nowosibirsk	(UTC+06:00) Nowosibirsk (RTZ 5)
1820	Asien/Rangun	(UTC+06:30) Yangon (Rangun)
1910	Asien/Bangkok	(UTC+07:00) Bangkok, Hanoi, Jakarta
1900	Asien/Krasnojarsk	(UTC+07:00) Krasnojarsk (RTZ 6)
2000	Asien/Schanghai	(UTC+08:00) Peking, Chongqing, Hongkong, Urumchi
2010	Asien/Irkutsk	(UTC+08:00) Irkutsk (RTZ 7)
2020	Asien/Singapur	(UTC+08:00) Kuala Lumpur, Singapur
2040	Australien/Perth	(UTC+08:00) Perth
2030	Asien/Taipeh	(UTC+08:00) Taipeh
2050	Asien/Ulan-Bator	(UTC+08:00) Ulan-Bator
2110	Asien/Tokio	(UTC+09:00) Osaka, Sapporo, Tokio
2100	Asien/Seoul	(UTC+09:00) Seoul
2120	Asien/Jakutsk	(UTC+09:00) Jakutsk (RTZ 8)
2140	Australien/Adelaide	(UTC+09:30) Adelaide

ID	Olson-Datenbank-ID	Name
2130	Australien/Darwin	(UTC+09:30) Darwin
2210	Australien/Brisbane	(UTC+10:00) Brisbane
2200	Australien/Sydney	(UTC+10:00) Canberra, Melbourne, Sydney
2240	Pazifik/Port_Moresby	(UTC+10:00) Guam, Port Moresby
2220	Australien/Hobart	(UTC+10:00) Hobart
2310	Asien/Magadan	(UTC+10:00) Magadan
2230	Asien/Wladiwostok	(UTC+10:00) Wladiwostok, Magadan (RTZ 9)
2300	Pazifik/Guadalcanal	(UTC+11:00) Salomonen, Neukaledonien
2410	Pazifik/Auckland	(UTC+12:00) Auckland, Wellington
2430	Etc/GMT-12	(UTC+12:00) Koordinierte Weltzeit+12
2400	Pazifik/Fidschi	(UTC+12:00) Fidschi
2500	Pazifik/Tongatapu	(UTC+13:00) Nuku'alofa
2510	Pazifik/Apia	(UTC+13:00) Samoa

DeleteSchedule

Löscht einen oder mehrere Zeitpläne, die vom Scheduler-Dienst verwaltet werden.

Der infacmd sch DeleteSchedule-Befehl verwendet die folgende Syntax:

```
DeleteSchedule
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ScheduleName|-scn> schedule_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sch DeleteSchedule“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ScheduleName -scn	schedule_name	Name des zu löschenden Zeitplans.

ListSchedule

Listet Zeitpläne oder geplante Objekte auf, die vom Scheduler-Dienst verwaltet werden. Der Befehl gibt Zeitpläne oder geplante Objekte zurück, die allen eingegebenen Optionen entsprechen.

Der infacmd sch ListSchedule-Befehl verwendet die folgende Syntax:

```
ListSchedule
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-ScheduleName|-scn> schedule_name]
[<-Description|-scd> description]
[<-RunnableObjects|-ro> runnable_objects]
[<-ScheduleStatus|-ss> created|scheduled|paused|complete]
[<-NumberOfFireTimes|-n> number_of_fire_times]
[<-MaxResults|-m> max_results]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp ListSchedule“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
ScheduleName -scn	schedule_name	Optional. Gibt Zeitpläne mit n Namen zurück.
Beschreibung -scd	Beschreibung	Optional. Gibt Zeitpläne mit n Beschreibungen zurück.

RunnableObjects
-ro
	runnableObjects	Optional. Listet die Zeitpläne auf, die ein Objekt ausführen. Geben Sie den Objekttyp und Pfad im Datenintegrationsdienst in folgendem Format ein:
		`'{mapping|workflow}://dis_name/app_name/obj_name'`
		Beispiel:
		`'mapping://dis_demo/app_demo/mapping_demo'`

ScheduleStatus -ss	created|scheduled|paused|completed	Optional. Gibt Zeitpläne mit n Statusangaben zurück.
NumberOfFireTimes -n	number_of_fire_times	Optional. Gibt Zeitpläne zurück, die n Mal ausgeführt wurden.
Maxresults -m	max_results	Optional. Maximale Anzahl an Plänen, die vom Befehl zurückgegeben werden sollen.

ListServiceOptions

Gibt eine Liste mit den Eigenschaften zurück, die für den Scheduler-Dienst konfiguriert sind.

Der infacmd sch ListServiceOptions-Befehl verwendet die folgende Syntax:

```
ListServiceOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sch ListServiceOptions“ beschrieben:

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

Option	Argument	Beschreibung
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

ListServiceProcessOptions

Gibt eine Liste mit den Eigenschaften zurück, die für einen Scheduler-Dienstprozess konfiguriert sind.

Der infacmd sch ListServiceProcessOptions-Befehl verwendet die folgende Syntax:

```
ListServiceProcessOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sch ListServiceProcessOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Geben Sie Scheduler_Service ein.

Option	Argument	Beschreibung
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeName -nn	node_name	Name des Knotens, auf dem der Dienstprozess ausgeführt wird.

PauseAll

Hält alle Zeitpläne an, die vom Scheduler-Dienst verwaltet werden. Wenn Sie die Zeitpläne anhalten, werden bis zu deren Fortsetzung auch die in den Zeitplänen ausgeführten Objekte angehalten.

Der infacmd sch PauseAll-Befehl verwendet die folgende Syntax:

```
PauseAll
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sch PauseAll“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

PauseSchedule

Hält einen Zeitplan an, der vom Scheduler-Dienst verwaltet wird. Wenn Sie einen Zeitplan anhalten, werden bis zu dessen Fortsetzung auch die im Zeitplan ausgeführten Objekte angehalten.

Der infacmd sch PauseSchedule-Befehl verwendet die folgende Syntax:

```
PauseSchedule
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ScheduleName|-scn> schedule_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sch PauseSchedule“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ScheduleName -scn	schedule_name	Name des Zeitplans, der angehalten werden soll. Beim Namen des Zeitplans wird die Groß-/Kleinschreibung beachtet.

ResumeAll

Setzt alle angehaltenen Zeitpläne fort, die vom Scheduler-Dienst verwaltet werden.

Der infacmd sch ResumeAll-Befehl verwendet die folgende Syntax:

```
ResumeAll
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sch ResumeAll“ beschrieben:

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

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

ResumeSchedule

Setzt einen angehaltenen Zeitplan fort, der vom Scheduler-Dienst verwaltet wird.

Der infacmd sch ResumeSchedule-Befehl verwendet die folgende Syntax:

```
ResumeSchedule
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ScheduleName|-scn> schedule_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sch ResumeSchedule“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
ScheduleName -scn	schedule_name	Name des angehaltenen Zeitplans, der fortgesetzt werden soll.

UpdateSchedule

Aktualisiert einen Zeitplan, der vom Scheduler-Dienst verwaltet wird. Aktualisieren Sie einen Zeitplan, um die Start- oder Endzeiten, Wiederholungen oder Objekte zu ändern, die im Zeitplan ausgeführt werden. Führen Sie zum Anzeigen der aktuellen Optionen den infacmd sch ListSchedule-Befehl aus.

Der infacmd sch UpdateSchedule-Befehl verwendet die folgende Syntax:

```
UpdateSchedule
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ScheduleName|-scn> schedule_name
[<-ScheduleDescription|-scd> schedule_description]
<-Recurrence|-r> once|daily|weekly|monthly
<-StartTime|-st> yyyy-MM-dd HH:mm
[<-EndTime|-et> yyyy-MM-dd HH:mm]
[<-TimeZone|-tz> time_zone]
[<-DailyRunEvery|-dre> daily_run_every]
[<-RunDaysOfWeek|-rdw> mon|tue|wed|thu|fri|sat|sun]
[<-RunDayOfWeekMonth|-rdwm> monday|tuesday|wednesday|thursday|friday|saturday|sunday]
[<-RunDayOfMonth|-rdm> 1-30|LAST_DAY_OF_MONTH]
[<-RepeatCount|-rc> repeat_count]
[<-RemoveRunnableObjects|-rro> removeRunnableObjects]
[<-AddRunnableObjects|-aro> addRunnableObjects]
```

Zum Konfigurieren mehrerer Werte für ein Argument trennen Sie die Werte durch Kommas.

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sch UpdateSchedule“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ScheduleName -scn	schedule_name	Erforderlich. Name des Zeitplans. Beim Namen des Zeitplans wird die Groß-/Kleinschreibung beachtet.
-Description -scd	schedule_description	Optional. Beschreibung des Zeitplans.
-Recurrence -r	once|daily|weekly|monthly	Erforderlich. Geben Sie an, ob der Zeitplan einmal oder mehrmals ausgeführt wird.
-StartTime -st	yyyy-MM-dd HH:mm	Erforderlich. Datum und Uhrzeit des Beginns der Wiederholung.
-EndTime -et	yyyy-MM-dd HH:mm	Optional. Datum und Uhrzeit des Endes der Wiederholung.
-TimeZone -tz	Zeitzone	Optional. Zeitzone für den Anfangszeitpunkt des Zeitplans. Zum Konfigurieren der Zeitzone können Sie die ID-Nummer der Zeitzone oder die Olson-Datenbank-ID eingeben. Standardwert ist das Gebietsschema des Client-Computers.
-DailyRunEvery -dre	daily_run_every	Optional. Führen Sie den Zeitplan intervallweise aus. In der folgenden Liste werden die Optionen beschrieben, die Sie konfigurieren können: - Minute(n). Führen Sie den Zeitplan täglich alle n Minuten aus. - Stunde(n). Führen Sie den Zeitplan täglich alle n Stunden aus. - Tag(e). Führen Sie den Zeitplan alle n Tage aus. - Woche(n). Führen Sie den Zeitplan alle n Wochen aus. - Monat(e). Führen Sie den Zeitplan alle n Monate aus. - Jahr(e). Führen Sie den Zeitplan alle n Jahre aus. - ERSTER. Führen Sie den Zeitplan an jedem ersten n-ten Tag des Monats aus. Verwenden Sie die Option -rdwm, um den Wochentag oder die Wochentage anzugeben. - ZWEITER. Führen Sie den Zeitplan an jedem zweiten n-ten Tag des Monats aus. Verwenden Sie die Option -rdwm, um den Wochentag oder die Wochentage anzugeben. - DRITTER. Führen Sie den Zeitplan an jedem dritten n-ten Tag des Monats aus. Verwenden Sie die Option -rdwm, um den Wochentag oder die Wochentage anzugeben. - VIERTER. Führen Sie den Zeitplan an jedem vierten n-ten Tag des Monats aus. Verwenden Sie die Option -rdwm, um den Wochentag oder die Wochentage anzugeben. - LETZTER. Führen Sie den Zeitplan an jedem letzten n-ten Tag des Monats aus. Verwenden Sie die Option -rdwm, um den Wochentag oder die Wochentage anzugeben.

Option	Argument	Beschreibung
-RunDaysOfWeek -rdw	mon|tue|wed|thu|fri|sat|sun	Optional. Führen Sie den Zeitplan an bestimmten Wochentagen aus.
-RunDayOfWeekMonth -rdwm	monday|tuesday| wednesday|thursday|friday| saturday|sunday	Optional. Führen Sie den Zeitplan monatlich an bestimmten Wochentagen aus. Verwenden Sie die Optionen -dre, um den Zeitplan alle ersten, zweiten, dritten, vierten oder letzten n-ten Tage des Monats auszuführen.
-RunDayofMonth -rdm	1-30| LAST_DAY_OF_MONTH	Optional. Führen Sie den Zeitplan an Tag n des Monats aus.
-RepeatCount -rc	repeat_count	Optional. Beenden Sie die Wiederholung nach einer bestimmten Anzahl an Ausführungen statt an einem bestimmten Datum.

RemoveRunnableObjects
-rro
	removeRunnableObjects	Optional. Entfernt Objekte aus dem Zeitplan. Geben Sie Objekte in folgendem Format ein:
		`"{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]]"]`

-AddRunnableObjects
-aro
	addRunnableObjects	Optional. Fügt dem Zeitplan Objekte hinzu. Objekte, die geplant werden sollen. Geben Sie den Objekttyp und dann den Pfad des Objekts im Datenintegrationsdienst an. Beispiel:
		`"mapping:DIS_1234/Application_mapping/ Mapping_abc"`
		Optional können Sie die folgenden Argumente verwenden, um eine Parameterdatei, einen Parametersatz, das Ausführen als Benutzer oder ein Betriebssystemprofil für das Objekt zu konfigurieren:
		- parameterFilePath=PATH_TO_PARAMETER_FILE
		- parameterSet=PARAMETER_SET_NAME
		- runAsUser=USER_NAME &runAsUserSecurityDomain=SECURITY_DOMAIN &runAsUserPassword=PASSWORD
		- osProfileName=OS_PROFILE_NAME
		Beispiel:
		`"workflow:DIS_1234/Application_workflow/ Workflow_abc?parameterFilePath=`
		`C://Informatica/Parameter Files/Parameter.xml`
		`&runAsUser=Administrator`
		`&runAsUserSecurityDomain=Native`
		`&runAsUserPassword=Administrator"`

Eine Liste mit den gültigen Zeitzonenwerten finden Sie unter “Gültige Zeitzonenparameter” auf Seite 869.

UpdateServiceOptions

Aktualisiert die Eigenschaften für den Scheduler-Dienst. Führen Sie zum Anzeigen der aktuellen Optionen den infacmd sch ListServiceOptions-Befehl aus.

Der infacmd sch UpdateServiceOptions-Befehl verwendet die folgende Syntax:

```
UpdateServiceOptions

<-DomainName:-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gatway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-NodeName|-nn> primary node name]

[<-BackupNodes|-bn> node_name1,node_name2,...]

<-Options|-o> options
```

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

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

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-NodeName -nn	Name des primären Knotens	Optional. Primärer Knoten, auf dem der Dienst ausgeführt wird.
-BackupNodes -bn	node_name1,node_name2,...	Optional. Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist.
Optionen -o	options	Optional. Geben Sie jede Option durch ein Leerzeichen getrennt ein.

Optionen des Scheduler-Diensts

Verwenden Sie die Optionen des Scheduler-Diensts mit dem infacmd sch UpdateServiceOptions-Befehl.

Geben Sie die Optionen des Scheduler-Diensts in folgendem Format ein:

```
... -o option_type.option_name=value
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Optionen des Scheduler-Diensts beschrieben:

Option	Beschreibung
SchedulerPersistenceOptions.SchedulerRepositoryServiceName	Der dem Scheduler-Dienst zugeordnete Modellrepository-Dienst.
SchedulerPersistenceOptions.SchedulerRepositoryUsername	Benutzername eines Administrator-Benutzers in der Informatica-Domäne. Nicht verfügbar für eine Domäne mit Kerberos-Authentifizierung.
SchedulerPersistenceOptions.SchedulerRepositoryPassword	Passwort des Administrator-Benutzers in der Informatica-Domäne. Nicht verfügbar für eine Domäne mit Kerberos-Authentifizierung.
SchedulerPersistenceOptions.SchedulerRepositorySecurityDomain	LDAP-Sicherheitsdomäne für den Benutzer, der den Scheduler-Dienst verwaltet. Das Sicherheitsdomänenfeld wird für Benutzer mit nativer oder Kerberos-Authentifizierung nicht angezeigt.
SchedulerLoggingOptions.SchedulerLogLevel	Gibt den Standardschweregrad für die Dienstprotokolle an. Wählen Sie eine der folgenden Optionen aus: - Schwerwiegend. Schreibt FATAL-Meldungen in das Protokoll. Zu FATAL-Meldungen gehören nicht behebbare Systemfehler, die bewirken, dass der Dienst beendet wird oder nicht mehr verfügbar ist. - Fehler: Schreibt FATAL- und ERROR-Codemeldungen in das Protokoll. Zu ERROR-Meldungen gehören Verbindungsfehler, Fehler beim Speichern oder Abrufen von Metadaten, Dienstfehler. - Warnung. Schreibt FATAL-, WARNING- und ERROR-Meldungen in das Protokoll. WARNING-Fehler beinhalten wiederherstellbare Systemfehler oder Warnungen. - Info. Schreibt FATAL-, INFO-, WARNING- und ERROR-Meldungen in das Protokoll. INFO-Meldungen beinhalten System- und Dienständerungsmeldungen. - Trace. Schreibt FATAL-, TRACE-, INFO-, WARNING- und ERROR-Meldungen in das Protokoll. In TRACE-Meldungen werden fehlerhafte Benutzeranfragen protokolliert. - Debug. Schreibt FATAL-, DEBUG-, TRACE-, INFO-, WARNING- und ERROR-Meldungen in das Protokoll. DEBUG-Meldungen sind Benutzeranfrageprotokolle.
SchedulerStorageOptions.SchedulerTempFileLocation	Pfad des Verzeichnisses, aus dem Parameterdateien gelesen und in das Parameterdateien geschrieben werden. Konfigurieren Sie für den Speicherort der temporären Dateien ein Verzeichnis, auf das alle Knoten in der Domäne zugreifen können.

UpdateServiceProcessOptions

Aktualisiert die Eigenschaften für einen Scheduler-Dienstprozess. Führen Sie zum Anzeigen der aktuellen Prozesskonfiguration den infacmd sch ListServiceProcessOptions-Befehl aus.

Der infacmd sch UpdateServiceProcessOptions-Befehl verwendet die folgende Syntax:

```
UpdateServiceProcessOptions

<-DomainName:-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gatway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-NodeName|-nn> node_name]

<-Options|-o> options
```

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

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
NodeName -nn	node_name	Name des Knotens, auf dem der Dienstprozess ausgeführt wird.
Optionen -o	options	Optional. Geben Sie jede Option durch ein Leerzeichen getrennt ein.

Optionen des Scheduler-Dienstprozesses

Verwenden Sie die Optionen des Scheduler-Diensts mit dem infacmd sch UpdateServiceOptions-Befehl.

Geben Sie die Optionen des Scheduler-Diensts in folgendem Format ein:

```
... -o option_type.option_name=value
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Optionen des Scheduler-Diensts beschrieben:

Option	Beschreibung
SchedulerServiceAdvancedOptions.JVMOptions	Java Virtual Machine (JVM)-Befehlszeilenoptionen zum Ausführen von Java-basierten Programmen. Bei der Konfiguration von JVM-Optionen müssen Sie die Eigenschaften für den Java SDK-Klassenpfad, den Java SDK-Minimalspeicher und den Java SDK-Maximalspeicher festlegen. Sie müssen die folgenden JVM-Befehlszeilenoptionen einstellen: - Xms. Minimale Heap-Größe. Standardwert ist 256 m. - MaxPermSize. Maximale permanente Generierungsgröße. Standardwert ist 128 m. - Dfile.encoding. Dateiverschlüsselung. Standardwert ist UTF-8.
HttpConfigurationOptions.KeyStoreFile	Pfad und Dateiname der Schlüsselspeicherdatei, die die Schlüssel und Zertifikate enthält. Erforderlich, wenn Sie HTTPS-Verbindungen für den Dienst verwenden. Sie können eine Schlüsselspeicherdatei mit einem Keytool erstellen. Bei Keytool handelt es sich um ein Dienstprogramm, das private oder öffentliche Schlüsselpaare und zugeordnete Zertifikate in einer Schlüsselspeicherdatei erzeugt und speichert. Sie können das selbstsignierte Zertifikat nutzen oder ein Zertifikat verwenden, das von einer Zertifizierungsstelle signiert wurde.
HttpConfigurationOptions.KeyStorePassword	Passwort für die Schlüsselspeicherdatei.
HttpConfigurationOptions.TrustStoreFile	Pfad und Dateiname der Truststore-Datei, die Authentifizierungszertifikate enthält, die vom Dienst als vertrauenswürdig eingestuft werden.
HttpConfigurationOptions.TrustStorePassword	Passwort für die Schlüsselspeicherdatei.
HttpConfigurationOptions.SSLProtocol	Zu verwendendes Secure Sockets Layer-Protokoll. Standardwert ist TLS.
SchedulerServiceSecurityOptions.HttpPort	Eindeutige HTTP-Portnummer für den Scheduler-Dienstprozess, wenn der Dienst das HTTP-Protokoll verwendet. Standardwert ist 6211.
SchedulerServiceSecurityOptions.HttpsPort	Eindeutige HTTPS-Portnummer für den Scheduler-Dienstprozess, wenn der Dienst das HTTPS-Protokoll verwendet. Wenn Sie eine HTTPS-Portnummer einrichten, müssen Sie auch die Schlüsselspeicherdatei definieren, die die erforderlichen Schlüssel und Zertifikate enthält.

Upgrade

Aktualisiert die Konfiguration des Scheduler-Diensts. Führen Sie „sch Upgrade“ aus, wenn Sie eine Aktualisierung auf die aktuelle Informatica-Version durchführen.

Der infacmd sch Upgrade-Befehl verwendet die folgende Syntax:

```
Upgrade

<-DomainName:-dn> domain_name
```

```
<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gatway_host1:port gateway_host2:port...]

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sch Upgrade“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

KAPITEL 24

infacmd search-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- CreateService, 899
- ListServiceOptions, 902
- ListServiceProcessOptions, 904
- UpdateServiceOptions, 906
- UpdateServiceProcessOptions, 908

CreateService

Erstellt einen Suchdienst. Der Suchdienst wird standardmäßig aktiviert, wenn Sie ihn erstellen.

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

```
CreateService
<-DomainName|-dn> domain_name
<-NodeName|-nn> node_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-FolderPath|-fp> full_folder_path]
[<-BackupNodes|-bn> node_name1,node_name2,...]
<-SearchServicePort|-sp> search_service_port_number
<-IndexLocation|-il> search_index_location
<-ExtractionInterval|-ei> search_extraction_interval
<-RepositoryService|-rsn> model_repository_service_name
<-searchUserName|-sun> username_for_search_repositories
<-searchPassword|-spd> password_for_search_repositories
```

```
[<-searchSecurityDomain|-ssd> security_domain_of_search_repositories]
```

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

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

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Suchdiensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codeseite des verbundenen Repositorys kompatibel sein. Der Name darf nicht länger als 230 Zeichen sein und keine Leerzeichen, Wagenrückläufe, Tabulatoren oder die folgenden Zeichen enthalten: `/ * ? < > " |`
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-FolderPath -fp	full_folder_path	Optional. Vollständiger Pfad ohne den Domänennamen zu dem Ordner, zu dem Sie den Suchdienst hinzufügen möchten. Folgendes Format ist erforderlich: /parent_folder/child_folder Standardwert ist „/“ (die Domäne).
-BackupNodes -bn	node_name1,node_name2,...	Optional. Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist. Sie können Sicherungsknoten konfigurieren, wenn Sie hohe Verfügbarkeit haben.
-SearchServicePort -sp	search_service_port_number	Erforderlich. Port, auf dem der Suchdienst ausgeführt wird.
-IndexLocation -il	search_index_location	Das Verzeichnis, das die Suchindexdateien enthält.
-ExtractionInterval -ei	search_extraction_interval	Intervall in Sekunden, in dem der Suchdienst den Suchdienst aktualisiert.
-RepositoryService -rsn	model_repository_service_name	Modellrepository-Dienst für die Zuordnung zum Suchdienst. Der Modellrepository-Dienst kann keinem anderen Suchdienst zugeordnet werden.
-searchUserName -sun	username_for_search_repositories	Benutzername zum Zugriff auf den Modellrepository-Dienst. Der Modellrepository-Benutzer muss über die Administratorrolle verfügen.

Option	Argument	Beschreibung
-searchPassword -spd	password_for_search_repositories	Benutzerpasswort zum Zugriff auf den Modellrepository-Dienst.
-searchSecurityDomain -ssdn	security_domain_of_search_repositories	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu dem der Modellrepository-Benutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

ListServiceOptions

Listet die Eigenschaften für einen Suchdienst auf.

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

```
ListServiceOptions

<-DomainName|-dn> domain_name

<-NodeName|-nn> node_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd search ListServiceOptions“ beschrieben:

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

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Suchdiensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

ListServiceProcessOptions

Listet die Eigenschaften für einen Suchdienstprozess auf.

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

```
ListServiceProcessOptions

<-DomainName|-dn> domain_name

<-NodeName|-nn> node_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd search ListServiceProcessOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Dienstprozess ausgeführt wird.

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

.

UpdateServiceOptions

Aktualisiert Suchdiensteigenschaften. Führen Sie zum Anzeigen der aktuellen Eigenschaften den infacmd search ListServiceOptions-Befehl aus.

Sie können die Eigenschaften ändern, während der Suchdienst ausgeführt wird. Sie müssen den Dienst jedoch recyceln, damit die Änderungen wirksam werden.

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

```
UpdateServiceOptions

<-DomainName|-dn> domain_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-Options|-o> options]

[<-NodeName|-nn> node name]

[<-BackupNodes|-bn> node_name1,node_name2,...]
```

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

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.

Option	Argument	Beschreibung
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Suchdiensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Options -o	optionen	Optional. Geben Sie jede Option durch ein Leerzeichen getrennt ein. Setzen Sie einen Optionswert in doppelte Anführungszeichen, wenn er ein Leerzeichen enthält. Führen Sie zum Anzeigen der Optionen den infacmd search ListServiceOptions-Befehl aus.
-NodeName -nn	Name des Knotens	Optional. Knoten, auf dem dieser Suchdienst ausgeführt wird.
-BackupNodes -bn	node_name1,node_name2,...	Optional. Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist. Sie können Sicherungsknoten konfigurieren, wenn Sie hohe Verfügbarkeit haben.

UpdateServiceProcessOptions

Aktualisiert Eigenschaften für einen Suchdienstprozess. Führen Sie zum Anzeigen der aktuellen Eigenschaften den infacmd search ListServiceProcessOptions-Befehl aus.

Geben Sie Verbindungsoptionen im folgenden Format ein:

```
... -o option_name=value option_name=value ...
```

Trennen Sie mehrere Optionen mit einem Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

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

```
UpdateServiceProcessOptions

<-DomainName|-dn> domain_name

<-NodeName|-nn> node_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Options|-o> options
```

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

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
NodeName -nn	node_name	Erforderlich. Knoten, auf dem der Suchdienst ausgeführt wird.

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

KAPITEL 25

infacmd sql-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- ExecuteSQL, 910
- ListColumnOptions, 911
- ListColumnPermissions, 913
- ListSQLDataServiceOptions, 915
- ListSQLDataServicePermissions, 917
- ListSQLDataServices, 918
- ListStoredProcedurePermissions, 920
- ListTableOptions, 922
- ListTablePermissions, 924
- PurgeTableCache, 925
- RefreshTableCache , 927
- RenameSQLDataService, 929
- SetColumnPermissions, 931
- SetSQLDataServicePermissions, 933
- SetStoredProcedurePermissions, 936
- SetTablePermissions, 939
- StartSQLDataService, 941
- StopSQLDataService, 943
- UpdateColumnOptions, 945
- UpdateSQLDataServiceOptions, 948
- UpdateTableOptions, 951

ExecuteSQL

Führt SQL-Anweisungen aus, die auf einen SQL-Datendienst zugreifen.

Führen Sie infacmd sql ExecuteSQL im interaktiven oder nicht interaktiven Modus aus. Wenn Sie ExecuteSQL im interaktiven Modus ausführen, können Sie SQL-Anweisungen eingeben, ohne ein Skript zu schreiben. Wenn Sie den interaktiven Modus verwenden, geben Sie den Verbindungsstring ohne die Option -sql ein. Sie können

nachfolgende SQL-Anweisungen ausführen, ohne die Verbindungsinformationen für jede Anweisung einzugeben.

Der Befehl infacmd sql ExecuteSQL verwendet die folgende Syntax:

```
ExecuteSQL

<-ConnectString|-cs> connection_string

[<-Sql> sql_statement]
```

In der folgenden Tabelle werden die infacmd sql ExecuteSQL-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung

-ConnectString
-cs
	connection_string	Erforderlich. Geben Sie einen SQL-Datendienst-Verbindungsstring mit folgender Syntax ein:
		`jdbc:informatica:sqlds/`
		`<optional security domain\>`
		`<optional user name>/`
		`<optional user password>@`
		`<domain host name>:`
		`<domain HTTP port>?dis=`
		`<Data Integration Service name>&sqlds=`
		`<runtime SQL data service name>`
		Optional können Sie Optionen in folgendem Format hinzufügen:
		`... &<option_name>=<option_value>`
		Der Verbindungsstring weist folgende Option und folgenden Wert auf:
		SQLDataServiceOptions.disableResultSetCache=true
		Deaktiviert das Ergebnissatz-Caching für eine SQL-Datendienstabfrage, wenn der SQL-Datendienst für das Caching des Ergebnissatzes konfiguriert ist.

-Sql	sql_statement	Optional. Geben Sie eine SQL-Anweisung ein, wenn der interaktive Modus bei der Ausführung nicht verwendet werden soll.

ListColumnOptions

Listet die Eigenschaften für Spalten in einer virtuellen Tabelle auf.

Der infacmd sql ListColumnOptions-Befehl verwendet die folgende Syntax:

```
ListColumnOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-SQLDataService|-sqlds> sql_data_service
<-Table|-t> schema.table
<-Column|-c> column
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql ListColumnOptions“ beschrieben:

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

Option	Argument	Beschreibung
SQLDataService -sqlds	sql_data_service	Erforderlich. Name des SQL-Datendiensts.
-Table -t	schema.table	Erforderlich. Name der Tabelle. Definieren Sie die Tabelle mit der folgenden Syntax: `<schema_name>.<table_name>`
-Column -c	column	Erforderlich. Name der Spalte.

ListColumnPermissions

Listet Benutzer- und Gruppenberechtigungen für eine virtuelle Spalte auf.

Der Befehl „infacmd sql ListColumnPermissions“ verwendet die folgende Syntax:

```
ListColumnPermissions

<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-SQLDataService|-sqlds> sql_data_service
<-Table|-t> schema.table
<-Column|-c> column
<<-Direct> direct_permission_only|<-Effective> effective_permission_only>
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql ListTablePermissions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.

Option	Argument	Beschreibung
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeitdauer in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
SQLDataService -sqlds	sql_data_service	Erforderlich. Name des SQL-Datendiensts. Sie müssen den Namen des SQL-Datendiensts zu dem Anwendungsnamen als Präfix hinzufügen. Verwenden Sie folgende Syntax: `<application_name>.<SQL_data_service_name>`
-Table -t	schema.table	Erforderlich. Name der Tabelle. Definieren Sie die Tabelle mit der folgenden Syntax: `<schema_name>.<table_name>`

Option	Argument	Beschreibung
-Column -c	column	Erforderlich. Name der zu aktualisierenden Spalte.
-Direct | -Effective>	direct | effective	Erforderlich. Geben Sie entweder direct oder effective ein. Direkte Berechtigungen sind Berechtigungen, die dem Benutzer oder der Gruppe direkt zugewiesen werden. Effektive Berechtigungen umfassen direkte Berechtigungen und geerbte Berechtigungen.

ListSQLDataServiceOptions

Listet die Eigenschaften eines SQL-Datendiensts auf, der in einem Datenintegrationsdienst bereitgestellt wird.

Der Befehl „infacmd sql ListSQLDataServiceOptions“ verwendet die folgende Syntax:

```
ListSQLDataServiceOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-SQLDataService|-sqlds> sql_data_service
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql ListSQLDataServiceOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.

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

ListSQLDataServicePermissions

Listet die Berechtigungen für einen SQL-Datendienst auf.

Der Befehl „infacmd sql ListSQLDataServicePermissions“ verwendet die folgende Syntax:

```
ListSQLDataServicePermissions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-SQLDataService|-sqlds> sql_data_service

<<-Direct> direct_permission_only|<-Effective> effective_permission_only>
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql ListSQLDataServicePermissions“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
SQLDataService -sqlds	sql_data_service	Erforderlich. Name des SQL-Datendiensts. Sie müssen den Namen des SQL-Datendiensts zu dem Anwendungsnamen als Präfix hinzufügen. Verwenden Sie folgende Syntax: `<application_name>.<SQL_data_service_name>`
-Direct | -Effective>	direct | effective	Erforderlich. Ebene der aufzulistenden Berechtigungen. Direkte Berechtigungen sind Berechtigungen, die dem Benutzer oder der Gruppe direkt zugewiesen werden. Effektive Berechtigungen umfassen direkte Berechtigungen und geerbte Berechtigungen.

ListSQLDataServices

Listet die SQL-Datendienste für einen Datenintegrationsdienst auf.

Der Befehl „infacmd sql ListSQLDataServices“ verwendet die folgende Syntax:

```
ListSQLDataServices

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password
```

```
[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql ListSQLDataServices“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Erforderlich. Datenintegrationsdienst, auf dem die Anwendung bereitgestellt wird.

ListStoredProcedurePermissions

Listet die Berechtigungen für eine gespeicherte Prozedur auf.

Der Befehl „infacmd sql ListStoredProcedurePermissions“ verwendet die folgende Syntax:

```
ListStoredProcedurePermissions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-SQLDataService|-sqlds> sql_data_service

<-StoredProcedure|-sp> stored_procedure

<<-Direct> direct_permission_only|<-Effective> effective_permission_only>
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql ListStoredProcedurePermissions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.

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

Option	Argument	Beschreibung
StoredProcedure -sp	stored_procedure	Erforderlich. Name der gespeicherten Prozedur.
-Direct | -Effective>	direct | effective	Erforderlich. Ebene der aufzulistenden Berechtigungen. Direkte Berechtigungen sind Berechtigungen, die dem Benutzer oder der Gruppe direkt zugewiesen werden. Effektive Berechtigungen umfassen direkte Berechtigungen und geerbte Berechtigungen.

ListTableOptions

Listet die Eigenschaften für eine virtuelle Tabelle auf.

Der Befehl „infacmd sql ListTableOptions“ verwendet die folgende Syntax:

```
ListTableOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-SQLDataService|-sqlds> sql_data_service

<-Table|-t> schema.table
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql ListTableOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.

Option	Argument	Beschreibung
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
SQLDataService -sqlds	sql_data_service	Erforderlich. Name des SQL-Datendiensts. Sie müssen den Namen des SQL-Datendiensts zu dem Anwendungsnamen als Präfix hinzufügen. Verwenden Sie folgende Syntax: `<application_name>.<SQL_data_service_name>`
-Table -t	schema.table	Erforderlich. Name der Tabelle. Definieren Sie die Tabelle mit der folgenden Syntax: `<schema_name>.<table_name>`

ListTablePermissions

Listet Gruppen- und Benutzerberechtigungen für eine virtuelle Tabelle auf.

Der Befehl „infacmd sql ListTablePermissions“ verwendet die folgende Syntax:

```
ListTablePermissions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-SQLDataService|-sqlds> sql_data_service

<-Table|-t> schema.table

<<-Direct> direct_permission_only|<-Effective> effective_permission_only>
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql ListTablePermissions“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
SQLDataService -sqlds	sql_data_service	Erforderlich. Name des SQL-Datendiensts. Sie müssen den Namen des SQL-Datendiensts zu dem Anwendungsnamen als Präfix hinzufügen. Verwenden Sie folgende Syntax: `<application_name>.<SQL_data_service_name>`
-Table -t	schema.table	Erforderlich. Name der Tabelle. Definieren Sie die Tabelle mit der folgenden Syntax: `<schema_name>.<table_name>`
-Direct | -Effective>	direct | effective	Erforderlich. Geben Sie entweder direct oder effective ein. Direkte Berechtigungen sind Berechtigungen, die dem Benutzer oder der Gruppe direkt zugewiesen werden. Effektive Berechtigungen umfassen direkte Berechtigungen und geerbte Berechtigungen.

PurgeTableCache

Bereinigt den Cache für virtuelle Tabellen.

Der Befehl „infacmd sql PurgeTableCache“ verwendet die folgende Syntax:

```
PurgeTableCache

<-DomainName|-dn> domain_name

<-UserName|-un> user_name
```

```
<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-SQLDataService|-sqlds> sql_data_service

<-Table|-t> table
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql PurgeTableCache“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.
-SQLDataService -sqlds	sql_data_service	Erforderlich. Name des SQL-Datendiensts. Sie müssen -sqlds als Präfix an den Anwendungsnamen anhängen. Verwenden Sie folgende Syntax: `<application_name>.<SQL_data_service_name>`
-Table -t	table	Erforderlich. Name des zu löschenden Cache für virtuelle Tabellen.

RefreshTableCache

Aktualisiert den Cache eine virtuelle Tabelle.

Der Befehl „infacmd sql RefreshTableCache“ verwendet die folgende Syntax:

```
RefreshTableCache

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-SQLDataService|-sqlds> sql_data_service

<-Table|-t> table
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql RefreshTableCache“ beschrieben:

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

Option	Argument	Beschreibung
-SQLDataService -sqlds	sql_data_service	Erforderlich. Name des SQL-Datendiensts. Sie müssen -sqlds als Präfix an den Anwendungsnamen anhängen. Verwenden Sie folgende Syntax: `<application_name>.<SQL_data_service_name>`
-Table -t	table	Erforderlich. Name des zu aktualisierenden Cache für virtuelle Tabellen.

RenameSQLDataService

Benennt einen SQL-Datendienst um, der in einem Datenintegrationsdienst bereitgestellt wird.

Der Befehl „infacmd sql RenameSQLDataService“ verwendet die folgende Syntax:

```
RenameSQLDataService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-SQLDataService|-sqlds> sql_data_service

<-NewName|-n> new_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql RenameSQLDataService“ beschrieben:

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

Option	Argument	Beschreibung
-SQLDataService -sqlds	sql_data_service	Erforderlich. Name des umzubenennenden SQL-Datendiensts. Sie müssen den Namen des SQL-Datendiensts zu dem Anwendungsnamen als Präfix hinzufügen. Verwenden Sie folgende Syntax: `<application_name>.<SQL_data_service_name>`
NewName -n	new_name	Erforderlich. Neuer Name für den SQL-Datendienst.

SetColumnPermissions

Verweigert einer Gruppe oder einem Benutzer den Zugriff auf eine Spalte in einer SQL-Abfrage.

Der Befehl „infacmd sql SetColumnPermissions“ verwendet die folgende Syntax:

```
SetColumnPermissions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-SQLDataService|-sqlds> sql_data_service

<-Table|-t> schema.table

<-Column|-c> column_name

<<-GranteeUserName|-gun> grantee_user_name|<-GranteeGroupName|-ggn> grantee_group_name>

[<-GranteeSecurityDomain|-gsdn> grantee_security_domain]

<-DeniedPermissions|-dp> denied_permissions
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql SetColumnPermissions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.

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

Option	Argument	Beschreibung
-Table -t	schema.table	Erforderlich. Name der virtuellen Tabelle. Geben Sie die Tabelle in folgendem Format ein: `<schema_name>.<table_name>`
-Column -c	column	Name der zu aktualisierenden Spalte.
-GranteeUserName|GranteeGroupName -gun|-ggn	grantee_user_name| grantee_group_name	Erforderlich. Benutzername bzw. Gruppenname, für den Berechtigungen festgelegt oder verweigert werden sollen.
-GranteeSecurityDomain -gsdn	grantee_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden und Benutzerberechtigungen gewähren. Name der Sicherheitsdomäne, zu der der Benutzer gehört.
-DeniedPermissions -dp	denied_permissions	Erforderlich. Geben Sie „SQL_Select“ ein, um einen Benutzer daran zu hindern, die Spalte in eine SELECT-Anweisung aufzunehmen.

SetSQLDataServicePermissions

Richtet die Gruppen- oder Benutzerberechtigungen für einen SQL-Datendienst ein. Sie können Berechtigungen auch verweigern.

Der Befehl „infacmd sql SetSQLDataServicePermissions“ verwendet die folgende Syntax:

```
SetSQLDataServicePermissions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-SQLDataService|-sqlds> sql_data_service

<<-GranteeUserName|-gun> grantee_user_name|<-GranteeGroupName|-ggn> grantee_group_name>

[<-GranteeSecurityDomain|-gsdn> grantee_security_domain]

<-AllowedPermissions|-ap> allowed_permissions

<-DeniedPermissions|-dp> denied_permissions
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql SetSQLDataServicePermissions“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der *infacmd* versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-SQLDataService -sqlds	sql_data_service	Erforderlich. Name des SQL-Datendiensts. Sie müssen den Namen des SQL-Datendiensts zu dem Anwendungsnamen als Präfix hinzufügen. Verwenden Sie folgende Syntax: `<application_name>.<SQL_data_service_name>`
-GranteeUserName| GranteeGroupName -gun|-ggn	grantee_user_name| grantee_group_name	Erforderlich. Benutzername bzw. Gruppenname, für den Berechtigungen festgelegt oder verweigert werden sollen.
-GranteeSecurityDomain -gsdn	grantee_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden und Benutzerberechtigungen gewähren. Name der Sicherheitsdomäne, zu der der Benutzer gehört.
-AllowedPermissions -ap	allowed_permissions	Erforderlich. Liste der durch Leerzeichen getrennten Berechtigungen. Geben Sie eine der folgenden Berechtigungen ein: - Grant. Benutzer können mithilfe des Administrator Tools oder des infacmd-Befehlszeilenprogramms Berechtigungen für den SQL-Datendienst gewähren oder widerrufen. - Execute. Benutzer können alle virtuellen gespeicherten Prozeduren im SQL-Datendienst mithilfe eines JDBC- oder ODBC-Client-Tools ausführen. - SQL_Select. Benutzer können SQL SELECT-Anweisungen in virtuellen Tabellen im SQL-Datendienst mithilfe eines JDBC- oder ODBC-Client-Tools ausführen.
-DeniedPermissions -dp	denied_permissions	Optional. Liste der Berechtigungen, die Benutzern verweigert werden sollen. Trennen Sie jeden Parameter durch ein Leerzeichen. Geben Sie eine der folgenden Berechtigungen ein: - EXECUTE. Benutzer können virtuell gespeicherte Prozeduren im SQL-Datendienst nicht ausführen. - SQL_SELECT. Benutzer können keine SELECT-Anweisungen in beliebigen Tabellen im SQL-Datendienst ausführen.

SetStoredProcedurePermissions

Richtet Benutzer- und Gruppenberechtigungen für eine gespeicherte Prozedur ein. Sie können Berechtigungen auch verweigern.

Der Befehl „infacmd sql SetStoredProcedurePermissions“ verwendet die folgende Syntax:

```
SetStoredProcedurePermissions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-SQLDataService|-sqlds> sql_data_service

<-StoredProcedure|-sp> stored_procedure

<<-GranteeUserName|-gun> grantee_user_name|<-GranteeGroupName|-ggn> grantee_group_name>

[<-GranteeSecurityDomain|-gsdn> grantee_security_domain]

<-AllowedPermissions|-ap> allowed_permissions

<-DeniedPermissions|-dp> denied_permissions
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql SetStoredProcedurePermissions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-SQLDataService -sqlds	sql_data_service	Erforderlich. Name des SQL-Datendiensts mit der gespeicherten Prozedur. Sie müssen den Namen des SQL-Datendiensts zu dem Anwendungsnamen als Präfix hinzufügen. Verwenden Sie folgende Syntax: `<application_name>.<SQL_data_service_name>`
-StoredProcedure -sp	stored_procedure	Erforderlich. Name der gespeicherten Prozedur.
-GranteeUserName|GranteeGroupName -gun|-ggn	grantee_user_name| grantee_group_name	Erforderlich. Benutzername bzw. Gruppenname, für den Berechtigungen festgelegt oder verweigert werden sollen.
-GranteeSecurityDomain -gsdn	grantee_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden und Benutzerberechtigungen gewähren. Name der Sicherheitsdomäne, zu der der Benutzer gehört.
-AllowedPermissions -ap	list_of_allowed_permissions_separated_by_space	Erforderlich. Liste der zulässigen Berechtigungen. Geben Sie einen der folgenden Parameter durch Leerzeichen getrennt ein: - Grant. Benutzer können mithilfe des Administrator Tools oder des infacmd-Befehlszeilenprogramms Berechtigungen für die gespeicherten Prozedurobjekte gewähren oder widerrufen. - Execute. Benutzer können virtuelle gespeicherte Prozeduren im SQL-Datendienst mithilfe eines JDBC- oder ODBC-Client-Tools ausführen.
-DeniedPermissions -dp	denied_permissions	Optional. Liste der Berechtigungen, die Benutzern verweigert werden sollen. Geben Sie einen der folgenden Parameter durch Leerzeichen getrennt ein: - GRANT. Benutzer können Berechtigungen für die Objekte der gespeicherten Prozedur weder gewähren noch entziehen. - EXECUTE. Benutzer können keine gespeicherte Prozedur im SQL-Datendienst ausführen.

SetTablePermissions

Richtet Gruppen- und Benutzerberechtigungen für eine virtuelle Tabelle ein.

Der Befehl „infacmd sql SetTablePermissions“ verwendet die folgende Syntax:

```
SetTablePermissions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-SQLDataService|-sqlds> sql_data_service

<-Table|-t> schema.table

<<-GranteeUserName|-gun> grantee_user_name|<-GranteeGroupName|-ggn> grantee_group_name>

[<-GranteeSecurityDomain|-gsdn> grantee_security_domain]

<-AllowedPermissions|-ap> allowed_permissions

<-DeniedPermissions|-dp> denied_permissions

[<-RLSPredicate|-rls> row_level_security_predicate]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql SetTablePermissions“ beschrieben:

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

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-SQLDataService -sqlds	sql_data_service	Erforderlich. Name des SQL-Datendiensts mit der virtuellen Tabelle. Sie müssen den Namen des SQL-Datendiensts zu dem Anwendungsnamen als Präfix hinzufügen. Verwenden Sie folgende Syntax: `<application_name>.<SQL_data_service_name>`
-Table -t	schema.table	Erforderlich. Name der virtuellen Tabelle. Geben Sie die Tabelle in folgendem Format ein: `<schema_name>.<table_name>`
-GranteeUserName| GranteeGroupName -gun|-ggn	grantee_user_name| grantee_group_name	Erforderlich. Benutzername bzw. Gruppenname, für den Berechtigungen festgelegt oder verweigert werden sollen.

Option	Argument	Beschreibung
-GranteeSecurityDomain -gsdn	grantee_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden und Benutzerberechtigungen gewähren. Name der Sicherheitsdomäne, zu der der Benutzer gehört.
-AllowedPermissions -ap	list_of_allowed_permissions	Erforderlich. Liste der zulässigen Berechtigungen. Geben Sie einen der folgenden Parameter durch Leerzeichen getrennt ein: - Grant. Benutzer können mithilfe des Administrator Tools oder des infacmd-Befehlszeilenprogramms Berechtigungen für die gespeicherten Prozedurobjekte gewähren oder widerrufen. - SQL_Select. Benutzer können SQL-Abfragen anhand der Tabelle durchführen.
-DeniedPermissions -dp	denied_permissions	Optional. Liste der Berechtigungen, die Benutzern verweigert werden sollen. Geben Sie einen der folgenden Parameter durch Leerzeichen getrennt ein: - GRANT. Benutzer können Berechtigungen für die Tabelle weder gewähren noch entziehen. - SQL_SELECT. Benutzer können keine SQL-Abfragen anhand der Tabelle durchführen.
-RLSPredicate -rls	row_level_security_predicate	Optional. Listet das Sicherheitsprädikat auf Zeilenebene zum Anwenden auf SELECT-Anweisungen auf.

StartSQLDataService

Startet einen SQL-Datendienst.

Der Befehl „infacmd sql StartSQLDataService“ verwendet die folgende Syntax:

```
StartSQLDataServiceOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-SQLDataService|-sqlds> sql_data_service
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql StartSQLDataService“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-SQLDataService -sqlds	sql_data_service	Erforderlich. Name des SQL-Datendiensts. Sie müssen den Namen des SQL-Datendiensts zu dem Anwendungsnamen als Präfix hinzufügen. Verwenden Sie folgende Syntax: `<application_name>.<SQL_data_service_name>`

StopSQLDataService

Hält die Ausführung eines SQL-Datendiensts an.

Der Befehl „infacmd sql StopSQLDataService“ verwendet die folgende Syntax:

```
StopSQLDataService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-SQLDataService|-sqlds> sql_data_service
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql StopSQLDataService“ beschrieben:

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

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem der SQL-Datendienst bereitgestellt wird.
-SQLDataService -sqlds	sql_data_service	Erforderlich. Name des anzuhaltenden SQL-Datendiensts. Sie müssen den Namen des SQL-Datendiensts zu dem Anwendungsnamen als Präfix hinzufügen. Verwenden Sie folgende Syntax: `<application_name>.<SQL_data_service_name>`

UpdateColumnOptions

Legt die Spaltenoptionen fest, um zu bestimmen, was beim Auswählen einer eingeschränkten Spalte in einer Abfrage geschieht. Sie können den Wert mit NULL oder mit einem konstanten Wert ersetzen.

Der Befehl „infacmd sql UpdateColumnOptions“ verwendet die folgende Syntax:

```
UpdateColumnOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-SQLDataService|-sqlds> sql_data_service

<-Table|-t> schema.table

<-Column|-c> column_name

<-Options|-o> options
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql UpdateColumnOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem die Anwendung bereitgestellt wird.

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

Option	Argument	Beschreibung
-Table -t	schema.table	Erforderlich. Name der virtuellen Tabelle. Geben Sie die Tabelle in folgendem Format ein: `<schema_name>.<table_name>`
-Column -c	column	Spaltenname.
-Options -o	options	Erforderlich. Geben Sie jede Option durch ein Leerzeichen getrennt ein. Führen Sie zum Anzeigen der aktuellen Optionen den infacmd sql ListColumnOptions-Befehl aus.

Spaltenoptionen

Verwenden Sie Spaltenoptionen zum Aktualisieren einer Spalte. Verwenden Sie die Spaltenoptionen mit dem Befehl infacmd sql UpdateColumnOptions.

Geben Sie die Spaltenoptionen in folgendem Format ein:

```
... -o UpdateColumnOptions.option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden Spaltenoptionen beschrieben:

Optionen	Beschreibung
ColumnOptions.DenyWith	Wenn Sie Sicherheit auf Spaltenebene verwenden, bestimmt diese Eigenschaft, ob die Abfrage fehlschlagen oder der Wert der eingeschränkten Spalte ersetzt werden soll. Sie können den Spaltenwert durch NULL oder einen konstanten Wert ersetzen. Wählen Sie eine der folgenden Optionen aus: - ERROR. Lässt die Abfrage fehlschlagen und gibt einen Fehler zurück. - NULL. Gibt Nullwerte für eine eingeschränkte Spalte in jeder Zeile zurück. - VALUE. Gibt einen konstanten Wert anstelle der eingeschränkten Spalte in jeder Zeile zurück. Konfigurieren Sie den konstanten Wert in der Option InsufficientPermissionValue.
ColumnOptions.InsuffiicientPermissionValue	Ersetzt den Wert der eingeschränkten Spalte durch einen konstanten Wert. Der Standardwert ist ein leerer String. Wenn Sie ColumnOptions.DenyWith nicht konfigurieren, ignoriert der Data Integration Service die Option InsufficientPermissionValue.

UpdateSQLDataServiceOptions

Aktualisiert SQL-Datendienst-Eigenschaften. Sie müssen vor dem Aktualisieren der Eigenschaften den SQL-Datendienst beenden.

Der Befehl „infacmd sql UpdateSQLDataServiceOptions“ verwendet die folgende Syntax:

```
UpdateSQLDataServiceOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-SQLDataService|-sqlds> sql_data_service

<-Options|-o> options
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql UpdateSQLDataServiceOptions“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-SQLDataService -sqlds	sql_data_service	Erforderlich. Name des SQL-Datendiensts. Sie müssen den Namen des SQL-Datendiensts zu dem Anwendungsnamen als Präfix hinzufügen. Verwenden Sie folgende Syntax: `<application_name>.<SQL_data_service_name>`
options -o	options	Erforderlich. Liste der zu aktualisierenden Optionen. Geben Sie Optionen und Werte durch Leerzeichen getrennt ein. Führen Sie zum Anzeigen der Optionen für einen SQL-Datendienst infacmd sql ListSQLDataServiceOptions aus.

SQL-Datendienst-Optionen

Verwenden Sie SQL-Datendienst-Optionen zum Aktualisieren eines SQL-Datendienstes. Verwenden Sie SQL-Datendienst-Optionen mit dem Befehl infacmd sql UpdateSQLDataServiceOptions.

Geben Sie SQL-Datendienst-Optionen in folgendem Format ein:

```
... -o SQLDataServiceOptions.option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden Verbindungsoptionen für infacmd sql UpdateSQLDataServiceOptions beschrieben:

Option	Beschreibung
SQLDataServiceOptions.startupType	Legt fest, ob der SQL-Datendienst beim Starten der Anwendung oder des SQL-Datendienstes zur Ausführung aktiviert ist. Geben Sie ENABLED ein, damit der SQL-Datendienst ausgeführt wird. Geben Sie DISABLED ein, damit der SQL-Datendienst nicht ausgeführt wird.
SQLDataServiceOptions.traceLevel	Ebene der in das Sitzungsprotokoll geschriebenen Fehlermeldungen. Geben Sie eine der folgenden Meldungsebenen an: - Schwerwiegend - Fehler - Info - Trace - Debug
SQLDataServiceOptions.connectionTimeout	Maximale Anzahl an Millisekunden, in denen auf eine Verbindung zum SQL-Datendienst gewartet wird. Standardwert ist 3.600.000.
SQLDataServiceOptions.requestTimeout	Maximale Anzahl an Millisekunden, in denen bei einer SQL-Anfrage auf eine Antwort vom SQL-Datendienst gewartet wird. Standardwert ist 3.600.000.
SQLDataServiceOptions.sortOrder	Sortierreihenfolge, die der Data Integration Service zum Sortieren und Vergleichen von Daten verwendet, wenn er im Unicode-Modus ausgeführt wird. Sie können die Sortierreihenfolge basierend auf Ihrer Codeseite auswählen. Wenn der Data Integration Service im ASCII-Modus ausgeführt wird, ignoriert er den Sortierreihenfolgenwert und verwendet eine binäre Sortierreihenfolge. Die Standardeinstellung ist "binär".
SQLDataServiceOptions.maxActiveConnections	Maximale Anzahl an aktiven Verbindungen zum SQL-Datendienst. Standardwert ist 10.
SQLDataServiceOptions.ResultSetCacheExpirationPeriod	Die Anzahl an Millisekunden, die der Ergebnissatz-Cache verwendet werden kann. Wenn der Wert auf -1 festgelegt ist, läuft der Cache nie ab. Wenn der Wert auf 0 festgelegt ist, ist das Ergebnissatz-Caching deaktiviert. Änderungen des Ablaufzeitraums gelten nicht für vorhandene Caches. Wenn alle Caches denselben Ablaufzeitraum verwenden sollen, bereinigen Sie den Ergebnissatz-Cache, nachdem Sie den Ablaufzeitraum geändert haben. Standardwert ist 0.

Option	Beschreibung
SQLDataServiceOptions.DTMKeepAliveTime	Anzahl der Millisekunden, für die die DTM-Instanz geöffnet bleibt, nachdem sie die letzte Anfrage abgeschlossen hat. Identische SQL-Abfragen können die offene Instanz wiederverwenden. Verwenden Sie die Keep Alive-Zeit, um die Leistung zu erhöhen, wenn die für die Verarbeitung der SQL-Abfrage erforderliche Zeit im Vergleich zur Dauer der Initialisierung der DTM-Instanz gering ist. Wenn die Abfrage fehlschlägt, wird die DTM-Instanz beendet. Muss eine Ganzzahl sein. Eine negative Ganzzahl bedeutet, dass die DTM-Keep Alive-Zeit für den Data Integration Service verwendet wird. 0 bedeutet, dass der Data Integration Service die DTM-Instanz nicht im Speicher beibehält. Standardwert ist -1.
SQLDataServiceOptions.optimizeLevel	Die Optimierungsebene, die der Data Integration Service für das Objekt anwendet. Geben Sie den numerischen Wert ein, der mit der Optimierungsebene verbunden ist, die Sie konfigurieren möchten. Sie können Sie einen der folgenden numerischen Werte eingeben: - 0. Der Datenintegrationsdienst wendet keine Optimierung an. - 1. Der Datenintegrationsdienst wendet die frühe Projektionsoptimierungsmethode an. - 2. Der Datenintegrationsdienst wendet die Optimierungsmethoden „Frühe Projektion“, „Frühe Auswahl“, „Push-Into“ und „Prädikat“ an. - 3. Der Datenintegrationsdienst wendet die Optimierungsmethoden „Kostenbasiert“, „Frühe Projektion“, „Frühe Auswahl“, „Push-Into“, „Prädikat“ und „Semi-Join“ an.

UpdateTableOptions

Aktualisiert die virtuellen Tabelleneigenschaften. Sie müssen vor dem Aktualisieren der Eigenschaften den SQL-Datendienst beenden.

Der Befehl „infacmd sql UpdateTableOptions“ verwendet die folgende Syntax:

```
UpdateTableOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-SQLDataService|-sqlds> sql_data_service

<-Table|-t> schema.table

<-Options|-o> options
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd sql UpdateTableOptions“ beschrieben:

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

Option	Argument	Beschreibung
SQLDataService -sqlds	sql_data_service	Erforderlich. Name des SQL-Datendiensts. Sie müssen den Namen des SQL-Datendiensts zu dem Anwendungsnamen als Präfix hinzufügen. Verwenden Sie folgende Syntax: `<application_name>.<SQL_data_service_name>`
-Table -t	schema.table	Erforderlich. Name der Tabelle. Verwenden Sie folgende Syntax: `<schema_name>.<table_name>`
Options -o	options	Erforderlich. Geben Sie das Name-Wert-Paar durch Leerzeichen getrennt ein.

Virtuelle Tabellenoptionen

Verwenden Sie die virtuellen Tabellenoptionen, um das Zwischenspeichern für eine virtuelle Tabelle zu konfigurieren. Verwenden Sie die virtuellen Tabellenoptionen mit dem infacmd sql UpdateTableOptions-Befehl.

Geben Sie virtuelle Tabellenoptionen im folgenden Format ein:

```
... -o option_type.option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

Die folgende Tabelle beschreibt die virtuellen Tabellenoptionen:

Option	Beschreibung
VirtualTableOptions.CachingEnabled	Zwischenspeichern der virtuellen Tabelle in der Cache-Datenbank des Datenobjekts. „True“ oder „False“. Standardwert ist „True“.
VirtualTableOptions.CacheRefreshPeriod	Anzahl der Minuten zwischen den Cache-Aktualisierungen. Standardwert ist Null.
VirtualTableOptions.CacheTableName	Der Name der benutzerverwalteten Tabelle, aus der der Datenintegrationsdienst auf den Cache der virtuellen Tabelle zugreift. Eine benutzerverwaltete Cache-Tabelle ist eine Tabelle in der Cache-Datenbank des Datenobjekts, die Sie bei Bedarf erstellen, füllen und manuell aktualisieren können. Wenn Sie einen Cache-Tabellennamen angeben, verwaltet der Datenobjekt-Cache-Manager den Cache für das Objekt nicht und ignoriert den Cache-Aktualisierungszeitraum. Wenn Sie keinen Cache-Tabellennamen angeben, verwaltet der Datenobjekt-Cache-Manager den Cache für das Objekt.

KAPITEL 26

infacmd tdm-Befehlsreferenz

Das „infacmd tdm“-Programm verwaltet den Test Data Manager-Dienst. Mit den „infacmd tdm“-Befehlen können Sie den Dienst erstellen, Inhalte zum Dienst hinzufügen und den Dienst aktivieren bzw. deaktivieren.

Dieses Kapitel umfasst die Befehle, die Sie mit dem „infacmd tdm“-Programm verwenden können. Führen Sie die Befehle im Pfad <INFA_HOME\isp\bin aus.

Hinweis: Bei der Ausführung der Befehle im Kerberos-Authentifizierungsmodus müssen Sie die Optionen für den Benutzernamen und das Passwort nicht hinzufügen.

CreateService

Erstellt einen Test Data Manager-Dienst in einer Domäne.

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

```
CreateService

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name

<-LicenseName|-ln> license_name

<-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
```

```
<-EnableTDWService|-ets> enable_tdwservice

<-DISServiceName|-dis> data_integration_service

<-db_type|-dt> database_type (ORACLE, DB2, SQLSERVER or CUSTOM)

[<-customDriver|-cd> custom_driver_name]

<-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]

[<-httpProtocolType|-pt> http_protocol_type]

[<-jvmParams|-jp> jvmParameters]

[<-connPoolSize|-cp> conn_pool_size]

[<-jmxPort> jmx_port]

[<-shutdownPort> shutdown_port]
```

In der folgenden Tabelle werden „infacmd tdm CreateService"" beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Test Data Manager-Diensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichen müssen mit der Codepage des zugehörigen Repositorys kompatibel sein. Der Name darf maximal 230 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten: `/ * ? < > " |`

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

Option	Argument	Beschreibung
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Dienst ausgeführt wird.
-LicenseName -ln	license_name	Erforderlich. Name der Lizenz. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf maximal 79 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten: / * ? < > " |
-PCRSServicename -pcrs	power_center_repo_service	Name des PowerCenter-Repository-Diensts, mit dem sich TDM verbindet.
-PCISServicename -pcis	power_center_int_service	Name des PowerCenter-Integrationsdiensts, mit dem sich TDM verbindet.
-MRSServiceName -mrs	model_repo_service	Name des Modellrepository-Diensts, mit dem sich TDM verbindet.
-MRSUserName -rsun	model_repo_service_username	Erforderlich. Benutzername für die Verbindung zum Modellrepository.
-MRSPassword -rspd	model_repo_service_password	Erforderlich. Passwort für den Benutzernamen zur Verbindung mit dem Modellrepository. Beim Passwort wird die Groß-/Kleinschreibung beachtet.
-AnalystService -at	analyst_service	Optional. Der Name des Analyst-Diensts, der von TDM zur Objektverknüpfung verwendet wird. Erforderlich, wenn Sie die Asset-Linking-Funktion verwenden, um globale TDM-Objekte mit den Business Glossary-Objekten zu verknüpfen.
-MRSSecurityDomain -rsdn	model_repo_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Der Name der Sicherheitsdomäne, zu der der Benutzer gehört. Bei der Sicherheitsdomäne wird die Groß-/Kleinschreibung beachtet. Standardwert ist „Native“.
-EnableProfiling -ep	enable_profiling	Gibt Einstellungen für die Datenerkennung an. Auf TRUE festlegen, um die Datenerkennung zu aktivieren. Auf FALSE festlegen, um die Datenerkennung zu deaktivieren.
-EnableTDWService -ets	enable_tdwservice	Gibt Test Data Warehouse-Einstellungen an. Legen Sie diesen Wert auf „True“ fest, um ein Testdaten-Repository und einen Testdaten-Mart zu konfigurieren. Wenn dieser Wert auf „False“ festgelegt ist, müssen Sie kein Test Data Warehouse erstellen. Standardwert ist FALSE.

Option	Argument	Beschreibung
-DISServiceName -dis	data_integration_service	Name des Datenintegrationsdiensts, mit dem sich TDM verbindet.
-db_type -dt	database_type	Typ der TDM-Repository-Datenbank. Werte sind „Oracle“, „SQL Server“, „DB2“ oder „Benutzerdefiniert“.
-customDriver -cd	custom_driver_name	Benutzerdefinierte JDBC-Treiberparameter. Erforderlich, wenn Sie einen benutzerdefinierten Datenbanktyp verwenden möchten.
-DBUsername -du	db_user	Erforderlich. Konto für die Repository-Datenbank. Verwenden Sie den Datenbank-Client, um dieses Konto einzurichten.
-DBPassword -dp	db_password	Erforderlich. Passwort der Repository-Datenbank für den Datenbankbenutzer.

-DBUrl
-dl
	db_url	Erforderlich. JDBC-Verbindungszeichenfolge zur Datenbank für das TDM-Repository. Verwenden Sie eine der folgenden Syntaxen:
		Oracle:
		`jdbc:informatica:oracle: //<machineName>:<PortNo>;ServiceName=<DBName>; MaxPooledStatements=20; CatalogOptions=0; EnableServerResultCache=true`
		DB2:
		`jdbc:informatica:db2: //<host>:<port>; DatabaseName=<dbname>; BatchPerformanceWorkaround=true;DynamicSections=1000`
		SQLServer:
		`jdbc:informatica:sqlserver: //<host>:<port>; DatabaseName=<dbname>; SnapshotSerializable=true`

-DBConnString -dc	db_conn_string	Native Verbindungszeichenfolge für die TDM-Repository-Datenbank. Der Dienst verwendet die Verbindungszeichenfolge, um ein Verbindungsobjekt für das Test Data Manager- und PowerCenter-Repository zu erstellen.
-DbSchema -ds	db_schema	Optional. Der Schemaname für eine Microsoft SQL Server-Datenbank.

Option	Argument	Beschreibung
-DbTablespace -db	db_tablespace	Nur für eine DB2-Datenbank erforderlich. Beim Konfigurieren eines Tablespace-Namens erstellt der Test Data Manager-Dienst alle Repository-Tabellen im selben Tablespace. Sie können im Tablespace-Namen keine Leerzeichen verwenden. Der Tablespace muss auf einem Einzelknoten definiert werden und die Seitengröße muss 32 KB betragen. In einer Datenbank mit mehreren Partitionen müssen Sie diese Option auswählen. Wenn Sie in einer Datenbank mit einer Partition diese Option nicht auswählen, erstellt das Installationsprogramm die Tabellen im Standard-Tablespace.
-HttpPort	http_port	Erforderlich. Portnummer des Diensts.
-HttpsPort	https_port	Optional. Portnummer zum Sichern der Verbindung zum Administrator-Tool. Geben Sie diese Portnummer an, wenn Sie HTTPS für einen Knoten konfigurieren möchten.
-KeystoreFile -kf	keystore_file_location]	Optional. Schlüsselspeicherdatei, in der die Schlüssel und Zertifikate enthalten sind, die bei Verwendung des SSL-Protokolls mit PowerCenter erforderlich sind.
-KeystorePassword -kp	keystore_password	Optional. Wenn TLS aktiviert ist, müssen Sie ein Passwort festlegen.
-httpProtocolType -pt	http_protocol_type	Sicherheitsprotokoll, das vom Dienst verwendet wird. Geben Sie einen der folgenden Werte ein: - HTTP. In Anfragen an den Dienst muss eine HTTP-URL verwendet werden. - HTTPS. In Anfragen an den Dienst muss eine HTTPS-URL verwendet werden. - Beide. In Anfragen an den Dienst kann entweder eine HTTP- oder eine HTTPS-URL verwendet werden. Wenn Sie den HTTP-Protokolltyp auf „HTTPS“ oder „Beide“ einstellen, aktivieren Sie TLS (Transport Layer Security) für den Dienst. Sie können TLS auch für jeden Webdienst aktivieren, der für eine Anwendung bereitgestellt wurde. Wenn Sie HTTPS für den Dienst und TLS für den Webdienst aktivieren, verwendet der Webdienst eine HTTPS-URL. Wenn Sie HTTPS für den Dienst, TLS aber nicht für den Webdienst aktivieren, kann der Webdienst eine HTTP-URL oder eine HTTPS-URL verwenden. Wenn Sie TLS für einen Webdienst, HTTPS aber nicht für den Dienst aktivieren, startet der Webdienst nicht. Der Standardwert ist HTTP.

Option	Argument	Beschreibung
-jvmParams -jp	jvmParameters	Festzulegende JVM-Parameter: - Die Test Data Manager zugeordnete Heap-Größe. - Der Zeitraum, nach dessen Ablauf Datenbankverbindungen erneuert werden, wenn sich die TDM-Benutzeroberfläche weiterhin im Leerlauf befindet. Erforderlich, wenn Sie die Konfigurationseinstellungen der Datenbank in niedrigere Werte als die TDM-Standardwerte geändert haben. Bearbeiten Sie die Werte in TDM so, dass die Werte niedriger als die Datenbankwerte sind. Schließen Sie die JVM-Parameter in einfache Anführungszeichen und anschließend in doppelte Anführungszeichen ein. Beispiel: 'value' und dann "'value'". Die Option -Xms unterscheidet zwischen Groß- und Kleinschreibung. Beispiel: "'- **X**ms512m - **X**mx1024m - **XX**:MaxPermSize=512m'" - IDLE_TIME. `-DIDLE_TIME=<seconds>`. Standardwert ist 300 Sekunden. - CONNECT_TIME. `-DCONNECT_TIME=<seconds>`. Standardwert ist 5000 Sekunden.
-connPoolSize -cp	conn_pool_size	Optional. Die maximale Anzahl inaktiver Verbindungsinstanzen, die ein Pool für eine Datenbankverbindung aufrechterhält, bevor die maximale inaktive Zeit erreicht ist. Legen Sie diesen Wert auf eine höhere Anzahl als die Mindestanzahl an inaktiven Verbindungsinstanzen fest. Standardwert ist 15.
-jmxPort	jmx_port	Portnummer für die JMX/RMI-Verbindungen mit TDM. Standardwert ist 6675.
-shutdownPort	shutdown_port	Portnummer, die das Herunterfahren von TDM steuert.

CreateContents

Erstellt den Repository-Inhalt für das Test Data Manager-Repository.

Der Befehl „infacmd tdm CreateContents“ verwendet die folgende Syntax:

```
<-DomainName|-dn> domain_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name
```

```
<-Password|-pd> password

<-ServiceName|-sn> service_name

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd tdm CreateContents““ beschrieben:

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

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Der Name des Test Data Manager-Diensts.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

EnableService

Aktiviert den Test Data Manager-Dienst.

Der Befehl „infacmd tdm EnableService“ verwendet die folgende Syntax:

```
<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd idm EnableService““ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Diensts, zu dem Sie den Befehl ausführen möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.

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

DisableService

Deaktiviert den Test Data Manager-Dienst. Wenn Sie den Test Data Manager-Dienst deaktivieren, werden alle Dienstprozesse angehalten.

Der Befehl „infacmd tdm DisableService“ verwendet die folgende Syntax:

```
<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name
```

```
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-DisableMode|-dm> disable_mode: COMPLETE|ABORT|STOP
```

In der folgenden Tabelle werden „infacmd tdm DisableService"" beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-DisableMode -dm	disable_mode	Erforderlich. Definiert, wie der Dienst deaktiviert wird: - Vollständig. Deaktiviert den Dienst, nachdem alle Dienstprozesse gestoppt sind. - Abbrechen. Stoppt alle Prozesse sofort und deaktiviert dann den Dienst. - Stoppen. Stoppt alle laufenden Arbeitsabläufe und deaktiviert dann den Dienst.

KAPITEL 27

infacmd wfs-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- abortWorkflow, 966
- bulkComplete, 968
- cancelWorkflow, 970
- createTables, 972
- dropTables, 974
- listActiveWorkflowInstances, 976
- listMappingPersistedOutputs, 978
- listWorkflowParams, 980
- listWorkflows, 982
- recoverWorkflow, 984
- setMappingPersistedOutputs, 986
- startWorkflow, 989
- upgradeWorkflowParameterFile, 992

abortWorkflow

Bricht eine laufende Arbeitsablaufinstanz ab.

Wenn eine Zuweisungsaufgabe oder ein exklusives Gateway ausgeführt wird, schließt der Datenintegrationsdienst die Aufgabe oder das Gateway ab. Nach Abbruch oder Abschluss der Aufgabe bricht der Dienst die Arbeitsablaufinstanz ab. Der Dienst beginnt nicht mit der Ausführung von nachfolgenden Arbeitsablaufobjekten.

Der Befehl „infacmd wfs abortWorkflow“ verwendet die folgende Syntax:

```
abortWorkflow

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

<-InstanceId|-iid> instance_id
```

```
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd wfs abortWorkflow“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, der die Arbeitsablaufinstanz ausführt.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-InstanceId -iid	Instanz-ID des abzubrechenden Arbeitsablaufs	Erforderlich. Abzubrechende Arbeitsablaufinstanz-ID. Sie können die Arbeitsablaufinstanz-ID in den Arbeitsablaufeigenschaften auf der Registerkarte „Überwachen“ des Administrator Tools lesen. Sie können aber auch „infacmd wfs listActiveWorkflowInstances“ ausführen, um nach der Arbeitsablaufinstanz-ID zu suchen.

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

bulkComplete

Hält alle Vorgänge für eine Human-Aufgabe in einem bestimmten Arbeitsablauf an und übergibt die Datensätze, die von der Aufgabe angegeben werden, an die nächste Stufe im Arbeitsablauf. Der Befehl „bulkComplete“ aktualisiert den Status der Schritte in der Human-Aufgabe, um anzugeben, dass die Schritte abgeschlossen sind. Der von der Aufgabe ermittelte Status der Datensätze wird vom Befehl weder bearbeitet noch aktualisiert.

Der Befehl „bulkComplete“ verwendet die folgende Syntax:

```
bulkComplete

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

<-InstanceId|-iid> Instance_id

[<-SecurityDomain|-sdn> security_domain]

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd wfs bulkComplete“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, der die Arbeitsablaufinstanz ausführt.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
Instanz-ID -iid	Instance_ID	Erforderlich. Eindeutiger Bezeichner für den Arbeitsablauf, der die abzuschließende Human-Aufgabe ausführt. Sie können die Arbeitsablaufinstanz-ID in den Arbeitsablaufeigenschaften auf der Registerkarte „Überwachen“ des Administrator Tools lesen. Sie können aber auch „infacmd wfs listActiveWorkflowInstances“ ausführen, um nach der Arbeitsablaufinstanz-ID zu suchen.

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

cancelWorkflow

Bricht eine laufende Arbeitsablaufinstanz ab. Wenn Sie eine Arbeitsablaufinstanz abbrechen, beendet der Datenintegrationsdienst die Verarbeitung aller laufenden Aufgaben sowie die Verarbeitung der Arbeitsablaufinstanz. Der Service beginnt nicht mit der Ausführung von nachfolgenden Objekten.

Der Befehl „infacmd wfs cancelWorkflow“ verwendet die folgende Syntax:

```
cancelWorkflow

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

<-InstanceID|-iid> instance_ID

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

Die folgende Tabelle beschreibt die Optionen und Argumente für „infacmd wfs cancelWorkflow“:

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

Option	Argument	Beschreibung
-InstanceID -iid	instance_ID	Erforderlich. Abzubrechende Arbeitsablaufinstanz-ID. Sie können die Arbeitsablaufinstanz-ID in den Arbeitsablaufeigenschaften auf der Registerkarte „Überwachen“ des Administrator Tools lesen. Sie können aber auch „infacmd wfs listActiveWorkflowInstances“ ausführen, um nach der Arbeitsablaufinstanz-ID zu suchen.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

createTables

Erstellt die Datenbanktabellen, in denen Laufzeitmetadaten für den Arbeitsablauf gespeichert werden. Der Befehl erstellt leere Tabellen. Geben Sie bei Ausführung des Befehls den Dienst an, der die Arbeitsabläufe ausführt.

Überprüfen Sie vor dem Erstellen der Datenbanktabellen die folgenden Optionen auf dem Datenintegrationsdienst, der die Arbeitsabläufe ausführt:

- Das Workflow Orchestration-Dienstmodul ist auf dem Datenintegrationsdienst aktiv.
- Mit den Eigenschaften des Workflow Orchestration-Diensts wird die Verbindung für die Datenbank angegeben, in der die Arbeitsablaufmetadaten gespeichert werden.

Der createTables-Befehl verwendet die folgende Syntax:

```
createTables

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

<-ServiceName|-sn> service_name

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd wfs createTables“ beschrieben:

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

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts zum Ausführen der Arbeitsabläufe, die Metadaten in die Tabellen schreiben.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

dropTables

Löscht die Datenbanktabellen, in denen Laufzeitmetadaten für den Arbeitsablauf gespeichert werden.

Der dropTables-Befehl verwendet die folgende Syntax:

```
dropTables

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> Password

[<-SecurityDomain|-sdn> security_domain]

<-ServiceName|-sn> service_name

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd wfs dropTables“ beschrieben:

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

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Diensts, der die Arbeitsabläufe ausführt, deren Daten gelöscht werden sollen.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

listActiveWorkflowInstances

Listet aktive Arbeitsablaufinstanzen auf. Eine aktive Arbeitsablaufinstanz ist eine Instanz, für die eine Aktion ausgeführt werden kann. Listet den Status, die Arbeitsablaufinstanz-ID, den Arbeitsablaufnamen und den Anwendungsnamen für jede aktive Arbeitsablaufinstanz auf.

Aktive Arbeitsablaufinstanzen umfassen laufende Arbeitsablaufinstanzen sowie für die Wiederherstellung aktivierte Arbeitsablaufinstanzen, die abgebrochen werden.

Der Befehl „infacmd wfs listActiveWorkflowInstances“ verwendet die folgende Syntax:

```
listActiveWorkflowInstances

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

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

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd wfs listActiveWorkflowInstances“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, der die Arbeitsablaufinstanzen ausführt.

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

listMappingPersistedOutputs

Listet den Status aller dauerhaften Zuordnungsausgaben auf. Sie können die Werte der dauerhaften Zuordnungsausgabe mit dem infacmd wfs setMappingPersistedOutputs-Befehl aktualisieren.

Der infacmd wfs listMappingPersistedOutputs-Befehl verwendet die folgende Syntax:

```
listMappingPersistedOutputs

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Application|-a> application_name

<-Workflow|-wf> workflow_name

<-MappingTaskInstance|-mti> mapping_task_instance_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd wfs listMappingPersistedOutputs“ beschrieben:

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

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang. Erforderlich. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch. Optional. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Bei der Sicherheitsdomäne wird die Groß-/Kleinschreibung beachtet. Standardwert ist „Nativ“.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	application_name	Erforderlich. Name der Anwendung, die den Arbeitsablauf enthält.
-Workflow -wf	workflow_name	Erforderlich. Name des Arbeitsablaufs.
- mti	MappingTaskInstance	Erforderlich. Der Name einer Zuordnungsaufgabe, die die Zuordnungsausgaben erstellt hat.

listWorkflowParams

Listet die Parameter für einen Arbeitsablauf auf und erstellt eine Parameterdatei, die Sie für die Ausführung eines Arbeitsablaufs verwenden können. Der Befehl gibt eine XML-Datei mit Standardwerten zurück, die Sie aktualisieren können. Geben Sie den Parameterdateinamen an, wenn Sie den Arbeitsablauf mit infacmd wfs startWorkflow ausführen.

Der Befehl „infacmd wfs listWorkflowParams“ verwendet die folgende Syntax:

```
listWorkflowParams

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Application|-a> application_name

<-Workflow|-wf> workflow_name

[<-OutputFile|-o> output file_to_write_to]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd wfs listWorkflowParams“ beschrieben:

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

Option	Argument	Beschreibung
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang. Erforderlich. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch. Optional. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Bei der Sicherheitsdomäne wird die Groß-/Kleinschreibung beachtet. Standardwert ist „Native“.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	application_name	Erforderlich. Name der Anwendung, die den Arbeitsablauf enthält.
-Workflow -wf	workflow_name	Erforderlich. Name des Arbeitsablaufs.
- OutputFile - o	output file_to_write_to	Optional. Pfad und Dateiname der zu erstellenden Parameterdatei. Wenn Sie keine Datei angeben, zeigt der Befehl die Parameter in der Eingabeaufforderung an.

listWorkflowParams-Ausgabe

Der listWorkflowParams-Befehl gibt eine Parameterdatei als XML-Datei mit Standardwerten zurück, die Sie aktualisieren können.

Sie führen zum Beispiel den listWorkflowParams-Befehl in der Anwendung "MyApp" und im Arbeitsablauf "MyWorkflow" aus. Der Arbeitsablauf „MyWorkflow“ verfügt über einen Parameter mit der Bezeichnung „MyParameter“.

Der listWorkflowParams-Befehl gibt eine XML-Datei in folgendem Format zurück:

```
<?xml version="1.0" encoding="UTF-16LE"?>
<root xmlns="http://www.informatica.com/Parameterization/1.0"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema"
      version="2.0"><!--Specify deployed application specific parameters here.--><!--
    <application name="MyApp">
   <workflow name="MyWorkflow"/>
</application>--><project name="MyProject">
      <workflow name="MyWorkflow">
         <parameter name="MyParameter">Default</parameter>
      </workflow>
   </project>
</root>
```

Die Ausgabe-XML-Datei hat die folgenden Elemente der obersten Ebene:

Anwendungselement

Wenn Sie einen Parameter in einem Element auf der obersten Ebene der Anwendung definieren, wendet der Data Integration Service den Parameterwert an, wenn Sie den angegebenen Arbeitsablauf in der angegebenen Anwendung ausführen. Sie müssen mindestens ein Projektelement in eine Anwendung/einen Arbeitsablauf einbeziehen.

Standardmäßig befindet sich dieses Element auf der obersten Ebene in den Kommentaren. Entfernen Sie die Kommentare (!-- and -->), um dieses Element zu verwenden.

Projektelement

Wenn Sie einen Parameter in einem Element auf der obersten Ebene eines Projekts definieren, wendet der Data Integration Service den Parameterwert auf den angegebenen Arbeitsablauf in dem Projekt in allen bereitgestellten Anwendungen an. Der Dienst wendet den Parameterwert auch auf alle Arbeitsabläufe an, die die Objekte im Projekt verwenden.

Wenn Sie in einem Projekt denselben Parameter in einem Element auf der obersten Ebene einer Anwendung und ein Element in derselben Parameterdatei definieren, hat der im Anwendungselement definierte Parameterwert Vorrang.

listWorkflows

Listet die Arbeitsabläufe in einer Anwendung auf.

Der Befehl „infacmd wfs listWorkflows“ verwendet die folgende Syntax:

```
listWorkflows

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name
```

```
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd wfs listWorkflows“ beschrieben:

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

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

recoverWorkflow

Stellt eine Arbeitsablaufinstanz wieder her. Sie können eine Arbeitsablaufinstanz wiederherstellen, die von Ihnen abgebrochen oder durch einen behebbaren Fehler unterbrochen wurde. Wenn Sie eine Arbeitsablaufinstanz wiederherstellen, startet der Datenintegrationsdienst die Arbeitsablaufinstanz an der unterbrochenen Aufgabe neu und führt die unterbrochene Aufgabe erneut aus.

Der Befehl „infacmd wfs recoverWorkflow“ verwendet die folgende Syntax:

```
recoverWorkflow

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password
```

```
<-InstanceID|-iid> instance_ID

[<-Wait|-w> true|false]

[<-SecurityDomain|-sdn> security_domain]

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

Die folgende Tabelle beschreibt die Optionen und Argumente für „infacmd wfs recoverWorkflow“:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, der die ursprüngliche Arbeitsablaufinstanz ausgeführt hat.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-InstanceID -iid	Instanz-ID des wiederherzustellenden Arbeitsablaufs	Erforderlich. Wiederherzustellende Arbeitsablaufinstanz-ID. Sie können die Arbeitsablaufinstanz-ID in den Arbeitsablaufeigenschaften auf der Registerkarte „Überwachen“ des Administrator Tools lesen. Sie können aber auch „infacmd wfs listActiveWorkflowInstances“ ausführen, um nach der Arbeitsablaufinstanz-ID zu suchen.

Option	Argument	Beschreibung
-Wait -w	true|false	Optional. Gibt an, ob infacmd bis zur Wiederherstellung der Arbeitsablaufinstanz wartet, bevor eine Rückkehr zur Shell oder Eingabeaufforderung erfolgt. Wenn TRUE, kehrt infacmd nach Wiederherstellung der Arbeitsablaufinstanz zur Shell oder Eingabeaufforderung zurück. Sie können nachfolgende Befehle erst ausführen, wenn die Arbeitsablaufinstanz wiederhergestellt wurde. Ist die Option auf FALSE festgelegt, kehrt infacmd sofort zur Shell oder Eingabeaufforderung zurück. Sie müssen nicht auf die Wiederherstellung der Arbeitsablaufinstanz warten, bis Sie den nächsten Befehl ausführen. Standardwert ist „false“.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.

setMappingPersistedOutputs

Aktualisiert die dauerhaften Zuordnungsausgaben für eine Zuordnungsaufgabeninstanz in einem Arbeitsablauf. Oder setzt die dauerhaften Zuordnungsausgaben auf Nullwerte. Mit den Befehlsoptionen werden der Instanzname der Zuordnungsaufgabe sowie der Name der Anwendung und des Arbeitsablaufs angegeben.

Geben Sie zum Aktualisieren eines Werts ein Namen-Wert-Paar ein, das den Namen der Zuordnungsausgabe und den Wert enthält, in den er geändert werden soll. Verwenden Sie zum Zurücksetzen eines dauerhaften Werts auf Nullwerte die Option zum Zurücksetzen. Sie können bestimmte oder alle Zuordnungsausgaben für

eine Zuordnungsaufgabeninstanz zurücksetzen. Verwenden Sie zum Anzeigen dauerhafter Zuordnungsausgaben den infacmd listMappingPersistedOutputs-Befehl.

Der infacmd wfs setMappingPersistedOutputs-Befehl verwendet die folgende Syntax:

```
setMappingPersistedOutputs

<-DomainName|-dn> domain_name

[<-ServiceName|-sn> service_name]

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Application|-a> application_name

<-Workflow|-wf> workflow_name

<-MappingTaskInstance|-mti> mapping_task_instance_name]

<-outputValues|-onvp> space_separated_output_value_pairs

[<-resetOutputs |-reset> reset_outputs]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd wfs setMappingPersistedOutputs“ beschrieben:

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

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang. Erforderlich. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch. Optional. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Bei der Sicherheitsdomäne wird die Groß-/Kleinschreibung beachtet. Standardwert ist „Nativ“.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	application_name	Erforderlich. Name der Anwendung, die den Arbeitsablauf enthält.
-Workflow -wf	workflow_name	Erforderlich. Name des Arbeitsablaufs.
-MappingTaskInstance -mti	mappingTaskInstancename	Erforderlich. Der Name einer Zuordnungsaufgabe, die die Zuordnungsausgaben erstellt hat.

Option	Argument	Beschreibung
-outputvalues -onvp	space_separated_output_value_pairs	Optional. Ändert den dauerhaften Wert bestimmter Zuordnungsausgaben. Geben Sie durch Leerzeichen getrennte Namen-Wert-Paare in der folgenden Syntax ein: output_name=value output2_name=value output3_name=value
-ResetOutputs -reset	reset_outputs	Optional. Entfernt den Wert der Zuordnungsausgabe aus dem Repository. Geben Sie zum Zurücksetzen bestimmter Zuordnungsausgaben die Option zum Zurücksetzen mit durch Leerzeichen getrennten Zuordnungsausgabenamen in die folgende Syntax ein: -reset mapping_output_name mapping_output2_name mapping_output3_name

startWorkflow

Startet eine Instanz eines Arbeitsablaufs. Sie können mehrere Instanzen eines Arbeitsablaufs gleichzeitig ausführen. Sie können eine Parameterdatei für den Arbeitsablauf oder einen Parametersatz verwenden.

Der Befehl „infacmd wfs startWorkflow“ verwendet die folgende Syntax:

```
startWorkflow

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Application|-a> application_name

<-Workflow|-wf> workflow_name

[<-Wait|-w> true|false]

[<-ParameterFile|-pf> parameter file path]

[<-ParameterSet|-ps> ParameterSet name. Both ParameterFile and ParameterSet should not
be given]

[<-OsProfile|-osp> os_profile__name]
```

Der Befehl gibt die Ablaufinstanz-ID aus.

Die folgende Tabelle beschreibt infacmd wfs startWorkflow-Optionen und -Argumente:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch. Optional. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Bei der Sicherheitsdomäne wird die Groß-/Kleinschreibung beachtet. Standardwert ist „Nativ“.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	application_name	Erforderlich. Name der Anwendung, die den Arbeitsablauf enthält.
-Workflow -wf	workflow_name	Erforderlich. Name des zu startenden Arbeitsablaufs.
-Wait -w	true|false	Optional. Gibt an, ob infacmd bis zum Abschluss der Arbeitsablaufinstanz wartet, bevor eine Rückkehr zur Shell oder Eingabeaufforderung erfolgt. Wenn TRUE, kehrt infacmd nach Abschluss der Arbeitsablaufinstanz zur Shell oder Eingabeaufforderung zurück. Sie können nachfolgende Befehle erst ausführen, wenn die Arbeitsablaufinstanz abgeschlossen ist. Ist die Option auf FALSE festgelegt, kehrt infacmd sofort zur Shell oder Eingabeaufforderung zurück. Sie müssen nicht auf den Abschluss der Arbeitsablaufinstanz warten, bis Sie den nächsten Befehl ausführen. Standardwert ist „False“.
-ParameterFile -pf	parameter file path	Optional. Name und Pfad der Parameterdatei. Geben Sie einen Parameterdatei- und Parametersatznamen nicht im selben Befehl ein.

Option	Argument	Beschreibung
-ParameterSet -ps	parameter set	Optional. Name des zur Laufzeit zu verwendenden Parametersatzes. Die Parametersatzoption überschreibt alle mit einer Anwendung bereitgestellten Parametersätze. Geben Sie einen Parameterdatei- und Parametersatznamen nicht im selben Befehl ein.
-OsProfile -osp	os_profile_name	Optional. Name des Betriebssystemprofils, unter dem der Arbeitsablauf ausgeführt wird.

upgradeWorkflowParameterFile

Aktualisiert die Werte in einer Arbeitsablaufparameterdatei, um sicherzustellen, dass die Parameterwerte in der Datei in der aktuellen Version gültig sind. Beim Ausführen des Befehls geben Sie eine zu aktualisierende Arbeitsablaufparameterdatei sowie eine Zieldatei an, die die gültigen Parameterwerte enthalten soll.

Der Befehl „infacmd wfs upgradeWorkflowParameterFile“ verwendet die folgende Syntax:

```
upgradeWorkflowParameterFile

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Application|-a> application_name

<-Workflow|-wf> workflow_name

<-ParameterFile|-pf> parameter file path

<-TargetOutputFile|-of> output_file_path
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd wfs upgradeWorkflowParameterFile“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch. Optional. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Bei der Sicherheitsdomäne wird die Groß-/Kleinschreibung beachtet. Standardwert ist „Nativ“.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-Application -a	application_name	Erforderlich. Name der Anwendung, die den Arbeitsablauf enthält.
-Workflow -wf	workflow_name	Erforderlich. Name des Arbeitsablaufs, der die Parameterdatei mit den Werten liest.
-Wait -w	true|false	Optional. Gibt an, ob infacmd bis zum Abschluss der Arbeitsablaufinstanz wartet, bevor eine Rückkehr zur Shell oder Eingabeaufforderung erfolgt. Wenn TRUE, kehrt infacmd nach Abschluss der Arbeitsablaufinstanz zur Shell oder Eingabeaufforderung zurück. Sie können nachfolgende Befehle erst ausführen, wenn die Arbeitsablaufinstanz abgeschlossen ist. Ist die Option auf FALSE festgelegt, kehrt infacmd sofort zur Shell oder Eingabeaufforderung zurück. Sie müssen nicht auf den Abschluss der Arbeitsablaufinstanz warten, bis Sie den nächsten Befehl ausführen. Standardwert ist „False“.

Option	Argument	Beschreibung
-ParameterFile -pf	parameter file path	Erforderlich. Name und Speicherort der Parameterdatei, die die zu aktualisierenden Werte enthält.
-TargetOutputFile -of	parameter file path	Erforderlich. Name und Speicherort der Ausgabedatei aus dem Befehl. Die Ausgabedatei enthält die gültigen Parameter für die aktuelle Version.

KAPITEL 28

infacmd ws-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- ListOperationOptions, 996
- ListOperationPermissions, 998
- ListWebServiceOptions, 1000
- ListWebServicePermissions, 1002
- ListWebServices, 1004
- RenameWebService, 1006
- SetOperationPermissions, 1008
- SetWebServicePermissions, 1011
- StartWebService, 1014
- StopWebService, 1016
- UpdateOperationOptions, 1017
- UpdateWebServiceOptions, 1020

ListOperationOptions

Listet die Eigenschaften eines Webdienstvorgangs auf, der in einem Datenintegrationsdienst bereitgestellt wird.

Der Befehl „infacmd ws ListOperationOptions“ verwendet die folgende Syntax:

```
ListOperationOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-WebService|-ws> web_service

<-Operation|-op> operation
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ws ListOperationOptions“ beschrieben:

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

Option	Argument	Beschreibung
-WebService -ws	web_service	Erforderlich. Name des Webdiensts.
Operation -op	operation	Erforderlich. Name des Webdienstvorgangs, für den Eigenschaften aufgelistet werden sollen.

ListOperationPermissions

Listet Gruppen- und Benutzerberechtigungen für eine Webserviceoperation auf. Sie müssen direkte oder effektive Berechtigungen angeben.

Der Befehl „infacmd ws ListOperationPermissions“ verwendet die folgende Syntax:

```
ListOperationPermissions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-WebService|-ws> web_service

<-Operation|-op> operation

<<-Direct> direct_permission_only|<-Effective> effective_permission_only
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ws ListOperationPermissions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem der Webdienst bereitgestellt wird.

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-WebService -ws	web_service	Erforderlich. Name des Webdiensts.
-Operation -op	operation	Erforderlich. Name des Webdienstvorgangs, für den Eigenschaften aufgelistet werden sollen.
-Direct oder -Effective	direct_permission_only effective_permission_only	Erforderlich. Geben Sie Direct ein, um zugewiesene Berechtigungen aufzulisten. Geben Sie Effective ein, um geerbte Berechtigungen aufzulisten.

ListWebServiceOptions

Listen Sie die Eigenschaften eines Webdiensts auf, der in einem Datenintegrationsdienst bereitgestellt wird. Sie können die Eigenschaften unter Verwendung des Administrator-Tools oder infacmd ws UpdateWebServiceOptions konfigurieren.

Der Befehl „infacmd ws ListWebServiceOptions“ verwendet die folgende Syntax:

```
ListWebServiceOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-WebService|-ws> web_service
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ws ListWebServiceOptions“ beschrieben:

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

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-WebService -ws	web_service	Erforderlich. Name des Webdiensts.

ListWebServicePermissions

Listet Gruppen- und Benutzerberechtigungen für einen Webservice auf, der in einem Datenintegrationsdienst bereitgestellt wird. Sie müssen direkte oder effektive Berechtigungen angeben.

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ws ListWebServicePermissions“ beschrieben:

```
ListWebServicePermissions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-WebService|-ws> web_service

<<-Direct> direct_permission_only|<-Effective> effective_permission_only
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ws ListWebServicePermissions“ beschrieben:

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

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

ListWebServices

Listet die Webdienste für eine Anwendung auf. Wenn Sie keinen Anwendungsnamen eingeben, listet infacmd alle Webdienste für einen Datenintegrationsdienst auf.

Der Befehl „infacmd ws ListWebServices“ verwendet die folgende Syntax:

```
ListWebServices

<-DomainName|-dn> domain_name
```

```
<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-WebService|-ws> web_service

[<-Application|-a> application]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ws ListWebServices“ beschrieben:

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

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

RenameWebService

Umbenennen eines Webdiensts.

Der Befehl „infacmd ws RenameWebService“ verwendet die folgende Syntax:

```
RenameWebService

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-WebService|-ws> web_service

<-NewName|-n> new_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ws RenameWebService“ beschrieben:

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

Option	Argument	Beschreibung
-WebService -ws	web_service	Erforderlich. Name des Webdiensts.
-NewName -n	new_name	Erforderlich. Neuer Name für den Webdienst.

SetOperationPermissions

Legt die Gruppen- und Benutzerberechtigungen für einen Webdienstvorgang fest. Sie können Berechtigungen für einen Benutzer oder eine Gruppe festlegen oder verweigern.

Der Befehl „infacmd ws SetOperationPermissions“ verwendet die folgende Syntax:

```
SetOperationPermissions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-WebService|-ws> web_service

<-Operation|-op> operation

<-GranteeUserName|-gun> grantee_user_name|
<-GranteeGroupName|-ggn> grantee_group_name>

[<-GranteeSecurityDomain|-gsdn> grantee_security_domain]

[<-AllowedPermissions|-ap> list_of_allowed_permissions_separated_by_space]

[<-DeniedPermissions|-dp> list_of_denied_permissions_separated_by_space]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ws SetOperationPermissions“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-WebService -ws	web_service	Erforderlich. Name des Webdiensts.
-Operation -op	Operation	Erforderlich. Name des Webdienstvorgangs.
-GranteeUserName|GranteeGroupName -gun|-ggn	grantee_user_name| grantee_group_name	Erforderlich. Benutzername bzw. Gruppenname, für den Berechtigungen festgelegt oder verweigert werden sollen.
-GranteeSecurityDomain -gsdn	grantee_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden und Benutzerberechtigungen gewähren. Name der Sicherheitsdomäne, der der Benutzer angehört.

Option	Argument	Beschreibung
-AllowedPermissions -ap	list_of_allowed_permissions_separated_by_space	Erforderlich. Liste der zulässigen Berechtigungen. Geben Sie einen der folgenden Parameter durch Leerzeichen getrennt ein: - GRANT. Benutzer können mithilfe des Administrator-Tools oder des infacmd-Befehlszeilenprogramms Berechtigungen für die Operation gewähren oder widerrufen. - EXECUTE. Benutzer können die Operation ausführen.
-DeniedPermissions -dp	list_of_denied_permissions_separated_by_space	Optional. Liste der Berechtigungen, die Benutzern verweigert werden sollen. Geben Sie einen der folgenden Parameter durch Leerzeichen getrennt ein: - GRANT. Benutzer können Berechtigungen für den Vorgang weder gewähren noch entziehen. - EXECUTE. Benutzer können den Vorgang nicht ausführen.

SetWebServicePermissions

Legt die Benutzer- oder Gruppenberechtigungen für einen Webdienst fest. Sie können Berechtigungen für einen Benutzer oder eine Gruppe festlegen oder verweigern.

Der Befehl „infacmd ws SetWebServicePermissions“ verwendet die folgende Syntax:

```
SetWebServicePermissions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-WebService|-ws> web_service

<-GranteeUserName|-gun> grantee_user_name|
<-GranteeGroupName|-ggn> grantee_group_name>

[<-GranteeSecurityDomain|-gsdn> grantee_security_domain]

[<-AllowedPermissions|-ap> list_of_allowed_permissions_separated_by_space]

[<-DeniedPermissions|-dp> list_of_denied_permissions_separated_by_space]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ws SetWebServicePermissions“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-WebService -ws	web_service	Erforderlich. Name des Webdiensts.
-GranteeUserName|GranteeGroupName -gun|-ggn	grantee_user_name| grantee_group_name	Erforderlich. Benutzername bzw. Gruppenname, für den Berechtigungen festgelegt oder verweigert werden sollen.
-GranteeSecurityDomain -gsdn	grantee_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden und Benutzerberechtigungen gewähren. Name der Sicherheitsdomäne, der der Benutzer angehört.

Option	Argument	Beschreibung
-AllowedPermissions -ap	list_of_allowed_permissions_separated_by_space	Erforderlich. Liste der zulässigen Berechtigungen. Geben Sie einen der folgenden Parameter durch Leerzeichen getrennt ein: - GRANT. Benutzer können mithilfe des Administrator-Tools oder des infacmd-Befehlszeilenprogramms Berechtigungen für den Webdienst gewähren oder widerrufen. - EXECUTE. Benutzer können den Webdienst ausführen.
-DeniedPermissions -dp	list_of_denied_permissions_separated_by_space	Optional. Liste der Berechtigungen, die Benutzern verweigert werden sollen. Geben Sie einen der folgenden Parameter durch Leerzeichen getrennt ein: - GRANT. Benutzer können Berechtigungen für den Webdienst weder gewähren noch entziehen. - EXECUTE. Benutzer können den Webdienst nicht ausführen.

StartWebService

Startet einen Webdienst, der in einem Datenintegrationsdienst bereitgestellt wird.

Der Befehl „infacmd ws StartWebService“ verwendet die folgende Syntax:

```
StartWebService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-WebService|-ws> web_service
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ws StartWebService“ beschrieben:

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

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Name des Datenintegrationsdiensts, in dem der Webdienst bereitgestellt wird.
-WebService -ws	web_service	Erforderlich. Name des zu startenden Webdiensts.

StopWebService

Stoppt einen laufenden Webdienst.

Der Befehl „infacmd ws StopWebService“ verwendet die folgende Syntax:

```
StopWebService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-WebService|-ws> web_service
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ws StopWebService“ beschrieben:

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

Option	Argument	Beschreibung
-Password -pd	Passwort	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie einen Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-ServiceName -sn	service_name	Name des Datenintegrationsdiensts, in dem der Webdienst bereitgestellt wird.
-WebService -ws	web_service	Erforderlich. Name des zu beendenden Webdiensts.

UpdateOperationOptions

Aktualisiert die Eigenschaften einer Webdienst-Operation, die in einem Datenintegrationsdienst bereitgestellt wird.

Der Befehl „infacmd ws UpdateOperationOptions“ verwendet die folgende Syntax:

```
UpdateOperationOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name
```

```
<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-WebService|-ws> web_service

<-Operation|-op> operation

<-Options|-o> options
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ws UpdateOperationOptions“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Sie können den Zeitraum für das Belastbarkeits-Timeout mit der Option -re oder der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT festlegen. Wenn Sie den Zeitraum für das Belastbarkeits-Timeout mit beiden Methoden festlegen, hat die Option -re Vorrang.
-WebService -ws	web_service	Erforderlich. Name des Webdiensts.
Operation -op	operation	Erforderlich. Name des zu aktualisierenden Webdienstvorgangs.
-Options -o> options	optionen	Geben Sie die Webdienstoption im folgenden Format ein: `... -o option_type.option_name=value`

Operationsoptionen

Verwenden Sie Operationsoptionen zum Aktualisieren einer Web-Dienst-Operation. Verwenden Sie die Operationsoptionen mit infacmd ws UpdateOperationOptions.

Geben Sie Operationsoptionen in folgendem Format ein:

```
... -o OperationOptions.option_name=value ...
```

In der folgenden Tabelle wird eine Option für infacmd ws UpdateOperationOptions beschrieben:

Option	Beschreibung
WebServiceOperationOptions.ResultSetCacheExpirationPeriod	Zeitraum in Millisekunden, während dem der Ergebnissatz-Cache verwendet werden kann. Wenn der Wert auf -1 festgelegt ist, läuft der Cache nie ab. Wenn der Wert auf 0 festgelegt ist, ist das Ergebnissatz-Caching deaktiviert. Wenn alle Caches denselben Ablaufzeitraum verwenden sollen, bereinigen Sie den Ergebnissatz-Cache, nachdem Sie den Ablaufzeitraum geändert haben. Default is 0.

UpdateWebServiceOptions

Aktualisiert die Eigenschaften für einen Webdienst, der in einem Datenintegrationsdienst bereitgestellt wird. Um die Eigenschaften für diesen Webdienst anzuzeigen, können Sie infacmd ws ListWebServiceOptions verwenden.

Der Befehl „infacmd ws UpdateWebServiceOptions“ verwendet die folgende Syntax:

```
UpdateWebServiceOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-WebService|-ws> web_service

<-Options|-o> options
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd ws UpdateWebServiceOptions“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-ServiceName -sn	service_name	Erforderlich. Name des Datenintegrationsdiensts, auf dem der Webdienst bereitgestellt wird.

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

Web-Dienst-Optionen

Verwenden Sie eine bestimmte Syntax für die Eingabe von Web-Dienst-Optionen.

Geben Sie Web-Dienst-Optionen im folgenden Format ein:

```
... -o option_type.option_name=value
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden Web-Dienst-Optionen beschrieben:

Option	Beschreibung
WebServiceOptions.startupType	Legt fest, ob der Web-Dienst zur Ausführung aktiviert ist, wenn die Anwendung startet oder wenn Sie den Web-Dienst starten. Geben Sie "enabled" oder "disabled" ein.
WebServiceOptions.traceLevel	Level der in das Web-Dienst-Protokoll zur Laufzeit geschriebenen Fehlermeldungen. Geben Sie eine der folgenden Meldungslevel ein: - AUS - SCHWERWIEGEND - WARNUNG - INFO - FEIN - SUPERFEIN - ALLE
WebServiceOptions.requestTimeout	Maximale Anzahl an Millisekunden, in denen der Data Integration Service ein Operations-Mapping ausführt, bevor die Web-Dienst-Anfrage abläuft. Standardwert ist 3.600.000.
WebServiceOptions.maxConcurrentRequests	Maximale Anzahl an Anfragen, die der Web-Dienst auf einmal verarbeiten kann. Standardwert ist 10.
WebServiceOptions.sortOrder	Sortierreihenfolge, die der Data Integration Service zum Sortieren und Vergleichen von Daten verwendet, wenn er im Unicode-Modus ausgeführt wird. Die Standardeinstellung ist "binär".
WebServiceOptions.EnableTransportLayerSecurity	Gibt an, dass der Web-Dienst HTTPS verwenden muss. Wenn der Data Integration Service nicht zur Verwendung von HTTPS konfiguriert ist, wird der Web-Dienst nicht gestartet. Geben Sie TRUE oder FALSE ein.
WebServiceOptions.EnableWSSecurity	Aktiviert den Data Integration Service zu Validierung der Benutzeranmeldedaten sowie zur Sicherstellung, dass der Benutzer zur Ausführung der Web-Dienst-Operationen berechtigt ist. Geben Sie TRUE oder FALSE ein.

Option	Beschreibung
WebServiceOptions.optimizeLevel	Die Optimierungsebene, die der Data Integration Service für das Objekt anwendet. Geben Sie den numerischen Wert ein, der mit der Optimierungsebene verbunden ist, die Sie konfigurieren möchten. Sie können Sie einen der folgenden numerischen Werte eingeben: - 0. Der Datenintegrationsdienst wendet keine Optimierung an. - 1. Der Datenintegrationsdienst wendet die frühe Projektionsoptimierungsmethode an. - 2. Der Datenintegrationsdienst wendet die Optimierungsmethoden „Frühe Projektion“, „Frühe Auswahl“, „Push-Into“ und „Prädikat“ an. - 3. Der Datenintegrationsdienst wendet die Optimierungsmethoden „Kostenbasiert“, „Frühe Projektion“, „Frühe Auswahl“, „Push-Into“, „Prädikat“ und „Semi-Join“ an.
WebServiceOptions.DTMKeepAliveTime	Anzahl der Millisekunden, für die die DTM-Instanz geöffnet bleibt, nachdem sie die letzte Anfrage abgeschlossen hat. Webdienstanfragen für denselben Vorgang können die offene Instanz wiederverwenden. Verwenden Sie die Keep Alive-Zeit, um die Leistung zu erhöhen, wenn die für die Verarbeitung der Anfrage erforderliche Zeit im Vergleich zur Dauer der Initialisierung der DTM-Instanz gering ist. Wenn die Anfrage fehlschlägt, wird die DTM-Instanz beendet. Muss eine Ganzzahl sein. Eine negative Ganzzahl bedeutet, dass die DTM-Keep Alive-Zeit für den Data Integration Service verwendet wird. 0 bedeutet, dass der Data Integration Service die DTM-Instanz nicht im Speicher beibehält. Standardwert ist -1.

KAPITEL 29

infacmd xrf-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- generateReadableViewXML, 1024
- updateExportXML, 1024

generateReadableViewXML

Erstellt eine lesbare XML-Datei aus einer XML-Exportdatei. Die XML-Exportdatei kann Inhalte aus der exportierten Domäne oder aus dem Model Repository enthalten.

Der Befehl infacmd xrf generateReadableViewXML verwendet die folgende Syntax:

```
generateReadableViewXML

<-SourceExportFile|-sxf> source_export_file

<-TargetFile|-tf> target_file_Name
```

In der folgenden Tabelle werden infacmd xrf generateReadableViewXML-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-SourceExportFile -sxf	source_export_file	Erforderlich. Pfad und Dateiname der XML-Exportdatei.
-TargetFile -tf	target_file_Name	Erforderlich. Pfad und Dateiname der lesbaren XML-Datei.

updateExportXML

Aktualisiert eine Export-XML-Datei mit den Änderungen an der entsprechenden lesbaren XML-Datei. Sie können eine lesbare XML-Datei, die Inhalt aus dem Model Repository enthält, aktualisieren und die Export-XML-Datei mit den Änderungen erneut generieren.

Der infacmd xrf updateExportXML-Befehl verwendet die folgende Syntax:

```
updateExportXML
```

```
<SourceExportFile|-sxf> source_file
<generatedViewFile|-vf> view_file
<TargetFile|-tf> target_file_Name
```

In der folgenden Tabelle werden infacmd xrf updateExportXML-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-SourceExportFile -sxf	source_file	Erforderlich. Pfad und Dateiname der XML-Exportdatei.
-generatedViewFile -vf	view_file	Erforderlich. Pfad und Dateiname der lesbaren XML-Datei, die die erforderlichen Änderungen enthält.
-TargetFile -tf	target_file_Name	Erforderlich. Pfad und Dateiname der aktualisierten XML-Exportdatei.

KAPITEL 30

infacmd-Steuerdateien

Dieses Kapitel umfasst die folgenden Themen:

- infacmd-Steuerdateien - Übersicht, 1026
- Konfiguration von Steuerdateien, 1027
- Exportsteuerdateien, 1028
- Importsteuerdateien, 1032
- Regeln und Richtlinien für Steuerdateien, 1040
- Steuerdatei-Beispiele für Domänenobjekte, 1041
- Steuerdatei-Beispiele für Model Repository-Objekte, 1042

infacmd-Steuerdateien - Übersicht

Wenn Sie mit dem infacmd-Befehlszeilenprogramm Objekte exportieren und importieren, können Sie mit einer Kontrolldatei die Objekte filtern, die den Befehl exportieren oder importieren.

Sie können die folgenden Steuerdateien mit infacmd verwenden:

- Exportsteuerdatei. Verwenden Sie eine Exportsteuerdatei, um die Objekte anzugeben, die aus der Domäne oder aus dem Modellrepository in eine Exportdatei exportiert werden sollen.
- Exportsteuerdatei. Verwenden Sie eine Exportsteuerdatei, um die Objekte anzugeben, die aus dem Modellrepository in eine Exportdatei exportiert werden sollen.
- Importsteuerdatei. Verwenden Sie eine Importsteuerdatei, um die Objekte anzugeben, die aus der Exportdatei in die Domäne oder das Modellrepository importiert werden sollen.
- Importsteuerdatei. Verwenden Sie eine Importsteuerdatei, um die Objekte anzugeben, die aus der Exportdatei in das Modellrepository importiert werden sollen.

Wenn Sie während des Exports keine Exportsteuerdatei verwenden, werden die aus der Domäne oder dem angegebenen Modellrepository-Projekt exportierten Objekte nicht von infacmd gefiltert. Wenn Sie während des Imports in die Domäne keine Importsteuerdatei verwenden, importiert infacmd alle in der Exportdatei enthaltenen Objekte. Wenn Sie während des Imports in das Modellrepository keine Importsteuerdatei verwenden, importiert infacmd alle im angegebenen Projekt in der Exportdatei enthaltenen Objekte.

Wenn Sie während des Exports keine Exportsteuerdatei verwenden, werden die aus dem angegebenen Modellrepository-Projekt exportierten Objekte nicht von infacmd gefiltert. Wenn Sie während des Imports in das Modellrepository keine Importsteuerdatei verwenden, importiert infacmd alle im angegebenen Projekt in der Exportdatei enthaltenen Objekte.

Konfiguration von Steuerdateien

Eine Steuerdatei ist eine XML-Datei, die auf einer Export- oder Import-Schemadatei basiert. Sie können eine Steuerdatei basierend auf den folgenden Schemadateien erstellen:

- exportControl.xsd. Legt das Layout und die Syntax der Export-Steuerdateien fest.
- importControl.xsd. Legt das Layout und die Syntax der Import-Steuerdateien fest.

Sie können in folgendem Installationsverzeichnis auf die Schemadateien als Teil der oie-util.jar zugreifen:

```
<InformaticaInstallationDir>/services/shared/jars/shapp
```

Um aus der Befehlszeile auf exportControl.xsd und importControl.xsd zuzugreifen, wechseln Sie zum Speicherort von oie-util.jar und extrahieren die JAR-Datei mit dem folgenden Befehl:

```
jar -xvf <jar_name>
```

Sie können die Datei oie-util jar auch mit Packprogrammen wie WinRAR extrahieren oder die XSD-Dateien aus der Datei oie-util jar mit dem Java-Decompiler anzeigen, um auf die Schemadateien zuzugreifen.

Zum Erstellen einer Export-Steuerdatei erstellen Sie eine XML-Datei basierend auf der exportControl.xsd-Schemadatei. Die Datei muss mit einer XML-Deklaration und dem Speicherort der gehosteten Schemadatei im exportParams-Root-Element beginnen. Beziehen Sie die folgenden Zeilen in der Datei ein:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
...
</exportParams>
```

Zum Erstellen einer Import-Steuerdatei erstellen Sie eine XML-Datei basierend auf der importControl.xsd-Schemadatei. Die Datei muss mit einer XML-Deklaration und dem Speicherort der gehosteten Schemadatei im importParams-Root-Element beginnen. Beziehen Sie die folgenden Zeilen in der Datei ein:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<importParams xmlns="http://www.informatica.com/oie/importControl/9">
...
</importParams>
```

Binden Sie die verbleibenden Elemente und Attribute in die XML-Datei basierend auf den Objekten ein, die Sie exportieren oder importieren möchten.

Benennungskonventionen für Steuerdateien

Verwenden Sie einen eindeutigen Dateinamen für die Steuerdateien.

Fügen Sie jedem Dateinamen ein Präfix hinzu, um anzugeben, ob es sich um eine Export- oder Importsteuerdatei handelt. Verwenden Sie zum Beispiel die folgenden vorgeschlagenen Benennungskonventionen:

- ecf_<file_name>.xml für Exportsteuerdateien
- icf_<file_name>.xml für Importsteuerdateien

In Steuerdateien für Domänenobjekte können Sie außerdem den für den Export oder Import vorgesehenen Objekttyp im Dateinamen angeben.

Exportsteuerdateien

Eine Exportsteuerdatei ist eine XML-Datei, die Sie mit infacmd-Befehlen verwenden. Die Steuerdatei filtert die Objekte, die infacmd aus einer Domäne oder einem Modellrepository exportiert. Eine Exportsteuerdatei ist eine XML-Datei, die Sie mit infacmd-Befehlen verwenden. Die Steuerdatei filtert die Objekte, die infacmd aus einem Modellrepository exportiert.

Sie können eine Exportsteuerdatei mit den folgenden Befehlen verwenden:

Sie können eine Exportsteuerdatei mit den folgenden Befehlen verwenden:

infacmd isp ExportDomainObjects

Exportiert native Benutzer, native Gruppen, Rollen und Verbindungen aus der Domäne in eine Exportdatei im XML-Format. Wenn Sie eine Exportsteuerdatei für den Befehl angeben, filtern Sie die Objekte, die Sie exportieren möchten. Verwenden Sie zum Beispiel eine Steuerdatei zum Exportieren aller Objekte, die nach einem bestimmten Datum erstellt wurden, oder zum Exportieren von Verbindungen (aber keine anderen Objekttypen).

infacmd oie ExportObjects

Exportiert alle Modellrepository-Objekttypen aus einem angegebenen Projekt in eine Exportdatei im XML-Format. Wenn Sie eine Exportsteuerdatei für den Befehl angeben, filtern Sie die Objekte, die Sie exportieren möchten. Verwenden Sie zum Beispiel eine Steuerdatei zum Exportieren aller Objekte, die von einem bestimmten Benutzer erstellt wurden, oder zum Exportieren bestimmter Objekttypen in das Projekt.

Infacmd exportiert keine leeren Ordner. Beim Exportieren von Modellrepository-Objekten exportiert infacmd ebenfalls die abhängigen Objekte. Ein abhängiges Objekt ist ein Objekt, das von einem anderen Objekt verwendet wird. Abhängige Objekte können in demselben oder in anderen Projekten vorhanden sein.

Eine Exportsteuerdatei verwendet andere Parameter basierend darauf, ob Sie die Datei zum Exportieren von Domänenobjekten oder Modellrepository-Objekten konfigurieren.

Eine Exportsteuerdatei verwendet andere Parameter basierend darauf, ob Sie die Datei zum Exportieren von Modellrepository-Objekten konfigurieren.

Export-Steuerdatei-Parameter für Domänenobjekte

Verwenden Sie die Export-Steuerdatei-Parameter zum Konfigurieren der Objekte, die Sie aus der Domäne exportieren möchten.

Eine Export-Steuerdatei für Domänenobjekte kann die folgenden Elemente enthalten:

- exportParams. Kann mehrere objectList-Elemente enthalten.
- objectList. Enthält Attribute zum Filtern der Objekte nach Typ. Kann mehrere Objektelemente enthalten.
- object. Enthält ein Attribut zum Filtern von Objekten nach Namen.

In der folgenden Tabelle werden die Export-Steuerdateielemente aufgelistet, die konfigurierbare Attribute enthalten:

Element	Attributname	Attributbeschreibung
objectList	type	Erforderlich. Typ der zu exportierenden Domäne. Geben Sie einen der folgenden Werte an: - User - Group - Role - Connection Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden.
objectList	createdBefore	Optional. Datum und Uhrzeit. Exportiert Objekte des angegebenen Typs, die vor diesem Datum und dieser Uhrzeit erstellt wurde. Geben Sie das Datum und die Uhrzeit in folgendem Format ein: `yyyy-MM-dd HH:mm:ssZ`
objectList	createdAfter	Optional. Datum und Uhrzeit. Exportiert Objekte des angegebenen Typs, die nach diesem Datum und dieser Uhrzeit erstellt wurden. Geben Sie das Datum und die Uhrzeit in folgendem Format ein: `yyyy-MM-dd HH:mm:ssZ`
objectList	lastUpdatedBefore	Optional. Datum und Uhrzeit. Exportiert Objekte des angegebenen Typs, die nach diesem Datum und dieser Uhrzeit aktualisiert wurden. Geben Sie das Datum und die Uhrzeit in folgendem Format ein: `yyyy-MM-dd HH:mm:ssZ`
objectList	lastUpdatedAfter	Optional. Datum und Uhrzeit. Exportiert Objekte des angegebenen Typs, der nach diesem Datum und dieser Uhrzeit aktualisiert wurden. Geben Sie das Datum und die Uhrzeit in folgendem Format ein: `yyyy-MM-dd HH:mm:ssZ`
object	name	Erforderlich. Name des zu exportierenden Objekts. Wenn das einbezogene objectList-Element ein time-Attribut enthält, exportiert infacmd Objekte, die mit dem angegebenen Objektnamen und dem Zeitfilter übereinstimmen. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden.

Export-Steuerdatei-Beispiel für Domänenobjekte

Der folgende Code zeigt ein Beispiel einer Export-Steuerdatei für Domänenobjekte:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">

  <!-- Export a specific connection. -->
  <objectList type="connection" >
    <object name="connection1" />
  </objectList>

  <!-- Export groups created before the specified date and time. -->
  <objectList type="group" createdBefore="2010-11-12 10:00:00 +0530" />

  <!-- Export role1 and role2 if created after the specified date and time. -->
  <objectList type="role" createdAfter="2010-12-25 10:00:00 +0530">
    <object name="role1" />
    <object name="role2" />
  </objectList>
```

```
  <!-- Export all users. -->
  <objectList type="user" />
</exportParams>
```

Exportsteuerdateiparameter für Modellrepository-Objekte

Verwenden Sie die Exportsteuerdateiparameter zum Konfigurieren der Objekte, die Sie aus dem Modellrepository exportieren möchten.

Eine Exportsteuerdatei für Modellrepository-Objekte kann die folgenden Elemente enthalten:

- exportParams. Kann ein einzelnes folders-Element enthalten.
- folders. Kann mehrere folder-Elemente enthalten.
- folder. Enthält Attribute zum Filtern von Objekten in einem angegebenen Ordner. Kann mehrere objectList-Elemente enthalten.
- objectList. Enthält Attribute zum Filtern der Objekte nach Typ. Kann mehrere Objektelemente enthalten.
- object. Enthält ein Attribut zum Filtern von Objekten nach Namen.

In der folgenden Tabelle werden die konfigurierbaren Attribute für das Ordnerelement in der Exportsteuerdatei beschrieben:

Attributname	Attributbeschreibung
Pfad	Optional. Pfad des Ordners, der die zu exportierenden Objekte enthält. Verwenden Sie das folgende Format: `"/<folder_name>/<folder_name>"` Wenn beispielsweise ein Projekt einen Ordner mit dem Namen „F1“ enthält, ist „/F1“ der Ordnerpfad von F1. Um alle Objekte im Projekt zu exportieren, geben Sie „/“ an. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden. Standardwert ist „/“.
recursive	Optional. Zeigt an, ob Objekte aus Unterordnern des angegebenen Ordners exportiert werden sollen. Mit der Einstellung „true“ findet ein Export aus Unterordnern statt. Gültige Werte sind „true“ und „false“. Bei diesem Wert muss die Groß-/Kleinschreibung beachtet werden. Standardwert ist „true“.

auswählen	Optional. Zeigt an, ob infacmd alle übrigen Objekte im angegebenen Ordner exportiert, wenn Sie ein objectList-Element für den Ordner definieren. Bei Auswahl von „all“ werden alle übrigen Objekte exportiert. Zum Beispiel exportieren die folgenden Zeilen Zuordnungen, die von user1 erstellt wurden. Die Zeilen exportieren alle übrigen Objekte im angegebenen Ordner:
	`<folder path="/Testfolder" select="all">`
	`  <objectList type="Mapping" createdBy="user1" />`
	`</folder>`
	Wenn Sie ein objectList-Element definieren und das select-Attribut nicht verwenden, exportiert infacmd Objekte in Übereinstimmung mit den in objectList definierten Attributen. Zum Beispiel exportieren die folgenden Zeilen Zuordnungen, die von user1 im angegebenen Ordner erstellt wurden:
	`<folder path="/Testfolder">`
	`  <objectList type="Mapping" createdBy="user1" />`
	`</folder>`
	Wenn Sie kein objectList-Element für den Ordner definieren, ist „all“ der Standardwert des ausgewählten Attributs. Zum Beispiel exportiert die folgende Zeile alle Objekte in den angegebenen Ordner:
	`<folder path="/Testfolder" />`
	Gültiger Wert ist „all“.

Attributname	Attributbeschreibung
createdBy	Optional. Benutzername. Exportiert von diesem Benutzer erstellte Objekte. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden.
createdBefore	Optional. Datum und Uhrzeit. Exportiert vor diesem Datum und dieser Uhrzeit erstellte Objekte. Geben Sie das Datum und die Uhrzeit in folgendem Format ein: `yyyy-MM-dd HH:mm:ssZ`
createdAfter	Optional. Datum und Uhrzeit. Exportiert nach diesem Datum und dieser Uhrzeit erstellte Objekte. Geben Sie das Datum und die Uhrzeit in folgendem Format ein: `yyyy-MM-dd HH:mm:ssZ`
lastUpdatedBefore	Optional. Datum und Uhrzeit. Exportiert vor diesem Datum und dieser Uhrzeit aktualisierte Objekte. Geben Sie das Datum und die Uhrzeit in folgendem Format ein: `yyyy-MM-dd HH:mm:ssZ`
lastUpdatedAfter	Optional. Datum und Uhrzeit. Exportiert nach diesem Datum und dieser Uhrzeit aktualisierte Objekte. Geben Sie das Datum und die Uhrzeit in folgendem Format ein: `yyyy-MM-dd HH:mm:ssZ`
lastUpdatedBy	Optional. Benutzername. Exportiert Objekte, die von diesem Benutzer zuletzt aktualisiert wurden. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden.

In der folgenden Tabelle werden die konfigurierbaren Attribute für das objectList-Element in der Exportsteuerdatei beschrieben:

Attributname	Attributbeschreibung
Typ	Erforderlich. Typ des aus dem angegebenen Ordnerpfad zu exportierenden Modellrepository-Objekts. Gültige Werte beinhalten alle Objekttypen im Modellrepository. Sie können den Objekttyp in der Ansicht „Eigenschaften“ im Developer-Tool anzeigen. Beispielsweise können Sie „Relationales Datenobjekt“ oder „Profil“ eingeben. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden.
createdBy	Optional. Benutzername. Exportiert Objekte des angegebenen Typs, die von diesem Benutzer erstellt wurden. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden.
createdBefore	Optional. Datum und Uhrzeit. Exportiert Objekte des angegebenen Typs, die vor diesem Datum und dieser Uhrzeit erstellt wurden. Geben Sie das Datum und die Uhrzeit in folgendem Format ein: `yyyy-MM-dd HH:mm:ssZ`
createdAfter	Optional. Datum und Uhrzeit. Exportiert Objekte des angegebenen Typs, die nach diesem Datum und dieser Uhrzeit erstellt wurden. Geben Sie das Datum und die Uhrzeit in folgendem Format ein: `yyyy-MM-dd HH:mm:ssZ`
lastUpdatedBefore	Optional. Datum und Uhrzeit. Exportiert Objekte des angegebenen Typs, die vor diesem Datum und dieser Uhrzeit aktualisiert wurden. Geben Sie das Datum und die Uhrzeit in folgendem Format ein: `yyyy-MM-dd HH:mm:ssZ`

Attributname	Attributbeschreibung
lastUpdatedAfter	Optional. Datum und Uhrzeit. Exportiert Objekte des angegebenen Typs, die nach diesem Datum und dieser Uhrzeit aktualisiert wurden. Geben Sie das Datum und die Uhrzeit in folgendem Format ein: `yyyy-MM-dd HH:mm:ssZ`
lastUpdatedBy	Optional. Benutzername. Exportiert Objekte des angegebenen Typs, die von diesem Benutzer zuletzt aktualisiert wurden. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden.

In der folgenden Tabelle wird das konfigurierbare Attribut für das Objektelement in der Exportsteuerdatei beschrieben:

Attributname	Attributbeschreibung
name	Erforderlich. Name des zu exportierenden Objekts. Wenn das einbezogene objectList-Element ein user- oder time-Attribut enthält, exportiert infacmd Objekte, die mit dem angegebenen Objektnamen und dem Benutzer- oder Zeitfilter übereinstimmen. Bei diesem Wert muss die Groß-/Kleinschreibung beachtet werden.

Exportsteuerdateibeispiel für Modellrepository-Objekte

Der folgende Code zeigt ein Beispiel einer Exportsteuerdatei für Modellrepository-Objekte:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
 <folders>

   <!-- Consider exporting all objects in the project. Do not export from subfolders. -->
   <folder recursive="false" select="all">

      <!-- Export mapping1 if created by the specified user. -->
      <objectList type="Mapping" createdBy="user1">
        <object name="mapping1"/>
      <!-- Export all other mappings. -->
      </objectList>

      <!-- Export Aggregator transformations created by the specified user. -->
      <objectList type="Aggregator" createdBy="user1" />

    <!-- Export all remaining objects. -->
    </folder>
 </folders>
</exportParams>
```

Importsteuerdateien

Eine Importsteuerdatei ist eine XML-Datei, die Sie mit infacmd-Befehlen verwenden. Die Steuerdatei filtert die Objekte, die infacmd aus einer Exportdatei in eine Domäne oder ein Modellrepository importiert. Eine Importsteuerdatei ist eine XML-Datei, die Sie mit infacmd-Befehlen verwenden. Die Steuerdatei filtert die Objekte, die infacmd aus einer Exportdatei in ein Modellrepository importiert.

Sie können eine Importsteuerdatei mit den folgenden Befehlen verwenden:

Sie können eine Importsteuerdatei mit dem folgenden Befehl verwenden:

infacmd isp ImportDomainObjects

Importiert native Benutzer, native Gruppen, Rollen und Verbindungen aus einer Exportdatei in eine Domäne. Wenn Sie eine Importsteuerdatei für den Befehl angeben, können Sie die folgenden Aufgaben abschließen:

- Filtern der Objekte, die Sie importieren möchten (Verwenden Sie zum Beispiel die Steuerdatei zum Importieren eines bestimmten Objekttyps.)
- Konfigurieren von Konfliktlösungsstrategien für bestimmte Objekttypen oder Objekte

infacmd oie ImportObjects

Importiert Modellrepository-Objekte aus einer Exportdatei in ein Modellrepository. Wenn Sie eine Importsteuerdatei für den Befehl angeben, können Sie die folgenden Aufgaben abschließen:

- Filtern der Objekte, die Sie importieren möchten (Verwenden Sie zum Beispiel die Steuerdatei zum Importieren eines bestimmten Objekttyps.)
- Konfigurieren von Konfliktlösungsstrategien für bestimmte Objekttypen oder Objekte
- Zuordnen von Verbindungen im Quell-Repository zu Verbindungen im Target-Repository

Abhängige Modellrepository-Objekte können sich in verschiedenen Ordnern oder Projekten befinden. Sie müssen alle abhängigen Objekte mithilfe von folderMap-Elementen in die Importsteuerdatei einbeziehen. Andernfalls kann der Import mit einer Fehlermeldung fehlschlagen, da das Target-Repository kein abhängiges Objekt enthält.

Beim Importieren der Objekte können Sie eine Konfliktlösungsstrategie über die Befehlszeile oder Steuerdatei definieren. Die Steuerdatei hat Vorrang, wenn Sie eine Konfliktlösung in der Befehlszeile und der Steuerdatei definieren. Der Import schlägt fehl, wenn ein Konflikt auftritt und Sie keine Konfliktlösungsstrategie definiert haben.

Wenn Sie die Umbenennungs-Konfliktlösungsstrategie definieren, können Sie einen Namen in der Steuerdatei für ein bestimmtes Objekt angeben. Alternativ dazu kann infacmd durch Anhängen einer laufenden Nummer an das Ende des Namens einen Namen generieren.

Eine Importsteuerdatei verwendet andere Parameter basierend darauf, ob Sie die Datei zum Importieren von Domänenobjekten oder Modellrepository-Objekten konfigurieren.

Eine Importsteuerdatei verwendet andere Parameter basierend darauf, ob Sie die Datei zum Importieren von Domänenobjekten oder Modellrepository-Objekten konfigurieren.

Import-Steuerdatei-Parameter für Domänenobjekte

Verwenden Sie die Import-Steuerdatei-Parameter zum Konfigurieren der Objekte, die Sie aus einer XML-Datei in die Domäne importieren möchten.

Eine Import-Steuerdatei für Domänenobjekte kann die folgenden Elemente enthalten:

- importParams. Kann mehrere objectList-Elemente enthalten.
- objectList. Enthält Attribute zum Filtern der Objekte nach Typ. Kann mehrere Objektelemente enthalten.
- object. Enthält Attribute zum Filtern der Objekte nach Namen.

In der folgenden Tabelle werden die Import-Steuerdateielemente aufgelistet, die konfigurierbare Attribute enthalten:

Element	Attributname	Attributbeschreibung
objectList	type	Erforderlich. Typ des Domänenobjekts, das Sie importieren möchten. Geben Sie einen der folgenden Werte an: - User - Group - Role - Connection Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden.

objectList	select	Optional. Zeigt an, ob infacmd alle übrigen Objekte des angegebenen Typs importiert, wenn Sie ein object-Element für objectList definieren. Bei Auswahl von „all“ werden alle übrigen Objekte importiert. Zum Beispiel importieren die folgenden Zeilen Group1 mit einer Reuse-Lösungsstrategie. Die Zeilen importieren alle übrigen Gruppen mit einer Merge-Lösungsstrategie:
		`<objectList type="group" select="all" resolution="merge">`
		`  <object name="Group1" resolution="reuse" />`
		`</objectList>`
		Wenn Sie ein object-Element definieren und das select-Attribut nicht verwenden, exportiert infacmd Objekte in Übereinstimmung mit den im object-Element definierten Attributen. Zum Beispiel importieren die folgenden Zeilen Group1 mit einer Merge-Lösungsstrategie.
		`<objectList type="group" resolution="merge">`
		`  <object name="Group1" />`
		`</objectList>`
		Wenn Sie kein object-Element für objectList definieren, ist „all“ der Standardwert des ausgewählten Attributs. Zum Beispiel importieren die folgenden Zeilen alle Gruppen mit einer Merge-Lösungsstrategie.
		`<objectList type="group" resolution="merge" />`
		Gültiger Wert ist „all“.

objectList	resolution	Optional. Lösungsstrategie bei Auftreten eines Namenskonflikts. Gilt für alle Objekte des angegebenen Typs. Geben Sie einen der folgenden Werte an: - Replace. Ersetzen Sie das Target-Objekt mit dem Quellobjekt. - Rename. Benennen Sie das Quellobjekt mit einem generierten Namen um und importieren Sie es anschließend. - Reuse. Verwenden Sie das Objekt in der Target-Domäne wieder. - Merge. Führen Sie die Objekte in einem Objekt zusammen. Diese Option kann für Gruppen verwendet werden. Bei diesen Wert muss die Groß-/Kleinschreibung nicht beachtet werden.
object	name	Erforderlich. Der Name eines bestimmten zu importierenden Objekts des angegebene Objekttyps. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden.

Element	Attributname	Attributbeschreibung
object	resolution	Optional. Lösungsstrategie bei Auftreten eines Namenskonflikts für dieses Objekt. Geben Sie einen der folgenden Werte an: - Replace. Ersetzen Sie das Target-Objekt mit dem Quellobjekt. - Rename. Benennen Sie das Quellobjekt um und importieren Sie es anschließend. - Reuse. Verwenden Sie das Objekt in der Target-Domäne wieder. - Merge. Führen Sie die Objekte in einem Objekt zusammen. Diese Option kann für Gruppen verwendet werden. Bei diesen Wert muss die Groß-/Kleinschreibung nicht beachtet werden.
object	renameTo	Optional. Zu verwendender Name, wenn Rename die Konfliktlösungsstrategie ist. Wenn Sie keinen Namen festlegen, dann generiert infacmd einen Namen durch Anhängen einer Nummer am Ende des Namens. Infacmd ignoriert den Wert, wenn keine Konflikte auftreten oder wenn es sich bei der Konfliktlösungsstrategie nicht um Rename handelt.
object	renameIdTo	Optional. Zu verwendender ID-String beim Importieren eines Verbindungsobjekts und wenn die Konfliktlösungsstrategie „Umbenennen“ lautet. Wenn Sie keine Verbindungs-ID angeben, generiert infacmd eine ID, indem eine Nummer an das Ende der Verbindungs-ID angehängt wird. Infacmd ignoriert den Wert, wenn keine Konflikte auftreten oder wenn es sich bei der Konfliktlösungsstrategie nicht um Rename handelt.

Import-Steuerdatei-Beispiel für Domänenobjekte

Der folgende Code zeigt ein Beispiel einer Import-Steuerdatei für Domänenobjekte:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<importParams xmlns="http://www.informatica.com/oie/importControl/9">

 <! -- Import all connections, roles, and users. -->
 <objectList type="connection" resolution="replace" />
 <objectList type="role" resolution="reuse" />
 <objectList type="user" resolution="rename" />

 <! -- Import specific groups. -->
 <objectList type="group">
  <object name="g1" resolution="replace" />
  <object name="g2" resolution="merge" />
 </objectList>
</importParams>
```

Importsteuerdateiparameter für Modellrepository-Objekte

Verwenden Sie die Importsteuerdateiparameter zum Konfigurieren der Objekte, die Sie aus einer XML-Datei in das Modellrepository importieren möchten.

Eine Importsteuerdatei für Modellrepository-Objekte können die folgenden Elemente enthalten:

- importParams. Können ein einzelnes folderMaps-Element in einem einzelnen connectionInfo-Element enthalten.
- folderMaps. Kann Elemente aus mehreren folderMap-Elementen enthalten.
- folderMap. Enthält Attribute zum Filtern von Objekten in einem angegebenen Ordner. Kann mehrere objectList-Elemente enthalten.
- objectList. Enthält Attribute zum Filtern der Objekte nach Typ. Kann mehrere Objektelemente enthalten.
- object. Enthält Attribute zum Filtern der Objekte nach Namen.

- connectionInfo. Kann ein einzelnes rebindMap-Element enthalten.
- rebindMap. Kann mehrere rebind-Elemente enthalten.
- rebind. Enthält Attribute zum Zuordnen von Verbindungen im Quell-Repository zu Verbindungen im Target-Repository.

In der folgenden Tabelle werden die konfigurierbaren Attribute für das folderMap-Element in der Importsteuerdatei beschrieben:

Attributname	Attributbeschreibung
sourceProject	Erforderlich. Name des Quellprojekts in der Exportdatei, das die zu importierenden Objekte enthält. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden.
sourceFolderPath	Optional. Pfad des Quellordners in der Exportdatei, der die zu importierenden Objekte enthält. Verwenden Sie das folgende Format: `"/<folder_name>/<folder_name>"` Wenn beispielsweise ein Projekt einen Ordner mit dem Namen „F1“ enthält, ist „/F1“ der Ordnerpfad von F1. Um alle Objekte im Projekt zu importieren, geben Sie „/“ an. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden. Standardwert ist „/“.
targetProject	Erforderlich. Name des Projekts im Target-Repository, in das Objekte importiert werden sollen. Das Projekt muss im Repository vorhanden sein, bevor Sie diese Objekte importieren. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden.
targetFolderPath	Optional. Pfad des Ordners im Target-Repository, in das Sie Objekte importieren möchten. Verwenden Sie das folgende Format: `"/<folder_name>/<folder_name>"` Wenn beispielsweise ein Projekt einen Ordner mit dem Namen „F1“ enthält, ist „/F1“ der Ordnerpfad von F1. Um alle Objekte in das Target-Projekt zu importieren, geben Sie „/“ an. Der Ordner muss im Repository vorhanden sein, bevor Sie diese Objekte importieren. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden. Standardwert ist „/“.
recursive	Optional. Zeigt an, ob Objekte aus Unterordnern des angegebenen Ordners importiert werden sollen. Mit der Einstellung „true“ findet ein Import aus Unterordnern statt. Gültige Werte sind „true“ und „false“. Bei diesem Wert muss die Groß-/Kleinschreibung beachtet werden. Standardwert ist „true“.

Attributname	Attributbeschreibung

auswählen	Optional. Zeigt an, ob infacmd alle übrigen Objekte im angegebenen Projekt importiert, wenn Sie ein objectList-Element für folderMap definieren. Bei Auswahl von „all“ werden alle übrigen Objekte importiert. Zum Beispiel importieren die folgenden Zeilen Zuordnungen mit einer Reuse-Lösungsstrategie. Die Zeilen importieren alle übrigen Objekte mit einer Replace-Lösungsstrategie:
	`<folderMap sourceProject="p1" targetProject="p2" select="all" resolution="replace">`
	`  <objectList type="Mapping" resolution="reuse" />`
	`</folderMap>`
	Wenn Sie ein objectList-Element definieren und das select-Attribut nicht verwenden, importiert infacmd Objekte in Übereinstimmung mit den in objectList definierten Attribute. Zum Beispiel importieren die folgenden Zeilen Zuordnungen mit einer Replace-Lösungsstrategie:
	`<folderMap sourceProject="p1" targetProject="p2" resolution="replace">`
	`  <objectList type="Mapping" />`
	`</folderMap>`
	Wenn Sie kein objectList-Element für folderMap definieren, wird der Standardwert „all“ verwendet. Zum Beispiel importiert die folgende Zeile alle Objekte mit einer Replace-Lösungsstrategie:
	`<folderMap sourceProject="p1" targetProject="p2" resolution="replace" />`
	Gültiger Wert ist „all“.

resolution	Optional. Lösungsstrategie bei Auftreten eines Namenskonflikts. Gilt für alle Objekte in diesem Ordner. Geben Sie einen der folgenden Werte an: - Rename. Benennen Sie das Quellobjekt mit einem generierten Namen um und importieren Sie es anschließend. - Replace. Ersetzen Sie das Target-Objekt mit dem Quellobjekt. - Reuse. Verwenden Sie das Objekt im Modellrepository wieder. - Keine. Bei diesen Wert muss die Groß-/Kleinschreibung nicht beachtet werden. Der Standardwert ist „Keine“.

In der folgenden Tabelle werden die konfigurierbaren Attribute für das objectList-Element in der Importsteuerdatei beschrieben:

Attributname	Attributbeschreibung
Typ	Erforderlich. Typ des Modellrepository-Objekts, das in den angegebenen Ordnerpfad importiert werden soll. Gültige Werte beinhalten alle Objekttypen im Modellrepository. Sie können den Objekttyp in der Ansicht „Eigenschaften“ im Developer-Tool anzeigen. Beispielsweise können Sie „Relationales Datenobjekt“ oder „Profil“ eingeben. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden.

auswählen	Optional. Zeigt an, ob infacmd alle übrigen Objekte des angegebenen Typs importiert, wenn Sie ein object-Element für objectList definieren. Bei Auswahl von „all“ werden alle übrigen Objekte importiert. Zum Beispiel importieren die folgenden Zeilen MyMapping mit einer Reuse-Lösungsstrategie. Die Zeilen importieren alle übrigen Zuordnungen mit einer Replace-Lösungsstrategie:
	`<folderMap sourceProject="p1" targetProject="p2">`
	`  <objectList type="Mapping" select="all" resolution="replace">`
	`  <object name="MyMapping" resolution="reuse" />`
	`  </objectList>`
	`</folderMap>`
	Wenn Sie ein Objektelement definieren und das select-Attribut nicht verwenden, importiert infacmd Objekte in Übereinstimmung mit den im Objektelement definierten Attributen. Zum Beispiel importieren die folgenden Zeilen die Zuordnung namens MyMapping mit einer Replace-Lösungsstrategie:
	`<folderMap sourceProject="p1" targetProject="p2">`
	`  <objectList type="Mapping" resolution="replace">`
	`  <object name="MyMapping"/>`
	`  </objectList>`
	`</folderMap>`
	Wenn Sie kein object-Element für objectList definieren, wird der Standardwert „all“ verwendet. Zum Beispiel importieren die folgenden Zeilen alle Zuordnungen mit einer Replace-Lösungsstrategie:
	`<folderMap sourceProject="p1" targetProject="p2">`
	`  <objectList type="Mapping" resolution="replace" />`
	`</folderMap>`
	Gültiger Wert ist „all“.

resolution	Optional. Lösungsstrategie bei Auftreten eines Namenskonflikts. Gilt für alle Objekte des angegebenen Typs. Geben Sie einen der folgenden Werte an: - Rename. Benennen Sie das Quellobjekt mit einem generierten Namen um und importieren Sie es anschließend. - Replace. Ersetzen Sie das Target-Objekt mit dem Quellobjekt. - Reuse. Verwenden Sie das Objekt im Modellrepository wieder. - Keine. Bei diesen Wert muss die Groß-/Kleinschreibung nicht beachtet werden. Der Standardwert ist „Keine“.

In der folgenden Tabelle werden die konfigurierbaren Attribute für das Objektelement in der Importsteuerdatei beschrieben:

Attributname	Attributbeschreibung
name	Erforderlich. Name eines bestimmten zu importierenden Objekts des angegebenen Objekttyps. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden.
resolution	Optional. Lösungsstrategie bei Auftreten eines Namenskonflikts für dieses Objekt. Geben Sie einen der folgenden Werte an: - Rename. Benennen Sie das Quellobjekt um und importieren Sie es anschließend. - Replace. Ersetzen Sie das Target-Objekt mit dem Quellobjekt. - Reuse. Verwenden Sie das Objekt im Modellrepository wieder. - Keine. Bei diesen Wert muss die Groß-/Kleinschreibung nicht beachtet werden. Der Standardwert ist „Keine“.
renameTo	Optional. Zu verwendender Name, wenn Rename als Konfliktlösungsstrategie dient. Wenn Sie keinen Namen festlegen, generiert infacmd einen Namen durch Anhängen einer Zahl an das Ende des Namens. Infacmd ignoriert den Wert, wenn keine Konflikte auftreten oder wenn es sich bei der Konfliktlösungsstrategie nicht um Rename handelt.
renameIdTo	Optional. Zu verwendender ID-String beim Importieren eines Verbindungsobjekts und wenn die Konfliktlösungsstrategie „Umbenennen“ lautet. Wenn Sie keine Verbindungs-ID angeben, generiert infacmd eine ID, indem eine Nummer an das Ende der Verbindungs-ID angehängt wird. Infacmd ignoriert den Wert, wenn keine Konflikte auftreten oder wenn es sich bei der Konfliktlösungsstrategie nicht um Rename handelt.

In der folgenden Tabelle werden die konfigurierbaren Attribute für das rebind-Element in der Importsteuerdatei beschrieben:

Attributname	Attributbeschreibung
source	Erforderlich. Name einer Quellverbindung in der Datei, die Sie importieren. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden.
target	Erforderlich. Name einer Verbindung im Target-Modellrepository, die der Quellverbindung zugeordnet werden soll. Standardmäßig muss die Verbindung im Zielrepository vorhanden sein, bevor Sie diese Objekte importieren. Wenn die Verbindung nicht vorhanden ist, schlägt der Import fehl. Wenn Sie infacmd ausführen, können Sie die Validierung der Zielverbindung während des Imports überspringen. Wenn Sie die Validierung der Zielverbindung überspringen, wird der Import auch dann erfolgreich ausgeführt, wenn keine Verbindung im Zielrepository vorhanden ist. Bei diesem Wert muss die Groß-/Kleinschreibung nicht beachtet werden.

Importsteuerdateibeispiel für Modellrepository-Objekte

Der folgende Code zeigt ein Beispiel einer Importsteuerdatei für Modellrepository-Objekte:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<importParams xmlns="http://www.informatica.com/oie/importControl/9">
 <folderMaps>
  <folderMap sourceProject="project1" sourceFolderPath="/f1" targetProject="project2"
targetFolderPath="/f1" recursive="true">

    <! -- Import mapping1 with the Rename resolution strategy. -->
    <objectList type="Mapping" select="all" resolution="replace">
      <object name="mapping1" resolution="rename" renameTo="mapping1_new"/>

    <! -- Import all remaining mappings with the Replace resolution strategy. -->
    </objectList>
```

```
    <! -- Import all Aggregator transformations with the Replace resolution strategy. -->
    <objectList type="Aggregator" resolution="replace"/>

    <! -- Import all Filter transformations with no resolution strategy. -->
    <objectList type="Filter" resolution="none"/>
  </folderMap>
 </folderMaps>

 <! -- Map connections in the source repository to connections in the target repository.
-->
 <connectionInfo>
  <rebindMap>
   <rebind source="src_Conn1" target="tgt_Conn1"/>
   <rebind source="src_Conn2" target="tgt_Conn2"/>
  </rebindMap>
 </connectionInfo>
</importParams>
```

Regeln und Richtlinien für Steuerdateien

Überprüfen Sie die folgenden Regeln und Richtlinien, bevor Sie Steuerdateien erstellen:

- Bei Element- und Attributnamen muss die Groß-/Kleinschreibung nicht beachtet werden.
- Steuerdateien enthalten eine Hierarchie von XML-Elementen. Elemente auf verschiedenen Ebenen können dasselbe Attribut enthalten. Ein untergeordnetes Element erbt einen für das übergeordnete Element definierten Wert, wenn dasselbe Attribut nicht für das untergeordnete Element definiert ist. Die für das untergeordnete Element definierten Attributwerte überschreiben den Wert desselben Attributs, das für das übergeordnete Element definiert ist.
- Wenn ein Element mehrere Attribute definiert, exportiert oder importiert infacmd alle Objekte, die mit allen Attributfiltern übereinstimmen. Sie definieren zum Beispiel die Attribute createdBefore und lastUpdatedAfter für ein objectList-Element in einer Export-Steuerdatei. Infacmd exportiert Objekte des angegebenen Typs, die vor dem angegebenen Datum erstellt und nach dem angegebenen Datum zuletzt aktualisiert wurden.
- Die Werte der time-Attribute werden dabei nicht berücksichtigt. Sie legen zum Beispiel für createdAfter den Eintrag "2011-02-01 16:00:00-0800" in einer Export-Steuerdatei fest. Infacmd exportiert alle Objekte, die nach dem 1. Februar 2011 um 16 Uhr erstellt wurden. Infacmd exportiert alle keine Objekte, die am 1. Februar 2011 um 16 Uhr erstellt wurden.
- Sie können ein objectList-Element eines bestimmten Typs einmal in einer Steuerdatei für Domänenobjekte angeben. Sie geben zum Beispiel ein objectList-Element vom Typ "connection" an. Sie können kein anderes objectList-Element vom Typ "connection" in derselben Datei angeben.
- Sie können ein objectList-Element eines bestimmten Typs einmal in einem Ordner oder folderMap-Element für Model Repository-Objekte angeben. Sie geben zum Beispiel ein objectList-Element vom Typ "Flat File Data Object" an. Sie können kein anderes objectList-Element vom Typ "Flat File Data Object" in demselben Ordner oder folderMap-Element angeben.

Steuerdatei-Beispiele für Domänenobjekte

Sie können Domänenobjekte filtern, um diese nach Datum/Uhrzeit zu exportieren. Sie können Domänenobjekte filtern, um diese nach Objekttyp und Objektname zu exportieren und zu importieren.

Exportieren von Domänenobjekten nach Zeit

Um nach dem 25.12.2010 um 15:30 Uhr erstellte Benutzer zu exportieren, können Sie die folgende Steuerdatei erstellen:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
  <objectList type="user" createdAfter="2010-12-25 10:00:00 +0530" />
</exportParams>
```

Exportieren und Importieren von Domänenobjekten nach Typ

Um alle Benutzer, Gruppen und Rollen (aber keine Verbindungen) aus einer Domäne zu exportieren, können Sie die folgende Steuerdatei erstellen:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
  <objectList type="group"/>
  <objectList type="role" />
  <objectList type="user" />
</exportParams>
```

Um die Benutzer und Gruppen (aber keine Rollen) in die Target-Domäne zu importieren, können Sie die folgende Steuerdatei erstellen:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<importParams xmlns="http://www.informatica.com/oie/importControl/9">
  <objectList type="group" resolution="merge"/>
  <objectList type="user" resolution="replace" />
</importParams>
```

Exportieren und Importieren von Domänenobjekten nach Namen

Sie möchten alle Benutzer und Benutzergruppen und die Developer- und Analyst-Rollen aus der Quelldomäne exportieren. Sie möchten bestimmte Verbindungen exportieren, wenn diese nach dem 02.01.2011 um 08:00 Uhr erstellt wurden. Sie können die folgende Steuerdatei erstellen:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
  <objectList type="group"/>
  <objectList type="user" />
  <objectList type="role">
    <object name="Developer" />
    <object name="Analyst" />
  </objectList>
  <objectList type="connection" createdAfter="2011-02-01 16:00:00-0800">
    <object name="Connection1" />
    <object name="Connection2" />
    <object name="Connection3" />
  </objectList>
</exportParams>
```

Um alle Benutzer und Gruppen (und bestimmte Rollen und Verbindungen) in die Target-Domäne zu importieren, können Sie die folgende Steuerdatei erstellen:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<importParams xmlns="http://www.informatica.com/oie/importControl/9">
  <objectList type="group" resolution="reuse" />
  <objectList type="user" resolution="reuse" />
  <objectList type="role">
    <object name="Developer" resolution="replace" />
    <object name="Analyst" resolution="replace" />
  </objectList>
```

```
  <objectList type="connection">
    <object name="Connection1" resolution="rename" renameTo="ProdConnection1" />
    <object name="Connection2" resolution="rename" renameTo="ProdConnection2" />
    <object name="Connection3" resolution="rename" renameTo="ProdConnection3" />
  </objectList>
</importParams>
```

Steuerdatei-Beispiele für Model Repository-Objekte

Sie können den Export der Model Repository-Objekte nach Zeit oder Benutzer filtern. Sie können den Export oder Import der Model Repository-Objekte nach Objekttyp oder Objektnamen filtern.

Exportieren von Model Repository-Objekten nach Zeit

Um alle Objekte in einem Ordner namens Folder1 zu exportieren, die vor dem 02.01.2011 um 8:00 Uhr erstellt wurden, können Sie die folgende Steuerdatei erstellen:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
<folders>
  <folder path="/Folder1" createdBefore="2011-02-01 16:00:00-0800" />
</folders>
</exportParams>
```

Exportieren von Model Repository-Objekten nach Benutzer

Um alle Objekte in dem vom Administrator zuletzt aktualisierten Projekt zu exportieren, können Sie die folgende Steuerdatei erstellen:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
<folders>
  <folder lastUpdatedBy="Administrator" />
</folders>
</exportParams>
```

Exportieren und Importieren von Model Repository-Objekten nach Typ

Um alle Zuordnungen aus einem Ordner namens Folder1 zu exportieren, können Sie die folgende Steuerdatei erstellen:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
<folders>
  <folder path="/Folder1" />
    <objectList type="Mapping" />
  </folder>
</folders>
</exportParams>
```

Sie möchten zum Beispiel alle von user2 erstellten Mappings und alle übrigen von user1 erstellen Objekte exportieren. Das für das untergeordnete objectList-Element erstellte createdby-Attribut überschreibt dasselbe für das übergeordnete Ordnerelement definierte Attribut. Sie können die folgende Steuerdatei erstellen:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
<folders>
  <folder path="/Folder1" select="all" createdBy="user1" />
    <objectList type="Mapping" createdBy="user2" />
  </folder>
</folders>
</exportParams>
```

Sie möchten alle Mappings aus der Exportdatei importieren. Einige der aus Folder1 exportierten Mappings enthalten abhängige Objekte, die in Folder2 des Quell-Repositorys enthalten waren. Um abhängige Objekte zu importieren, müssen Sie alle abhängigen Objekte mithilfe von folderMap-Elementen in die Import-Steuerdatei einbeziehen. Sie möchten ebenfalls die Verbindungen im Quell-Repository zu den Verbindungen im Target-Repository zuordnen. Sie können die folgende Steuerdatei erstellen:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<importParams xmlns="http://www.informatica.com/oie/importControl/9">
<folderMaps>
  <folderMap sourceProject="DevProject" sourceFolderpath="/Folder1"
targetProject="TestProject" targetFolderPath="/TestFolder1" resolution="reuse">
    <objectList type="Mapping" />
  </folderMap>
  <folderMap sourceProject="DevProject" sourceFolderpath="/Folder2"
targetProject="TestProject" targetFolderPath="/TestFolder2" resolution="reuse" />
</folderMaps>
<connectionInfo>
  <rebindMap>
    <rebind source="src_connection1" target="tgt_connection1" />
    <rebind source="src_connection2" target="tgt_connection2" />
  </rebindMap>
</connectionInfo>
</importParams>
```

Exportieren und Importieren von Model Repository-Objekten nach Name

Sie möchten eine Zuordnung namens TestMapping exportieren, die nach dem 11.11.2010 um 15:59:59 Uhr erstellt wurde. Sie möchten alle übrigen Objekte in denselben Ordner exportieren. Sie können die folgende Steuerdatei erstellen:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
<folders>
  <folder path="/Folder1" select="all" />
    <objectList type="Mapping" createdAfter="2010-11-11 23:59:59-0800" >
      <object name="TestMapping" />
    </objectList>
  </folder>
</folders>
</exportParams>
```

Eine Exportdatei enthält Einfachdatei-Datenobjekte und relationale Datenobjekte. Sie möchten das Einfachdatei-Datenobjekt namens NewFlatFileDataObject und alle relationalen Datenobjekte aus der Exportdatei importieren. Sie können die folgende Steuerdatei erstellen:

```
<?xml version="1.0" encoding="UTF-16LE" standalone="yes" ?>
<importParams xmlns="http://www.informatica.com/oie/importControl/9">
 <folderMaps>
  <folderMap sourceProject="SampleProject" targetProject="SampleProject"
           targetFolderPath="/TestFolder">
   <objectList type="Flat File Data Object" resolution="replace" >
    <object name="NewFlatFileDataObject" />
   </objectList>
   <objectList type="Relational Data Object" resolution="replace" />
  </folderMap>
 </folderMaps>
</importParams>
```

KAPITEL 31

infasetup-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- Verwenden von infasetup, 1044
- BackupDomain, 1046
- DefineDomain, 1049
- DefineGatewayNode, 1061
- DefineWorkerNode, 1068
- DeleteDomain, 1072
- GenerateEncryptionKey, 1075
- Hilfe, 1076
- ListDomainCiphers, 1077
- MigrateEncryptionKey, 1078
- RestoreDomain, 1079
- SwitchToKerberosMode, 1082
- UpdateGatewayNode, 1083
- UpdateKerberosAdminUser, 1088
- UpdateKerberosConfig, 1089
- UpdateDomainCiphers, 1089
- UpdateWorkerNode, 1092
- UnlockUser, 1095
- ValidateandRegisterFeature, 1096

Verwenden von infasetup

infasetup ist ein Befehlszeilenprogramm zum Verwalten von PowerCenter-Domänen und -Knoten.

infasetup ist ein Befehlszeilenprogramm zum Aktualisieren des Gateway-Knotens.

Verwenden Sie *infasetup* zum Ändern der Domänen- und Knoteneigenschaften nach der Installation der PowerCenter-Dienste mit dem PowerCenter-Installationsprogramm. Sie können mit *infasetup* z. B. die Portnummer für einen Knoten ändern, nachdem Sie PowerCenter-Dienste installiert haben.

Verwenden Sie *infasetup* zum Ändern der Domänen- und Knoteneigenschaften, nachdem Sie die Domäne und die Dienste installiert haben.

Sie können mit *infasetup* Domänen sichern, wiederherstellen, definieren und löschen sowie Knoten definieren und aktualisieren.

Ausführen von Befehlen

infasetup wird über die Befehlszeile aufgerufen. Sie können Befehle direkt oder aus einem Skript, einer Batchdatei oder einem anderen Programm ausführen. Unter Windows handelt es sich bei *infasetup* um eine Batchdatei mit der Erweiterung .bat. Unter UNIX handelt es sich bei *infasetup* um eine Skriptdatei mit der Erweiterung .sh.

So führen Sie infasetup-Befehle aus:

1. Öffnen Sie die Eingabeaufforderung.

   Öffnen Sie unter Windows die Eingabeaufforderung als Administrator. Wenn Sie die Eingabeaufforderung nicht als Administrator öffnen, hat der Windows-Systemadministrator beim Zugriff auf Dateien im Informatica-Installationsverzeichnis möglicherweise Probleme.

2. Wechseln Sie an der Eingabeaufforderung zu dem Verzeichnis, in dem sich die ausführbare *infasetup*-Datei befindet.

   Standardmäßig wird *infasetup* im Verzeichnis <InformaticaInstallationDir>/isp/bin installiert.

3. Geben Sie `infasetup` unter Windows oder `infasetup.sh` unter UNIX gefolgt vom Befehlsnamen und den erforderlichen Optionen und Argumenten ein. Bei Befehlsnamen spielt die Groß- und Kleinschreibung keine Rolle.

   Beispiel:

   ```
   infasetup(.sh) command_name [-option1] argument_1 [-option2] argument_2...
   ```

Befehlsoptionen

Beim Ausführen von *infasetup* geben Sie Optionen für jeden Befehl gefolgt von den erforderlichen Argumenten ein. Befehlsoptionen wird unter Missachtung der Groß-/Kleinschreibung ein Bindestrich vorangestellt. Argumente folgen der Option.

Folgender Befehl beispielsweise aktualisiert einen Arbeitsknoten mit dem Namen "Node1" und der Adresse "Host1:9090":

```
infasetup UpdateWorkerNode -nn Node1 -na Host1:9090
```

Wenn Sie eine der erforderlichen Optionen weglassen oder falsch eingeben, schlägt der Befehl fehl und von *infasetup* wird eine Fehlermeldung zurückgegeben.

infasetup Befehlsreferenz

infasetup gibt die erfolgreiche oder fehlgeschlagene Ausführung eines Befehls mit einem Rückgabewert an. Rückgabewert (0) gibt an, dass der Befehl erfolgreich ausgeführt wurde. Rückgabewert (-1) gibt an, dass der Befehl fehlgeschlagen ist.

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

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

Verwenden von Datenbankverbindungsstrings

Einige *infasetup*-Befehle verwenden Verbindungsstrings, um eine Verbindung zur Domänen-Konfigurationsdatenbank herzustellen. Geben Sie den Host, Port und Dienstnamen der Datenbank als Teil des Verbindungsstrings an.

Sie können Verbindungsstrings mit den folgenden *infasetup*-Befehlen verwenden:

- BackupDomain
- DefineDomain
- DefineGatewayNode
- DeleteDomain
- RestoreDomain
- UpdateGatewayNode

In der folgenden Tabelle finden Sie eine Auflistung der Verbindungsstringsyntax für die einzelnen unterstützten Datenbanken:

Datenbankname	Verbindungsstring

Oracle	Oracle:
	`jdbc:informatica:oracle://host_name:port;SID=sid`
	Oracle RAC:
	`jdbc:informatica:oracle://host_name:port; ServiceName=[Service Name];AlternateServers=(server2:port);LoadBalancing=true`

Microsoft SQL Server	`jdbc:informatica:sqlserver://host_name:port; SelectMethod=cursor;DatabaseName=database_name`
IBM DB2	`jdbc:informatica:db2://host_name:port; DatabaseName=database_name`

BackupDomain

Sichert die Konfigurationsmetadaten für die Domäne. infasetup speichert die Metadaten der Backup-Domäne in einer Sicherungsdatei mit der Endung „mrep".

Beim Ausführen dieses Befehls sichert *infasetup* die Datenbanktabellen für die Domänenkonfiguration. Zum Wiederherstellen der Domäne in einer anderen Datenbank müssen Sie die Inhalte der Tabelle ISP_RUN_LOG manuell sichern, um die vorherigen Arbeitsablauf- und Sitzungsprotokolle zu erhalten.

Wenn der Befehl mit einem Java-Speicherfehler fehlschlägt, stellen Sie für „infasetup" mehr Systemspeicher zur Verfügung. Um mehr Systemspeicher zur Verfügung zu stellen, geben Sie den -Xmx-Wert in der Umgebungsvariable INFA_JAVA_CMD_OPTS an.

Der Befehl „BackupDomain" verwendet die folgende Syntax:

```
BackupDomain

<<-DatabaseAddress|-da> database_hostname:database_port|

<-DatabaseConnectionString|-cs> database_connection_string>

[<-DatabaseUserName|-du> database_user_name]
```

```
[<-DatabasePassword|-dp> database_password]

<-DatabaseType|-dt> database_type

[<-DatabaseServiceName|-ds> database_service_name]

<-BackupFile|-bf> backup_file_name

[<-Force|-f> overwrite_file]

[<-Tablespace|-ts> tablespace_name]

[<-SchemaName|-sc> schema_name (used for Microsoft SQL Server only)]

<-DomainName|-dn> domain_name

[<-DatabaseTlsEnabled|-dbtls> database_tls_enabled]

[<-DatabaseTruststorePassword|-dbtp> database_truststore_password]

[<-TrustedConnection|-tc> trusted_connection (used for Microsoft SQL Server only)]

[<-EncryptionKeyLocation|-kl> encryption_key_location]

[<-DatabaseTruststoreLocation|-dbtl> database_truststore_location]
```

In der folgenden Tabelle werden Optionen und Argumente für „*infasetup* BackupDomain“ beschrieben:

Option	Argument	Beschreibung
-DatabaseAddress -da	database_hostname:database_port	Erforderlich, wenn Sie die Option -DatabaseConnectionString (-cs) nicht verwenden. Name und Portnummer des Computers, auf dem die Konfigurationsdatenbank der Domäne gehostet wird.
-DatabaseConnectionString -cs	database_connection_string	Erforderlich, wenn Sie die Optionen -DatabaseAddress (-da) und -DatabaseServiceName (-ds) nicht verwenden. Verbindungsstring, der zum Herstellen einer Verbindung zur Konfigurationsdatenbank der Domäne verwendet wird. Geben Sie den Namen des Datenbankhosts, -ports und -diensts als Teil des Verbindungsstrings ein. Setzen Sie den Verbindungsstring zwischen Anführungszeichen.
-DatabaseUserName -du	database_user_name	Erforderlich, wenn Sie die Option -TrustedConnection (-tc) nicht verwenden. Konto für die Datenbank, die die Domänenkonfigurationsinformationen enthält.
-DatabasePassword -dp	database_password	Passwort aus der Datenbank für die Domänenkonfiguration des Datenbankbenutzers. Wenn Sie diese Option weglassen, verwendet *infasetup* das in der Umgebungsvariable INFA_DEFAULT_DATABASE_PASSWORD angegebene Passwort. Wird in der Umgebungsvariable kein Wert angegeben, müssen Sie ein Passwort unter Verwendung dieser Option eingeben.

Option	Argument	Beschreibung
-DatabaseType -dt	database_type	Erforderlich. Typ der Datenbank, in der die Metadaten der Domänenkonfiguration gespeichert werden. Zu den Datenbanktypen gehören: - db2 - oracle - mssqlserver - sybase
-DatabaseServiceName -ds	database_service_name	Erforderlich, wenn Sie die Option -DatabaseConnectionString (-cs) nicht verwenden. Der Name des Datenbankdiensts. Erforderlich für Oracle-, IBM DB2- und Microsoft SQL Server-Datenbanken. Geben Sie die SID für Oracle, den Dienstnamen für IBM DB2 oder den Datenbanknamen für Microsoft SQL Server ein.
-BackupFile -bf	backup_file_name	Erforderlich. Name und Pfad der Backup-Datei. Wenn Sie keinen Dateipfad angeben, erstellt *infasetup* die Backup-Datei im aktuellen Verzeichnis.
-Force -f	-	Optional. Überschreibt die Backup-Datei, wenn eine Datei mit demselben Namen bereits vorhanden ist.
-DomainName -dn	domain_name	Erforderlich. Name der Domäne.
-Tablespace -ts	tablespace_name	Erforderlich für eine IBM DB2-Datenbank. Name des Tablespace, in dem sich die Datenbanktabellen für die Domänenkonfiguration befinden.
-SchemaName -sc	schema_name	Optional. Name des Microsoft SQL Server-Schemas. Geben Sie einen Schemanamen ein, wenn Sie nicht das Standardschema verwenden.
-DatabaseTlsEnabled -dbtls	database_tls_enabled	Optional. Gibt an, ob die Informatica-Domänendatenbank mit TLS und SSL sicher ist. Setzen Sie diese Option für die sichere Datenbank auf True. Standardwert ist „False“. Wenn Sie die Option -dbtls ohne Wert angegeben wird, verwendet die Informatica-Domäne die sichere Kommunikation mit der Informatica-Domänendatenbank.
-DatabaseTruststorePassword -dbtp	database_truststore_password	Optional. Passwort für die Datenbank-Truststore-Datei für die sichere Datenbank.
-TrustedConnection -tc	-	Optional. Stellen Sie eine Verbindung zur Microsoft SQL Server-Datenbank über eine vertrauenswürdige Verbindung her. Die vertrauenswürdige Authentifizierung verwendet die Windows-Sicherheitsanmeldedaten des aktuellen Benutzers, um eine Verbindung zu Microsoft SQL Server herzustellen.

Option	Argument	Beschreibung
-EncryptionKeyLocation -kl	encryption_key_location	Verzeichnis, das den aktuellen Verschlüsselungsschlüssel enthält. Der Name der Verschlüsselungsdatei lautet sitekey.
-DatabaseTruststoreLocation -dbtl	database_truststore_location	Pfad und Dateiname der Truststore-Datei für die sichere Domänenrepository-Datenbank. Erforderlich, wenn Sie eine sichere Domänenrepository-Datenbank für die Domäne konfigurieren.

DefineDomain

Erstellt eine Domäne auf dem aktuellen Computer. Wenn Sie eine Domäne auf einem Computer definieren, auf dem eine Domäne gehostet wird, müssen Sie zuerst die Informatica-Dienste auf dem Computer beenden. Infasetup entfernt die vorhandenen Domänen- und Knoteneinstellungen. Starten Sie nach dem Definieren der neuen Domäne die Informatica-Dienste neu.

Zum Erstellen einer Domäne auf einem Windows-Computer müssen Sie zuerst den Hostport öffnen oder die Firewall deaktivieren.

Geben Sie im Anschluss an die Option (-f) im Befehl DefineDomain keine weiteren Zeichen ein. Wenn Sie zusätzliche Zeichen eingeben, schlägt *infasetup* unter Umständen mit einem unerwarteten Fehler fehl.

Der Befehl „DefineDomain“ verwendet die folgende Syntax:

```
DefineDomain
<<-DatabaseAddress|-da> database_hostname:database_port|
<-DatabaseConnectionString|-cs> database_connection_string>
[<-DatabaseUserName|-du> database_user_name]
[<-DatabasePassword|-dp> database_password]
<-DatabaseType|-dt> database_type ORACLE|DB2|MSSQLSERVER|SYBASE
[<-DatabaseServiceName|-ds> database_service_name]
[<-Tablespace|-ts> tablespace_name]
[<-SchemaName|-sc> schema_name (used for MSSQLServer 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]
[<-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]
[<-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]
```

In der folgenden Tabelle werden die Optionen und Argumente für „*infasetup* DefineDomain“ beschrieben:

Option	Argument	Beschreibung
-DatabaseAddress -da	database_hostname:database_port	Erforderlich, wenn Sie die Option -DatabaseConnectionString (-cs) nicht verwenden. Name und Portnummer des Computers, auf dem die Konfigurationsdatenbank der Domäne gehostet wird.
-DatabaseConnectionString -cs	database_connection_string	Erforderlich, wenn Sie die Optionen -DatabaseAddress (-da) und -DatabaseServiceName (-ds) nicht verwenden. Verbindungszeichenfolge, die zum Herstellen einer Verbindung zur Konfigurationsdatenbank der Domäne verwendet wird. Geben Sie den Namen des Datenbankhosts, -ports und -diensts als Teil der Verbindungszeichenfolge ein. Setzen Sie die Verbindungszeichenfolge in Anführungszeichen.
-DatabaseUserName -du	database_user_name	Erforderlich, wenn Sie die Option -TrustedConnection (-tc) nicht verwenden. Konto für die Datenbank, die die Domänenkonfigurationsinformationen enthält

Option	Argument	Beschreibung
-DatabasePassword -dp	database_password	Passwort aus der Datenbank für die Domänenkonfiguration des Datenbankbenutzers. Wenn Sie diese Option weglassen, verwendet *infasetup* das in der Umgebungsvariable INFA_DEFAULT_DATABASE_PASSWORD angegebene Passwort. Wenn in der Umgebungsvariable kein Wert angegeben ist, müssen Sie mithilfe dieser Option ein Passwort eingeben.
-DatabaseType -dt	database_type	Erforderlich. Typ der Datenbank, der die Domänenkonfigurations-Metadaten speichert Zu den Datenbanktypen gehören: - db2 - oracle - mssqlserver - sybase
-DatabaseServiceName -ds	database_service_name	Erforderlich, wenn Sie die Option -DatabaseConnectionString (-cs) nicht verwenden. Der Name des Datenbankdiensts. Erforderlich für Oracle-, IBM DB2- und Microsoft SQL Server-Datenbanken. Geben Sie die SID für Oracle, den Dienstnamen für IBM DB2 oder den Datenbanknamen für Microsoft SQL Server ein.
-Tablespace -ts	tablespace_name	Erforderlich für eine IBM DB2-Datenbank. Name des Tablespace, in dem sich die Datenbanktabellen für die Domänenkonfiguration befinden.
-SchemaName -sc	schema_name	Optional. Name des Microsoft SQL Server-Schemas. Geben Sie einen Schemanamen ein, wenn Sie nicht das Standardschema verwenden.

Option	Argument	Beschreibung
-DatabaseTlsEnabled -dbtls	database_tls_enabled	Optional. Gibt an, ob die Informatica-Domänendatenbank mit TLS und SSL sicher ist. Setzen Sie diese Option für die sichere Datenbank auf True. Standardwert ist „False“. Wenn die Option -dbtls ohne Wert angegeben wird, verwendet die Informatica-Domäne die sichere Kommunikation mit der Informatica-Domänendatenbank.
-DatabaseTruststorePassword -dbtp	database_truststore_password	Optional. Passwort für die Datenbank-Truststore-Datei für die sichere Datenbank.
-DomainName -dn	domain_name	Erforderlich. Name der Domäne. Domänennamen müssen zwischen 1 und 79 Zeichen umfassen und dürfen weder Leerzeichen noch die folgenden Zeichen enthalten: / * ? < > " |
-DomainDescription -de	domain_description	Optional. Beschreibung der Domäne.
-AdministratorName -ad	administrator_name	Erforderlich. Benutzername des Domänenadministrators.
-Password -pd	password	Optional für Kerberos-Domäne. Passwort des Domänenadministrators. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-LicenseName -ln	license_name	Optional. Name der Lizenz. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf maximal 79 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten: / * ? < > " |
-LicenseKeyFile -lf	license_key_file	Optional. Pfad zur Lizenzschlüsseldatei.
-LogServiceDirectory -ld	log_service_directory	Erforderlich. Freigegebener Verzeichnispfad, der vom Protokollmanager zum Speichern von Protokollereignisdateien verwendet wird.
-SystemLogDirectory -sld	system_log_directory	Optional. Verzeichnispfad zum Speichern von Systemprotokolldateien. Standard ist <INFA_home>/logs.
-NodeName -nn	node_name	Erforderlich. Name des Knotens. Knotennamen müssen zwischen 1 und 79 Zeichen umfassen und dürfen weder Leerzeichen noch die folgenden Zeichen enthalten:\ / * ? < > " |
-NodeAddress -na	node_host:port	Erforderlich. Hostname und Portnummer für den Computer, auf dem der Knoten gehostet wird. Wählen Sie eine verfügbare Portnummer aus.
-ServiceManagerPort -sp	service_manager_port	Optional. Portnummer, die vom Dienstmanager verwendet wird, um auf eingehende Verbindungsanfragen zu reagieren.

Option	Argument	Beschreibung
-EnableTLS -tls	enable_tls	Optional. Konfiguriert die sichere Kommunikation für die Dienste in der Informatica-Domäne. Wenn Sie die standardmäßigen, von Informatica bereitgestellten SSL-Zertifikate verwenden, müssen Sie die Schlüsselspeicher- und Truststore-Optionen nicht angeben. Wenn Sie das SSL-Zertifikat nicht verwenden, müssen Sie die Keystore- und Truststore-Optionen angeben. Gültige Werte sind „True“ oder „False“. Standardwert ist „False“. Wenn Sie die Option -tls ohne Wert angeben, verwendet die Informatica-Domäne die sichere Kommunikation zwischen Diensten. Zum Aktivieren der sicheren Kommunikation für die verbundenen Dienste oder Webanwendungen, z. B. das Administrator-Tool, das Analyst-Tool oder den Webdienst-Hub, konfigurieren Sie die sichere Kommunikation separat innerhalb der Anwendungen.

Option	Argument	Beschreibung
-NodeKeystore- -nk	node_keystore_directory	Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Erforderlich, wenn Sie Ihre SSL-Zertifikate verwenden. Verzeichnis, das die Schlüsselspeicherdateien enthält. Für die Informatica-Domäne müssen die SSL-Zertifikate im PEM-Format und in JKS-Dateien (Java Keystore) vorliegen. Das Verzeichnis muss Schlüsselspeicherdateien in den Formaten PEM und JKS enthalten. Die Schlüsselspeicherdateien müssen infa_keystore.jks und infa_keystore.pem lauten. Wenn die Schlüsselspeicherdatei, die Sie von der Zertifizierungsstelle erhalten, einen anderen Namen hat, müssen Sie sie in infa_keystore.jks und infa_keystore.pem umbenennen. Sie müssen für alle Knoten in der Domäne dieselben Schlüsselspeicherzertifikate verwenden.
-NodeKeystorePass -nkp	node_keystore_password	Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Erforderlich, wenn Sie Ihre SSL-Zertifikate verwenden. Passwort für die Schlüsselspeicherdatei infa_keystore.jks.

Option	Argument	Beschreibung
-NodeTruststore -nt	node_truststore_directory	Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Verzeichnis, das die Truststore-Dateien enthält. Für die Informatica-Domäne müssen die SSL-Zertifikate im PEM-Format und in JKS-Dateien (Java Keystore) vorliegen. Das Verzeichnis muss Truststore-Dateien in den Formaten PEM und JKS enthalten. Die Truststore-Dateien müssen die Namen infa_truststore.jks und infa_truststore.pem aufweisen. Wenn die Truststore-Datei, die Sie von der Zertifizierungsstelle erhalten haben, einen anderen Namen aufweist, müssen Sie sie in infa_truststore.jks und infa_truststore.pem umbenennen.
-NodeTruststorePass -ntp	node_truststore_password	Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Erforderlich, wenn Sie Ihre SSL-Zertifikate verwenden. Passwort für die infa_truststore.jks-Datei.
-EnableKerberos -krb	enable_kerberos	Optional. Konfiguriert die Informatica-Domäne zur Verwendung der Kerberos-Authentifizierung. Gültige Werte sind „True“ oder „False“. Bei True verwendet die Domäne die Kerberos-Authentifizierung, dann können Sie den Authentifizierungsmodus später nicht ändern. Nachdem Sie die Kerberos-Authentifizierung aktiviert haben, können Sie sie nicht deaktivieren. Standardwert ist „False“. Wenn Sie die Option -krb ohne einen Wert angeben, verwendet die Informatica-Domäne die Kerberos-Authentifizierung.

Option	Argument	Beschreibung
-ServiceRealmName -srn	realm_name_of_node_spn	Optional. Name des Kerberos-Bereichs, zu dem die Informatica-Domänendienste gehören. Stellen Sie sicher, dass Sie den gleichen Wert als -urn für die Kerberos-Authentifizierung angeben.
-UserRealmName -urn	realm_name_of_user_spn	Optional. Name des Kerberos-Bereichs, zu dem die Informatica-Domänenbenutzer gehören. Stellen Sie sicher, dass Sie den gleichen Wert als -srn für die Kerberos-Authentifizierung angeben.
-KeysDirectory -kd	Infa_keys_directory_location	Optional. Verzeichnis, in dem alle Schlüsseltabellendateien und der Verschlüsselungsschlüssel für die Informatica-Domäne gespeichert werden. Standardwert ist `<Informatica-Installationsverzeichnis>/isp/config/keys`.

Option	Argument	Beschreibung
-SPNShareLevel -spnSL	SPNShareLevel PROCESS |NODE	Optional. Gibt die Dienst-Prinzipalebene für die Domäne an. Legen Sie eine der folgenden Ebenen für die Eigenschaft fest: - Prozess Die Domäne erfordert einen eindeutigen Dienst-Prinzipalnamen (SPN) und eine Keytab-Datei für jeden Knoten und für jeden Dienst auf einem Knoten. Die Anzahl der für jeden Knoten erforderlichen SPNs und Keytab-Dateien hängt von der Anzahl der Dienstprozesse ab, die auf dem Knoten ausgeführt werden. Verwenden Sie die Knotenebenen-Option, wenn die Domäne keine hohe Sicherheitsstufe erfordert. - Knoten. Die Domäne verwendet einen SPN und eine Keytab-Datei für den Knoten und für alle Dienste, die auf dem Knoten ausgeführt werden. Sie erfordert außerdem einen separaten SPN und eine separate Keytab-Datei für alle HTTP-Prozesse auf dem Knoten. Standardwert ist „Prozess“.
-AdminconsolePort -ap	admin_tool_port	Port für den Zugriff auf Informatica Administrator.
-HttpsPort -hs	admin_tool_https_port	Optional. Portnummer zum Sichern der Verbindung zum Administrator-Tool. Geben Sie diese Portnummer an, wenn Sie HTTPS für einen Knoten konfigurieren möchten.
-KeystoreFile -kf	admin_tool_file_location	Optional. Schlüsselspeicherdatei, in der die Schlüssel und Zertifikate enthalten sind, die bei Verwendung des SSL-Protokolls erforderlich sind

Option	Argument	Beschreibung
-KeystorePass -kp	admin_tool_keystore_password	Optional. Ein Volltext-Passwort für die Schlüsselspeicherdatei. Sie können ein Passwort mit der Option -kp oder der Umgebungsvariable INFA_PASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -kp festgelegte Passwort Vorrang.
-MinProcessPort -mi	minimum_port	Erforderlich. Kleinste Portnummer für die Anwendungsdienstprozesse, die auf dem Knoten ausgeführt werden.
-MaxProcessPort -ma	maximum_port	Erforderlich. Größte Portnummer für die Anwendungsdienstprozesse, die auf dem Knoten ausgeführt werden.
-ServerPort -sv	server_shutdown_port	Optional. Vom Dienstmanager verwendete TCP/IP-Portnummer. Der Dienstmanager verwaltet Befehle zum Herunterfahren aus Domänenkomponenten auf diesem Port. Legen Sie diese Portnummer fest, wenn sich auf einem Computer mehrere Knoten befinden oder die Standardportnummer verwendet wird. Als Standardwert fungiert die Portnummer des Knotens plus eins.
-AdminconsoleShutdownPort -asp	admin_tool_shutdown_port	Portnummer, die das Herunterfahren für Informatica Administrator steuert.
-BackupDirectory -bd	backup_directory	Optional. Verzeichnis zum Speichern der Repository-Backup-Dateien. Der Zugriff auf das Verzeichnis muss über den Knoten möglich sein.

Option	Argument	Beschreibung
-ServiceResilienceTimeout -sr	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der *infasetup* versucht, eine Verbindung zur lokalen Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet *infasetup* den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben ist, wird der Standardwert von 180 Sekunden verwendet.
-ErrorLogLevel -el	fatal error warning info trace debug	Optional. Schweregradstufe für Protokollereignisse im Domänenprotokoll. Standardwert ist „info“.
-ResourceFile -rf	resource_file	Erforderlich. Datei, die eine Liste der verfügbaren Ressourcen für den Knoten enthält. Verwenden Sie die Datei „nodeoptions.xml“, die sich an folgendem Speicherort befindet: `<INFA_HOME>/isp/bin`
-TimeZone -tz	log_service_timezone_GMT+00:00	Optional. Zeitzone, die vom Protokollmanager beim Erzeugen von Protokollereignisdateien verwendet wird. Standardwert ist GMT +00:00. Konfigurieren Sie die Zeitzone in folgendem Format: `GMT(+/-)hh:mm`
-Force -f	-	Optional. Überschreibt die Datenbank, wenn eine Datenbank mit demselben Namen bereits vorhanden ist. Geben Sie im Anschluss an diese Option keine weiteren Zeichen ein.

Option	Argument	Beschreibung
-TrustedConnection -tc	-	Optional. Stellen Sie eine Verbindung zur Microsoft SQL Server-Datenbank über eine vertrauenswürdige Verbindung her. Die vertrauenswürdige Authentifizierung verwendet die Windows-Sicherheitsanmeldedaten des aktuellen Benutzers, um eine Verbindung zu Microsoft SQL Server herzustellen. **Hinweis:** Wenn Sie eine vertrauenswürdige Verbindung verwenden, konfigurieren Sie die Option DatabaseConnectionString.
-DatabaseTruststoreLocation -dbtl	database_truststore_location	Pfad und Dateiname der Truststore-Datei für die sichere Domänenrepository-Datenbank. Erforderlich, wenn Sie eine sichere Domänenrepository-Datenbank für die Domäne konfigurieren.

Wenn Sie DefineDomain auf einem Knoten ausführen, auf dem aktuell eine Domäne gehostet wird, konfigurieren Sie die folgenden Domäneneigenschaften neu:

- **Anwendungsdienste.** Erstellen Sie einen beliebigen Anwendungsdienst neu, der in der Domäne ausgeführt wurde.
- **Benutzer.** Erstellen Sie Benutzer neu.
- **Gateway-Knoten.** Konfigurieren Sie Gateway-Knoten in der Domäne.
- **Allgemeine Domäneneigenschaften.** Konfigurieren Sie Belastbarkeits-Timeout und die maximale Anzahl von Neustartversuchen für die Domäne.
- **Gitter.** Erstellen Sie ein beliebiges Gitter in der Domäne neu.
- **LDAP-Authentifizierung**. Konfigurieren Sie LDAP-Authentifizierung für die Domäne.
- **Log Manager-Eigenschaften.** Konfigurieren Sie den freigegebenen Verzeichnispfad, die Bereinigen-Eigenschaften und die Zeitzone des Log Managers.

Wenn Sie den Hostnamen oder die Portnummer des Gateway-Knotens ändern, müssen Sie darüber hinaus jeden Knoten unter Verwendung des *infacmd* AddDomainNode-Befehls zur Domäne hinzufügen.

DefineGatewayNode

Definiert einen Gateway-Knoten auf dem aktuellen Computer. Dieser Befehl überschreibt die Datei nodemeta.xml, welche die Konfigurationsmetadaten für den Knoten speichert. Nachdem Sie den Knoten

definiert haben, führen Sie den Befehl infacmd isp AddDomainNode aus, um den Knoten zur Domäne hinzuzufügen.

Der Befehl „DefineGatewayNode“ verwendet die folgende Syntax:

```
DefineGatewayNode

<-DatabaseAddress|-da> database_hostname:database_port|
<-DatabaseConnectionString|-cs> database_connection_string>
[<-DatabaseUserName|-du> database_user_name]
[<-DatabasePassword|-dp> database_password]
<-DatabaseType|-dt> database_type ORACLE|DB2|MSSQLSERVER|SYBASE
[<-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]
[<-EnableKerberos|-krb> enable_kerberos]
[<-ServiceRealmName|-srn> realm_name_of_node_spn]
[<-UserRealmName|-urn> realm_name_of_user_spn]
[<-KeysDirectory|-kd> Infa_keys_directory_location]
[<-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 only)]
[<-DatabaseTlsEnabled|-dbtls> database_tls_enabled]
[<-DatabaseTruststorePassword|-dbtp> database_truststore_password]
[<-TrustedConnection|-tc> trusted_connection (used for MSSQLServer only)]
[<-DatabaseTruststoreLocation|-dbtl> database_truststore_location]
```

In der folgenden Tabelle werden die Optionen und Argumente für „*infasetup* DefineGatewayNode“ beschrieben:

Option	Argument	Beschreibung
-DatabaseAddress -da	database_hostname:database_port	Erforderlich, wenn Sie die Option -DatabaseConnectionString (-cs) nicht verwenden. Name und Portnummer des Computers, auf dem die Konfigurationsdatenbank der Domäne gehostet wird.
-DatabaseConnectionString -cs	database_connection_string	Erforderlich, wenn Sie die Optionen -DatabaseAddress (-da) und -DatabaseServiceName (-ds) nicht verwenden. Verbindungszeichenfolge, die zum Herstellen einer Verbindung zur Konfigurationsdatenbank der Domäne verwendet wird. Geben Sie den Namen des Datenbankhosts, -ports und -diensts als Teil der Verbindungszeichenfolge ein. Setzen Sie die Verbindungszeichenfolge in Anführungszeichen.
-DatabaseUserName -du	database_user_name	Erforderlich, wenn Sie die Option -TrustedConnection (-tc) nicht verwenden. Konto für die Datenbank, die die Domänenkonfigurationsinformationen enthält.
-DatabasePassword -dp	database_password	Passwort aus der Datenbank für die Domänenkonfiguration des Datenbankbenutzers. Wenn Sie diese Option weglassen, verwendet *infasetup* das in der Umgebungsvariable INFA_DEFAULT_DATABASE_PASSWORD angegebene Passwort. Wird in der Umgebungsvariable kein Wert angegeben, müssen Sie ein Passwort unter Verwendung dieser Option eingeben.
-DatabaseType -dt	database_type	Erforderlich. Typ der Datenbank, in der die Domänenkonfigurationsmetadaten gespeichert werden. Zu den Datenbanktypen gehören: - db2 - oracle - mssqlserver - sybase
-DatabaseServiceName -ds	database_service_name	Erforderlich, wenn Sie die Option -DatabaseConnectionString (-cs) nicht verwenden. Der Name des Datenbankdiensts. Erforderlich für Oracle-, IBM DB2- und Microsoft SQL Server-Datenbanken. Geben Sie die SID für Oracle, den Dienstnamen für IBM DB2 oder den Datenbanknamen für Microsoft SQL Server ein.
-DomainName -dn	domain_name	Erforderlich. Name der Domäne.

Option	Argument	Beschreibung
-NodeName -nn	node_name	Optional. Name des Knotens. Knotennamen müssen zwischen 1 und 79 Zeichen umfassen und dürfen weder Leerzeichen noch die folgenden Zeichen enthalten:\ / * ? < > " |
-NodeAddress -na	node_host:port	Optional. Hostname und Portnummer für den Computer, auf dem der Knoten gehostet wird. Wählen Sie eine verfügbare Portnummer aus.
-ServiceManagerPort -sp	service_manager_port	Optional. Portnummer, die vom Dienstmanager verwendet wird, um auf eingehende Verbindungsanfragen zu reagieren.
-EnableTLS -tls	enable_tls	Optional. Konfiguriert die sichere Kommunikation für die Dienste in der Informatica-Domäne. Wenn Sie die standardmäßigen, von Informatica bereitgestellten SSL-Zertifikate verwenden, müssen Sie die Schlüsselspeicher- und Truststore-Optionen nicht angeben. Wenn Sie das SSL-Zertifikat nicht verwenden, müssen Sie die Keystore- und Truststore-Optionen angeben. Gültige Werte sind „True“ oder „False“. Standardwert ist „False“. Wenn Sie die Option -tls ohne Wert angeben, verwendet die Informatica-Domäne die sichere Kommunikation zwischen Diensten. Zum Aktivieren der sicheren Kommunikation für die verbundenen Dienste oder Webanwendungen, z. B. das Administrator Tool, das Analyst Tool oder den Webdienst-Hub, konfigurieren Sie die sichere Kommunikation separat innerhalb der Anwendungen.
-NodeKeystore -nk	node_keystore_directory	Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Erforderlich, wenn Sie Ihre SSL-Zertifikate verwenden. Verzeichnis, das die Schlüsselspeicherdateien enthält. Für die Informatica-Domäne müssen die SSL-Zertifikate im PEM-Format und in JKS-Dateien (Java Keystore) vorliegen. Das Verzeichnis muss Schlüsselspeicherdateien in den Formaten PEM und JKS enthalten. Die Schlüsselspeicherdateien müssen infa_keystore.jks und infa_keystore.pem lauten. Wenn die Schlüsselspeicherdatei, die Sie von der Zertifizierungsstelle erhalten, einen anderen Namen hat, müssen Sie sie in infa_keystore.jks und infa_keystore.pem umbenennen. Sie müssen für alle Knoten in der Domäne dieselben Schlüsselspeicherzertifikate verwenden.

Option	Argument	Beschreibung
-NodeKeystorePass -nkp	node_keystore_password	Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Erforderlich, wenn Sie Ihre SSL-Zertifikate verwenden. Passwort für die Schlüsselspeicherdatei infa_keystore.jks.
-NodeTruststore -nt	node_truststore_directory	Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Erforderlich, wenn Sie Ihre SSL-Zertifikate verwenden. Verzeichnis, das die Truststore-Dateien enthält. Für die Informatica-Domäne müssen die SSL-Zertifikate im PEM-Format und in JKS-Dateien (Java Keystore) vorliegen. Das Verzeichnis muss Truststore-Dateien in den Formaten PEM und JKS enthalten. Die Truststore-Dateien müssen die Namen infa_truststore.jks und infa_truststore.pem aufweisen. Wenn die Truststore-Datei, die Sie von der Zertifizierungsstelle erhalten haben, einen anderen Namen aufweist, müssen Sie sie in infa_truststore.jks und infa_truststore.pem umbenennen.
-NodeTruststorePass -ntp	node_truststore_password	Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Erforderlich, wenn Sie Ihre SSL-Zertifikate verwenden. Passwort für die infa_truststore.jks-Datei.
-EnableKerberos -krb	enable_kerberos	Optional. Konfiguriert die Informatica-Domäne zur Verwendung der Kerberos-Authentifizierung. Gültige Werte sind „True“ oder „False“. Bei True verwendet die Domäne die Kerberos-Authentifizierung, dann können Sie den Authentifizierungsmodus später nicht ändern. Nachdem Sie die Kerberos-Authentifizierung aktiviert haben, können Sie sie nicht deaktivieren. Standardwert ist „False“. Wenn Sie die Option -krb ohne einen Wert angeben, verwendet die Informatica-Domäne die Kerberos-Authentifizierung.
-ServiceRealmName -srn	realm_name_of_node_spn	Optional. Name des Kerberos-Bereichs, zu dem die Informatica-Domänendienste gehören. Stellen Sie sicher, dass Sie den gleichen Wert als -urn für die Kerberos-Authentifizierung angeben.
-UserRealmName -urn	realm_name_of_user_spn	Optional. Name des Kerberos-Bereichs, zu dem die Informatica-Domänenbenutzer gehören. Stellen Sie sicher, dass Sie den gleichen Wert als -srn für die Kerberos-Authentifizierung angeben.

Option	Argument	Beschreibung
-KeysDirectory -kd	Infa_keys_directory_location	Optional. Verzeichnis, in dem alle Schlüsseltabellendateien und der Verschlüsselungsschlüssel für die Informatica-Domäne gespeichert werden. Standardwert ist `<Informatica-Installationsverzeichnis>/isp/config/keys`.
-AdminconsolePort -ap	admin_tool_port	Optional. Port für den Zugriff auf Informatica Administrator.
-HttpsPort -hs	admin_tool_https_port	Optional. Portnummer, die vom Knoten für die Kommunikation zwischen dem Administrator Tool und dem Dienstmanager verwendet wird. Geben Sie diese Portnummer an, wenn Sie HTTPS für einen Knoten konfigurieren möchten. Zum Deaktivieren von HTTPS-Unterstützung für einen Knoten setzen Sie diese Portnummer auf Null.
-KeystoreFile -kf	admin_tool_keystore_file_location	Optional. Schlüsselspeicherdatei, in der die Schlüssel und Zertifikate enthalten sind, die bei Verwendung des SSL-Protokolls erforderlich sind
-KeystorePass -kp	admin_tool_keystore_password	Optional. Ein Volltext-Passwort für die Schlüsselspeicherdatei. Sie können ein Passwort mit der Option -kp oder der Umgebungsvariable INFA_PASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -kp festgelegte Passwort Vorrang.
-MinProcessPort -mi	minimum_port	Optional. Kleinste Portnummer für die Anwendungsdienstprozesse, die auf dem Knoten ausgeführt werden. Standardwert ist 11000.
-MaxProcessPort -ma	maximum_port	Optional. Größte Portnummer für die Anwendungsdienstprozesse, die auf dem Knoten ausgeführt werden. Standardwert ist 11999.
-LogServiceDirectory -ld	log_service_directory	Optional. Freigegebener Verzeichnispfad, der vom Protokollmanager zum Speichern von Protokollereignisdateien verwendet wird.
-SystemLogDirectory -sld	system_log_directory	Optional. Verzeichnispfad zum Speichern von Systemprotokolldateien. Standardwert ist <INFA_home>/logs.

Option	Argument	Beschreibung
-ServerPort -sv	server_shutdown_port	Optional. Vom Dienstmanager verwendete TCP/IP-Portnummer. Der Dienstmanager verwaltet Befehle zum Herunterfahren aus PowerCenter-Komponenten auf diesem Port. Legen Sie diese Portnummer fest, wenn sich auf einem Computer mehrere Knoten befinden oder die Standardportnummer verwendet wird. Standardwert ist 8005.
-AdminconsoleShutdownPort -asp	admin_tool_shutdown_port	Optional. Portnummer, die das Herunterfahren für Informatica Administrator steuert.
-BackupDirectory -bd	backup_directory	Optional. Verzeichnis zum Speichern der Repository-Backup-Dateien. Der Zugriff auf das Verzeichnis muss über den Knoten möglich sein.
-ErrorLogLevel -el	fatal error warning info trace debug	Optional. Schweregradstufe für Protokollereignisse im Domänenprotokoll. Standardwert ist „info“.
-ResourceFile -rf	resource_file	Erforderlich. Datei, die eine Liste der verfügbaren Ressourcen für den Knoten enthält. Verwenden Sie die Datei „nodeoptions.xml“, die sich in folgendem Verzeichnis befindet: `<INFA_HOME>\isp\bin`.
-Tablespace -ts	tablespace_name	Erforderlich für eine IBM DB2-Datenbank. Name des Tablespace, in dem sich die Datenbanktabellen für die Domänenkonfiguration befinden.
-SchemaName -sc	schema_name	Optional. Name des Microsoft SQL Server-Schemas. Geben Sie einen Schemanamen ein, wenn Sie nicht das Standardschema verwenden.
-DatabaseTlsEnabled -dbtls	database_tls_enabled	Optional. Gibt an, ob die Informatica-Domänendatenbank mit TLS und SSL sicher ist. Setzen Sie diese Option für die sichere Datenbank auf True. Standardwert ist „False“. Wenn die Option „-dbtls“ ohne Wert angegeben wird, verwendet die Informatica-Domäne die sichere Kommunikation mit der Informatica-Domänendatenbank.
-DatabaseTruststorePassword -dbtp	database_truststore_password	Optional. Passwort für die Datenbank-Truststore-Datei für die sichere Datenbank.

Option	Argument	Beschreibung
-TrustedConnection -tc	n/v	Optional. Stellen Sie eine Verbindung zur Microsoft SQL Server-Datenbank über eine vertrauenswürdige Verbindung her. Die vertrauenswürdige Authentifizierung verwendet die Windows-Sicherheitsanmeldedaten des aktuellen Benutzers, um eine Verbindung zu Microsoft SQL Server herzustellen.
-DatabaseTruststoreLocation -dbtl	database_truststore_location	Pfad und Dateiname der Truststore-Datei für die sichere Domänenrepository-Datenbank. Erforderlich, wenn Sie eine sichere Domänenrepository-Datenbank für die Domäne konfigurieren.

Verwandte Themen:

- "AddDomainNode" auf Seite 248

DefineWorkerNode

Definiert einen Arbeitsknoten auf dem aktuellen Computer. Infasetup erstellt die Datei „nodemeta.xml", in der die Konfigurationsmetadaten für den Knoten gespeichert werden. Wenn Sie diesen Befehl auf einem vorhandenen Knoten ausführen, überschreibt er die Konfigurationsmetadaten des Knotens. Nachdem Sie den Knoten definiert haben, führen Sie den Befehl infacmd isp AddDomainNode aus, um den Knoten zur Domäne hinzuzufügen.

Der Befehl „DefineWorkerNode" verwendet die folgende Syntax:

```
DefineWorkerNode
<-DomainName|-dn> domain_name
<-NodeName|-nn> node_name
<-NodeAddress|-na> node_host:port
[<-ServiceManagerPort|-sp> service_manager_port]
[<-EnableTLS|-tls> enable_tls]
[<-NodeKeystore|-nk> node_keystore_directory]
[<-NodeKeystorePass|-nkp> node_keystore_password]
[<-NodeTruststore|-nt> node_truststore_directory]
[<-NodeTruststorePass|-ntp> node_truststore_password]
[<-EnableKerberos|-krb> enable_kerberos]
[<-ServiceRealmName|-srn> realm_name_of_node_spn]
[<-UserRealmName|-urn> realm_name_of_user_spn]
[<-KeysDirectory|-kd> Infa_keys_directory_location]
[<-HttpsPort|-hs> admin_tool_https_port]
[<-NodeKeystoreFile|-kf> admin_tool_keystore_file_location]
[<-KeystorePass|-kp> admin_tool_keystore_password]
<-GatewayAddress|-dg> domain_gateway_host:port
[<-UserName|-un> user_name]
[<-SecurityDomain|-sdn> security domain]
[<-Password|-pd> password]
[<-MinProcessPort|-mi> minimum_port]
[<-MaxProcessPort|-ma> maximum_port]
[<-ServerPort|-sv> server_shutdown_port]
[<-BackupDirectory|-bd> backup_directory]
[<-ErrorLogLevel|-el> FATAL_ERROR_WARNING_INFO_TRACE_DEBUG]
<-ResourceFile|-rf> resource_file
[<-SystemLogDirectory|-sld> system_log_directory]
```

In der folgenden Tabelle werden die Optionen und Argumente für „*infasetup* DefineWorkerNode“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Domäne, mit der der Arbeitsknoten verknüpft ist.
-NodeName -nn	node_name	Erforderlich. Name des Knotens. Knotennamen müssen zwischen 1 und 79 Zeichen umfassen und dürfen weder Leerzeichen noch die folgenden Zeichen enthalten:\ / * ? < > " |
-NodeAddress -na	node_host:port	Erforderlich. Hostname und Portnummer für den Computer, auf dem der Knoten gehostet wird. Wählen Sie eine verfügbare Portnummer aus.
-ServiceManagerPort -sp	service_manager_port	Optional. Portnummer, die vom Dienstmanager verwendet wird, um auf eingehende Verbindungsanfragen zu reagieren.
-EnableTLS -tls	enable_tls	Optional. Konfiguriert die sichere Kommunikation für die Dienste in der Informatica-Domäne. Wenn Sie die standardmäßigen, von Informatica bereitgestellten SSL-Zertifikate verwenden, müssen Sie die Schlüsselspeicher- und Truststore-Optionen nicht angeben. Wenn Sie das SSL-Zertifikat nicht verwenden, müssen Sie die Keystore- und Truststore-Optionen angeben. Gültige Werte sind „True“ oder „False“. Standardwert ist „False“. Wenn Sie die Option -tls ohne Wert angeben, verwendet die Informatica-Domäne die sichere Kommunikation zwischen Diensten. Zum Aktivieren der sicheren Kommunikation für die verbundenen Dienste oder Webanwendungen, z. B. das Administrator Tool, das Analyst Tool oder den Webdienst-Hub, konfigurieren Sie die sichere Kommunikation separat innerhalb der Anwendungen.
-NodeKeystore -nk	node_keystore_directory	Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Erforderlich, wenn Sie Ihre SSL-Zertifikate verwenden. Verzeichnis, das die Schlüsselspeicherdateien enthält. Für die Informatica-Domäne müssen die SSL-Zertifikate im PEM-Format und in JKS-Dateien (Java Keystore) vorliegen. Das Verzeichnis muss Schlüsselspeicherdateien in den Formaten PEM und JKS enthalten. Die Schlüsselspeicherdateien müssen infa_keystore.jks und infa_keystore.pem lauten. Wenn die Schlüsselspeicherdatei, die Sie von der Zertifizierungsstelle erhalten, einen anderen Namen hat, müssen Sie sie in infa_keystore.jks und infa_keystore.pem umbenennen. Sie müssen für alle Knoten in der Domäne dieselben Schlüsselspeicherzertifikate verwenden.
-NodeKeystorePass -nkp	node_keystore_password	Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Erforderlich, wenn Sie Ihre SSL-Zertifikate verwenden. Passwort für die Schlüsselspeicherdatei infa_keystore.jks.

Option	Argument	Beschreibung
-NodeTruststore -nt	node_truststore_directory	Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Verzeichnis, das die Truststore-Dateien enthält. Für die Informatica-Domäne müssen die SSL-Zertifikate im PEM-Format und in JKS-Dateien (Java Keystore) vorliegen. Das Verzeichnis muss Truststore-Dateien in den Formaten PEM und JKS enthalten. Die Truststore-Dateien müssen die Namen infa_truststore.jks und infa_truststore.pem aufweisen. Wenn die Truststore-Datei, die Sie von der Zertifizierungsstelle erhalten haben, einen anderen Namen aufweist, müssen Sie sie in infa_truststore.jks und infa_truststore.pem umbenennen.
-NodeTruststorePass -ntp	node_truststore_password	Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Erforderlich, wenn Sie Ihre SSL-Zertifikate verwenden. Passwort für die infa_truststore.jks-Datei.
-EnableKerberos -krb	enable_kerberos	Optional. Konfiguriert die Informatica-Domäne zur Verwendung der Kerberos-Authentifizierung. Gültige Werte sind „True“ oder „False“. Bei True verwendet die Domäne die Kerberos-Authentifizierung, dann können Sie den Authentifizierungsmodus später nicht ändern. Nachdem Sie die Kerberos-Authentifizierung aktiviert haben, können Sie sie nicht deaktivieren. Standardwert ist „False“. Wenn Sie die Option -krb ohne einen Wert angeben, verwendet die Informatica-Domäne die Kerberos-Authentifizierung.
-ServiceRealmName -srn	realm_name_of_node_spn	Optional. Name des Kerberos-Bereichs, zu dem die Informatica-Domänendienste gehören. Stellen Sie sicher, dass Sie den gleichen Wert als -urn für die Kerberos-Authentifizierung angeben.
-UserRealmName -urn	realm_name_of_user_spn	Optional. Name des Kerberos-Bereichs, zu dem die Informatica-Domänenbenutzer gehören. Stellen Sie sicher, dass Sie den gleichen Wert als -srn für die Kerberos-Authentifizierung angeben.
-KeysDirectory -kd	Infa_keys_directory_location	Optional. Verzeichnis, in dem alle Schlüsseltabellendateien und der Verschlüsselungsschlüssel für die Informatica-Domäne gespeichert werden. Standardwert ist `<Informatica-Installationsverzeichnis>/isp/config/keys`.
-HttpsPort -hs	admin_tool_https_port	Optional. Portnummer, die vom Knoten für die Kommunikation zwischen dem Administrator Tool und dem Dienstmanager verwendet wird. Geben Sie diese Portnummer an, wenn Sie HTTPS für einen Knoten konfigurieren möchten. Zum Deaktivieren von HTTPS-Unterstützung für einen Knoten setzen Sie diese Portnummer auf Null.
-NodeKeystoreFile -kf	admin_tool_keystore_file_location	Optional. Schlüsselspeicherdatei, in der die Schlüssel und Zertifikate enthalten sind, die bei Verwendung des SSL-Protokolls erforderlich sind

Option	Argument	Beschreibung
-KeystorePass -kp	admin_tool_keystore_password	Optional. Ein Volltext-Passwort für die Schlüsselspeicherdatei. Sie können ein Passwort mit der Option -kp oder der Umgebungsvariable INFA_PASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -kp festgelegte Passwort Vorrang.
-GatewayAddress -dg	domain_gateway_host:port	Erforderlich. Name und Portnummer des Gateway-Hostcomputers.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-SecurityDomain -sdn	sicherheitsdomäne	Name der Sicherheitsdomäne, die Sie erstellen möchten und zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Sie können einen Wert für -sdn angeben oder den Standardwert basierend auf dem Authentifizierungsmodus verwenden: - Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Standardwert ist „Native“. Zum Arbeiten mit der LDAP-Authentifizierung müssen Sie den Wert für -sdn angeben. - Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Standardwert ist „Native“ für native Authentifizierung. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.

Option	Argument	Beschreibung
-MinProcessPort -mi	minimum_port	Optional. Kleinste Portnummer für die Anwendungsdienstprozesse, die auf dem Knoten ausgeführt werden. Standardwert ist 11000.
-MaxProcessPort -ma	maximum_port	Optional. Größte Portnummer für die Anwendungsdienstprozesse, die auf dem Knoten ausgeführt werden. Standardwert ist 11999.
-ServerPort -sv	server_shutdown_port	Optional. Vom Dienstmanager verwendete TCP/IP-Portnummer. Der Dienstmanager verwaltet Befehle zum Herunterfahren aus PowerCenter-Komponenten auf diesem Port. Legen Sie diese Portnummer fest, wenn sich auf einem Computer mehrere Knoten befinden oder die Standardportnummer verwendet wird. Standardwert ist 8005.
-BackupDirectory -bd	backup_directory	Optional. Verzeichnis zum Speichern der Repository-Backup-Dateien. Der Zugriff auf das Verzeichnis muss über den Knoten möglich sein.
-ErrorLogLevel -el	fatal error warning info trace debug	Optional. Schweregradstufe für Protokollereignisse im Domänenprotokoll. Standardwert ist „info“.
-ResourceFile -rf	resource_file	Erforderlich. Datei, die eine Liste der verfügbaren Ressourcen für den Knoten enthält. Verwenden Sie die Datei „nodeoptions.xml“, die sich in folgendem Verzeichnis befindet: `<INFA_HOME>\isp\bin`.
-SystemLogDirectory -sld	system_log_directory	Optional. Verzeichnispfad zum Speichern von Systemprotokolldateien. Standardwert ist <INFA_home>/logs.

DeleteDomain

Löscht Metadatentabellen der Domäne. Vor dem Ausführen dieses Befehls müssen Sie die Informatica-Dienste auf dem Computer beenden. Zum Löschen einer Domäne auf einem Windows-Computer müssen Sie ebenfalls den Hostport öffnen oder die Firewall deaktivieren.

Wenn der Befehl mit einem Java-Speicherfehler fehlschlägt, stellen Sie für „infasetup“ mehr Systemspeicher zur Verfügung. Um mehr Systemspeicher zur Verfügung zu stellen, geben Sie den -Xmx-Wert in der Umgebungsvariable INFA_JAVA_CMD_OPTS an.

Der Befehl „DeleteDomain“ verwendet die folgende Syntax:

```
DeleteDomain

<<-DatabaseAddress|-da> database_hostname:database_port|

<-DatabaseConnectionString|-cs> database_connection_string>
```

```
[<-DatabaseUserName|-du> database_user_name]

[<-DatabasePassword|-dp> database_password]

<-DatabaseType|-dt> database_type ORACLE|DB2|MSSQLSERVER|SYBASE

[<-DatabaseServiceName|-ds> database_service_name]

[<-Tablespace|-ts> tablespace_name]

[<-SchemaName|-sc> schema_name (used for Microsoft SQL Server only)]

[<-DatabaseTlsEnabled|-dbtls> database_tls_enabled]

[<-DatabaseTruststorePassword|-dbtp> database_truststore_password]

[<-TrustedConnection|-tc> trusted_connection (used for Microsoft SQL Server only)]

[<-EncryptionKeyLocation|-kl> encryption_key_location]

[<-DatabaseTruststoreLocation|-dbtl> database_truststore_location]
```

In der folgenden Tabelle werden die Optionen und Argumente für „*infasetup* DeleteDomain“ beschrieben:

Option	Argument	Beschreibung
-DatabaseAddress -da	database_hostname:database_port	Erforderlich, wenn Sie die Option -DatabaseConnectionString (-cs) nicht verwenden. Name und Portnummer des Computers, auf dem die Konfigurationsdatenbank der Domäne gehostet wird.
-DatabaseConnectionString -cs	database_connection_string	Erforderlich, wenn Sie die Optionen -DatabaseAddress (-da) und -DatabaseServiceName (-ds) nicht verwenden. Verbindungsstring, der zum Herstellen einer Verbindung zur Konfigurationsdatenbank der Domäne verwendet wird. Geben Sie den Namen des Datenbankhosts, -ports und -diensts als Teil des Verbindungsstrings ein. Setzen Sie den Verbindungsstring zwischen Anführungszeichen.
-DatabaseUserName -du	database_user_name	Erforderlich, wenn Sie die Option -TrustedConnection (-tc) nicht verwenden. Konto für die Datenbank, die die Domänenkonfigurationsinformationen enthält.
-DatabasePassword -dp	database_password	Passwort aus der Datenbank für die Domänenkonfiguration des Datenbankbenutzers. Wenn Sie diese Option weglassen, verwendet *infasetup* das in der Umgebungsvariable INFA_DEFAULT_DATABASE_PASSWORD angegebene Passwort. Wird in der Umgebungsvariable kein Wert angegeben, müssen Sie ein Passwort unter Verwendung dieser Option eingeben.

Option	Argument	Beschreibung
-DatabaseType -dt	database_type	Erforderlich. Typ der Datenbank, in der die Metadaten der Domänenkonfiguration gespeichert werden. Zu den Datenbanktypen gehören: - db2 - oracle - mssqlserver - sybase
-DatabaseServiceName -ds	database_service_name	Erforderlich, wenn Sie die Option -DatabaseConnectionString (-cs) nicht verwenden. Der Name des Datenbankdiensts. Erforderlich für Oracle-, IBM DB2- und Microsoft SQL Server-Datenbanken. Geben Sie die SID für Oracle, den Dienstnamen für IBM DB2 oder den Datenbanknamen für Microsoft SQL Server ein.
-Tablespace -ts	tablespace_name	Erforderlich für eine IBM DB2-Datenbank. Name des Tablespace, in dem sich die Datenbanktabellen für die Domänenkonfiguration befinden.
SchemaName -sc	schema_name	Optional. Name des Microsoft SQL Server-Schemas. Geben Sie einen Schemanamen ein, wenn Sie nicht das Standardschema verwenden.
-DatabaseTlsEnabled -dbtls	database_tls_enabled	Optional. Gibt an, ob die Informatica-Domänendatenbank mit TLS und SSL sicher ist. Setzen Sie diese Option für die sichere Datenbank auf True. Standardwert ist „False“. Wenn Sie die Option -dbtls ohne Wert angegeben wird, verwendet die Informatica-Domäne die sichere Kommunikation mit der Informatica-Domänendatenbank.
-DatabaseTruststorePassword -dbtp	database_truststore_password	Optional. Passwort für die Datenbank-Truststore-Datei für die sichere Datenbank.
-TrustedConnection -tc	-	Optional. Stellen Sie eine Verbindung zur Microsoft SQL Server-Datenbank über eine vertrauenswürdige Verbindung her. Die vertrauenswürdige Authentifizierung verwendet die Windows-Sicherheitsanmeldedaten des aktuellen Benutzers, um eine Verbindung zu Microsoft SQL Server herzustellen.

Option	Argument	Beschreibung
-EncryptionKeyLocation -kl	encryption_key_location	Verzeichnis, das den aktuellen Verschlüsselungsschlüssel enthält. Der Name der Verschlüsselungsdatei lautet sitekey. Informatica benennt die aktuelle sitekey-Datei in sitekey_old um und generiert einen Verschlüsselungsschlüssel in einer neuen Datei mit dem Namen sitekey in demselben Verzeichnis.
-DatabaseTruststoreLocation -dbtl	database_truststore_location	Pfad und Dateiname der Truststore-Datei für die sichere Domänenrepository-Datenbank. Erforderlich, wenn Sie eine sichere Domänenrepository-Datenbank für die Domäne konfigurieren.

GenerateEncryptionKey

Generieren Sie einen Verschlüsselungsschlüssel, um vertrauliche Daten wie Passwörter in der Informatica-Domäne zu sichern.

Der Befehl GenerateEncryptionKey verwendet die folgende Syntax:

```
GenerateEncryptionKey

<-Keyword|-kw> keyword

<-DomainName|-dn> domain_name

[<-EncryptionKeyLocation|-kl> encryption_key_location]
```

In der folgenden Tabelle werden Optionen und Argumente für *infasetup* GenerateEncryptionKey beschrieben:

Option	Argument	Beschreibung
-Keyword -kw	keyword	Erforderlich. Die Textzeichenfolge, die als Basiswort verwendet wird, aus dem ein Verschlüsselungsschlüssel generiert werden soll. Das Schlüsselwort muss die folgenden Kriterien erfüllen: - Hat eine Länge von 8 bis 20 Zeichen - Enthält mindestens einen Großbuchstaben - Enthält mindestens einen Kleinbuchstaben - Enthält mindestens eine Zahl - Enthält keine Leerzeichen
-DomainName -dn	domain_name	Erforderlich. Name der Domäne.
-EncryptionKeyLocation -kl	encryption_key_location	Optional. Verzeichnis, das den aktuellen Verschlüsselungsschlüssel enthält. Der Name der Verschlüsselungsdatei lautet sitekey. Informatica benennt die aktuelle sitekey-Datei in sitekey_old um und generiert einen Verschlüsselungsschlüssel in einer neuen Datei mit dem Namen sitekey in demselben Verzeichnis. Um den Befehl erneut auszuführen, wenn mindestens zwei Sitekey-Dateien im Verzeichnis vorhanden sind, stellen Sie sicher, dass Sie die Sitekey-Dateien sichern. Sie können anschließend den Befehl zum Erstellen der Sitekey-Datei ausführen, bevor Sie die Sitekey-Dateien aus der Sicherung wiederherstellen.

Hilfe

Der Befehl Help zeigt die Optionen und Argumente für einen Befehl an. Wenn Sie den Befehlsnamen weglassen, listet *infasetup* alle Befehle auf.

Der Befehl Help verwendet die folgende Syntax:

```
Help [command]
```

Wenn Sie beispielsweise `infasetup Help UpdateWorkerNode` eingeben, gibt *infasetup* die folgenden Optionen und Argumente für den Befehl UpdateWorkerNode zurück:

```
UpdateWorkerNode [<-DomainName|-dn> domain_name] <-NodeName|-nn> node_name][<-
NodeAddress|-na> node_host:port]
[<-GatewayAddress|-dg> domain_gateway_host:port][<-UserName|-un> user_name][<-Password|-
pd> password][<-ServerPort|-sv> server_admin_port_number]
```

In der folgenden Tabelle werden die *infasetup* Help-Option und das -Argument beschrieben:

Option	Argument	Beschreibung
-	Befehl	Optional. Name des Befehls. Wenn Sie den Befehlsnamen weglassen, listet *infasetup* alle Befehle auf.

ListDomainCiphers

Dies dient zur Anzeige von einer oder mehreren der folgenden Listen mit Chiffre-Suites: Blacklist, Standardliste, Gültigkeitsliste oder Whitelist.

Blacklist

Liste mit Chiffre-Suites, die von der Informatica-Domäne blockiert werden sollen. Wenn Sie der Blacklist eine Chiffre-Suite hinzufügen, entfernt die Informatica-Domäne diese Chiffre-Suite aus der Gültigkeitsliste. Sie können Chiffre-Suites, die sich in der Standardliste befinden, zur Blacklist hinzufügen.

Standardliste

Liste mit Chiffre-Suites, die von der Informatica-Domäne standardmäßig unterstützt werden.

Whitelist

Liste mit Chiffre-Suites, die von der Informatica-Domäne zusätzlich zu denen in der Standardliste unterstützt werden sollen. Wenn Sie der Whitelist eine Chiffre-Suite hinzufügen, fügt die Informatica-Domäne die Chiffre-Suite zur Gültigkeitsliste hinzu. Chiffre-Suites, die sich in der Standardliste befinden, müssen nicht zur Whitelist hinzugefügt werden.

Für den Befehl „ListDomainCiphers“ wird die folgende Syntax verwendet:

```
[<-list|-l>] ALL|BLACK|DEFAULT|EFFECTIVE|WHITE

[<-domainConfig|-dc> true|false]
```

Hinweis: Dieser Befehl kann nicht auf dem Arbeitsknoten ausgeführt werden.

In der folgenden Tabelle werden die Optionen und Argumente für „infasetup listDomainCiphers“ beschrieben:

Option	Argument	Beschreibung
-list -l	ALL BLACK DEFAULT EFFECTIVE WHITE	Optional. Die anzuzeigende Konfigurationsliste mit Chiffre-Suites. Mit dem Argument „ALL“ werden die Blacklist, Standardliste, Gültigkeitsliste und Whitelist angezeigt. Mit dem Argument „BLACK“ wird die Blacklist angezeigt. Mit dem Argument „DEFAULT“ wird die Standardliste angezeigt. Mit dem Argument „EFFECTIVE“ wird die Gültigkeitsliste angezeigt. Mit dem Argument „WHITE“ wird die Whitelist angezeigt. **Hinweis:** Bei den Argumenten wird zwischen Groß- und Kleinschreibung unterschieden. Wird bei Ausführung des Befehls auf einem Gateway-Knoten diese Option ausgelassen, werden mit dem Befehl sämtliche Konfigurationslisten mit Chiffre-Suites angezeigt.
-domainConfig -dc	True Falsch	Optional. Zeigt die Listen mit Chiffre-Suites für die Informatica-Domäne oder für den Gateway-Knoten an, in der/dem der Befehl ausgeführt wird. Standardmäßig werden mit dem Befehl Listen mit Chiffre-Suites für die Domäne angezeigt. Setzen Sie diese Option auf „true“ (wahr), um die Listen mit Chiffre-Suites für die Domäne anzuzeigen. Setzen Sie diese Option auf „false“ (falsch), um die Listen mit Chiffre-Suites für den Gateway-Knoten anzuzeigen, in dem der Befehl ausgeführt wird. **Hinweis:** Auf Gateway-Knoten können keine Whitelists oder Blacklists angezeigt werden.

MigrateEncryptionKey

Ändern Sie den Verschlüsselungsschlüssel, um vertrauliche Daten wie Passwörter in der Informatica-Domäne zu sichern.

```
MigrateEncryptionKey

<-LocationOfEncryptionKeys|-loc> location_of_encryption_keys

[<-IsDomainMigrated|-mig> is_domain_migrated]
```

Hinweis: Wenn die Domäne enthält einen Berichterstellungsdienst enthält, ändern Sie den Verschlüsselungsschlüssel nicht. Der Befehl „migrateEncryptionKey“ schlägt fehl, wenn die Domäne einen Berichterstellungsdienst enthält.

In der folgenden Tabelle werden *infasetup* MigrateEncryptionKey“ beschrieben:

Option	Argument	Beschreibung
-LocationOfEncryptionKeys -loc	location_of_encryption_keys	Erforderlich. Verzeichnis, in dem die alte Verschlüsselungsschlüsseldatei mit dem Namen siteKey_old und die neue Verschlüsselungsschlüsseldatei mit dem Namen siteKey gespeichert sind. Das Verzeichnis muss die alten und neuen Verschlüsselungsschlüsseldateien enthalten. Wenn die alten und neuen Verschlüsselungsschlüsseldateien in verschiedenen Verzeichnissen gespeichert werden, kopieren Sie die Verschlüsselungsschlüsseldateien in dasselbe Verzeichnis. Wenn die Domäne mehrere Knoten enthält, muss dieses Verzeichnis allen Knoten in der Domäne zugänglich sein, in der Sie den Befehl „migrateEncryptionKey“ ausführen.
-IsDomainMigrated -mig	is_domain_migrated	Optional. Gibt an, ob die Domäne für die Verwendung des neuesten Verschlüsselungsschlüssels aktualisiert wurde. Beim erstmaligen Ausführen des Befehls „migrateEncryptionKey“ legen Sie diese Option auf FALSE fest, um anzugeben, dass die Domäne den alten Verschlüsselungsschlüssel verwendet. Nach dem erstmaligen Ausführen des Befehls „migrateEncryptionKey“ zum Aktualisieren anderer Knoten in der Domäne setzen Sie diese Option auf TRUE fest, um anzugeben, dass die Domäne für die Verwendung des neuesten Verschlüsselungsschlüssels aktualisiert wurde. Sie können den Befehl „migrateEncryptionKey“ auch ohne diese Option ausführen. Standardwert ist „true“.

RestoreDomain

Stelle die Konfigurationsmetadaten für die Domäne aus einer .mrep-Backup-Datei wieder her. Wenn Sie über eine Backup-Datei aus einer früheren Informatica-Version verfügen, müssen Sie die frühere Version zum Wiederherstellen der Domäne verwenden.

Sie müssen die Domäne vor dem Ausführen dieses Befehls herunterfahren.

Wenn Sie die Domäne in einer anderen als der ursprünglichen Backup-Datenbank wiederherstellen, müssen Sie die Inhalte der Tabelle ISP_RUN_LOG wiederherstellen, um die früheren Arbeitsablaufs- und Sitzungsprotokolle zu erhalten.

Wenn der Befehl mit einem Java-Speicherfehler fehlschlägt, stellen Sie für „infasetup“ mehr Systemspeicher zur Verfügung. Um mehr Systemspeicher zur Verfügung zu stellen, geben Sie den -Xmx-Wert in der Umgebungsvariable INFA_JAVA_CMD_OPTS an.

Der Befehl „RestoreDomain“ verwendet die folgende Syntax:

```
RestoreDomain
<<-DatabaseAddress|-da> database_hostname:database_port|
<-DatabaseConnectionString|-cs> database_connection_string>
[<-DatabaseUserName|-du> database_user_name]
[<-DatabasePassword|-dp> database_password]
<-DatabaseType|-dt> database_type
[<-DatabaseServiceName|-ds> database_service_name]
<-BackupFile|-bf> backup_file_name
[<-Force|-f>]
[<-ClearNodeAssociation|-ca>]
[<-Tablespace|-ts> tablespace_name]
[<-SchemaName|-sc> schema_name (used for MSSQLServer only)]
[<-DatabaseTlsEnabled|-dbtls> database_tls_enabled]
[<-DatabaseTruststorePassword|-dbtp> database_truststore_password]
[<-TrustedConnection|-tc> trusted_connection (used for MSSQLServer only)]
[<-EncryptionKeyLocation|-kl> encryption_key_location]
[<-DatabaseTruststoreLocation|-dbtl> database_truststore_location]
```

In der folgenden Tabelle werden *infasetup* RestoreDomain“ beschrieben:

Option	Argument	Beschreibung
-DatabaseAddress -da	database_hostname:database_port	Erforderlich, wenn Sie die Option -DatabaseConnectionString (-cs) nicht verwenden. Name und Portnummer des Computers, auf dem die Konfigurationsdatenbank der Domäne gehostet wird.
-DatabaseConnectionString -cs	database_connection_string	Erforderlich, wenn Sie die Optionen -DatabaseAddress (-da) und -DatabaseServiceName (-ds) nicht verwenden. Verbindungszeichenfolge, die zum Herstellen einer Verbindung zur Konfigurationsdatenbank der Domäne verwendet wird. Geben Sie den Namen des Datenbankhosts, -ports und -diensts als Teil der Verbindungszeichenfolge ein. Setzen Sie die Verbindungszeichenfolge in Anführungszeichen.
-DatabaseUserName -du	database_user_name	Erforderlich, wenn Sie die Option -TrustedConnection (-tc) nicht verwenden. Konto für die Datenbank, die die Domänenkonfigurationsinformationen enthält

Option	Argument	Beschreibung
-DatabasePassword -dp	database_password	Passwort aus der Datenbank für die Domänenkonfiguration des Datenbankbenutzers. Wenn Sie diese Option weglassen, verwendet *infasetup* das in der Umgebungsvariable INFA_DEFAULT_DATABASE_PASSWORD angegebene Passwort. Wird in der Umgebungsvariable kein Wert angegeben, müssen Sie ein Passwort unter Verwendung dieser Option eingeben.
-DatabaseType -dt	database_type	Erforderlich. Typ der Datenbank, der die Domänenkonfigurations-Metadaten speichert Zu den Datenbanktypen gehören: - db2 - oracle - mssqlserver - sybase
-DatabaseServiceName -ds	database_service_name	Erforderlich, wenn Sie die Option -DatabaseConnectionString (-cs) nicht verwenden. Der Name des Datenbankdiensts. Erforderlich für Oracle-, IBM DB2- und Microsoft SQL Server-Datenbanken. Geben Sie die SID für Oracle, den Dienstnamen für IBM DB2 oder den Datenbanknamen für Microsoft SQL Server ein.
-BackupFile -bf	backup_file_name	Erforderlich. Name und Pfad der Backup-Datei. Wenn Sie keinen Dateipfad angeben, erstellt *infasetup* die Backup-Datei im aktuellen Verzeichnis.
-Force -f	-	Optional. Überschreibt die Datenbank, wenn eine Datenbank mit demselben Namen bereits vorhanden ist. Geben Sie im Anschluss an diese Option keine weiteren Zeichen ein.
-ClearNodeAssociation -ca	-	Optional. Löscht Knotenzuordnungen beim Wiederherstellen der Domäne. Eine gesicherte Domäne enthält beispielsweise den Knoten „Node1“ auf dem Computer „MyHost:9090“. Wenn Sie diese Option auswählen, wird die Verbindung zwischen dem Knotennamen „Node1“ und der Adresse „MyHost:9090“ beim Wiederherstellen der Domäne unterbrochen. Sie können dann „MyHost:9090“ einen anderen Knoten zuordnen. Wenn Sie diese Option nicht angeben, behält „Node1“ die Verbindung zu „MyHost:9090“ bei. Wenn Sie die Domäne wiederherstellen und „MyHost:9090“ einen anderen Knoten zuordnen, wird der Knoten nicht gestartet.
-Tablespace -ts	tablespace_name	Erforderlich für eine IBM DB2-Datenbank. Name des Tablespace, in dem sich die Datenbanktabellen für die Domänenkonfiguration befinden.
-SchemaName -sc	schema_name	Optional. Name des Microsoft SQL Server-Schemas. Geben Sie einen Schemanamen ein, wenn Sie nicht das Standardschema verwenden.

Option	Argument	Beschreibung
-DatabaseTlsEnabled -dbtls	database_tls_enabled	Optional. Gibt an, ob die Informatica-Domänendatenbank mit TLS und SSL sicher ist. Setzen Sie diese Option für die sichere Datenbank auf True. Standardwert ist „False“. Wenn Sie die Option -dbtls ohne Wert angegeben wird, verwendet die Informatica-Domäne die sichere Kommunikation mit der Informatica-Domänendatenbank.
-DatabaseTruststorePassword -dbtp	database_truststore_password	Optional. Passwort für die Datenbank-Truststore-Datei für die sichere Datenbank.
-TrustedConnection -tc	-	Optional. Stellen Sie eine Verbindung zur Microsoft SQL Server-Datenbank über eine vertrauenswürdige Verbindung her. Die vertrauenswürdige Authentifizierung verwendet die Windows-Sicherheitsanmeldedaten des aktuellen Benutzers, um eine Verbindung zu Microsoft SQL Server herzustellen.
-EncryptionKeyLocation -kl	encryption_key_location	Optional. Verzeichnis, das den aktuellen Verschlüsselungsschlüssel enthält. Der Name der Verschlüsselungsdatei lautet sitekey.
-DatabaseTruststoreLocation -dbtl	database_truststore_location	Optional. Pfad und Dateiname der Truststore-Datei für die sichere Datenbank Erforderlich, wenn Sie eine sichere Domänenrepository-Datenbank für die Domäne konfigurieren.

SwitchToKerberosMode

Konfigurieren Sie die Informatica-Domäne zur Verwendung der Kerberos-Authentifizierung.

Der Befehl SwitchToKerberosMode verwendet die folgende Syntax:

```
SwitchToKerberosMode

<-administratorName|-ad> administrator_name

<-ServiceRealmName|-srn> realm_name_of_node_spn

<-UserRealmName|-urn> realm_name_of_user_spn

[<-SPNShareLevel|-spnSL> SPNShareLevel PROCESS|NODE]
```

In der folgenden Tabelle werden *infasetup* SwitchToKerberosMode-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-administratorName -ad	administrator_name	Erforderlich. Name des Benutzers, der als Standardadministrator ausgewählt werden soll
-ServiceRealmName -srn	realm_name_of_node_spn	Erforderlich. Name des Kerberos-Bereichs, zu dem die Informatica-Domänendienste gehören. Stellen Sie sicher, dass Sie den gleichen Wert als -urn für die Kerberos-Authentifizierung angeben.
-UserRealmName -urn	realm_name_of_user_spn	Erforderlich. Name des Kerberos-Bereichs, zu dem die Informatica-Domänenbenutzer gehören. Stellen Sie sicher, dass Sie den gleichen Wert als -srn für die Kerberos-Authentifizierung angeben.
SPNShareLevel -spnSL	SPNShareLevel PROCESS|NODE]	Optional. Gibt die Dienst-Prinzipalebene für die Domäne an. Legen Sie eine der folgenden Ebenen für die Eigenschaft fest: - Prozess Die Domäne erfordert einen eindeutigen Dienst-Prinzipalnamen (SPN) und eine Keytab-Datei für jeden Knoten und für jeden Dienst auf einem Knoten. Die Anzahl der für jeden Knoten erforderlichen SPNs und Keytab-Dateien hängt von der Anzahl der Dienstprozesse ab, die auf dem Knoten ausgeführt werden. Empfohlen für Produktionsdomänen. - Knoten. Die Domäne verwendet einen SPN und eine Keytab-Datei für den Knoten und für alle Dienste, die auf dem Knoten ausgeführt werden. Sie erfordert außerdem einen separaten SPN und eine separate Keytab-Datei für alle HTTP-Prozesse auf dem Knoten. Empfohlen für Test- und Entwicklungsdomänen. Empfohlen für Test- und Entwicklungsdomänen. Standardwert ist „Prozess“.

UpdateGatewayNode

Aktualisiert die Konnektivitätsinformationen für einen Gateway-Knoten auf dem aktuellen Computer. Führen Sie vor dem Aktualisieren des Gateway-Knotens den infacmd isp ShutDownNode-Befehl aus, um den Knoten herunterzufahren. Aktualisiert einen Gateway-Knoten auf dem aktuellen Computer. Führen Sie vor dem Aktualisieren des Gateway-Knotens den infaservice-Befehl zum Herunterfahren im Verzeichnis `<InformaticaInstallationDir>\tomcat\bin` aus, um den Knoten herunterzufahren.

Der Befehl „UpdateGatewayNode“ verwendet die folgende Syntax:

```
UpdateGatewayNode
[<-DatabaseAddress|-da> database_hostname:database_port|<-DatabaseConnectionString|-cs>
database_connection_string]
[<-DatabaseUserName|-du> database_user_name]
[<-DatabasePassword|-dp> database_password]
[<-DatabaseType|-dt> database_type ORACLE|DB2|MSSQLSERVER|SYBASE]
[<-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]
[<-EnableKerberos|-krb> enable_kerberos]
[<-ServiceRealmName|-srn> realm_name_of_node_spn]
[<-UserRealmName|-urn> realm_name_of_user_spn]
[<-KeysDirectory|-kd> Infa_keys_directory_location]
[<-AdminconsolePort|-ap> admin_tool_port]
[<-HttpsPort|-hs> admin_tool_https_port]
[<-KeystoreFile|-kf> admin_tool_keystore_file_location]
[<-KeystorePass|-kp> admin_tool_keystore_password]
[<-LogServiceDirectory|-ld> log_service_directory]
[<-SystemLogDirectory|-sld> system_log_directory]
[<-ServerPort|-sv> server_shutdown_port]
[<-AdminconsoleShutdownPort|-asp> admin_tool_shutdown_port]
[<-Tablespace|-ts> tablespace_name]
[<-SchemaName|-sc> schema_name (used for MSSQLServer only)]
[<-DatabaseTlsEnabled|-dbtls> database_tls_enabled]
[<-DatabaseTruststorePassword|-dbtp> database_truststore_password]
[<-DatabaseTruststoreLocation|-dbtl> database_truststore_location]
[<-TrustedConnection|-tc> trusted_connection (used for MSSQLServer only)]
[<-resetHostPort|-rst> resetHostPort]
```

In der folgenden Tabelle werden die Optionen und Argumente für „*infasetup* UpdateGatewayNode“ beschrieben:

Option	Argument	Beschreibung
-DatabaseAddress -da	database_hostname:database_port	Erforderlich, wenn Sie die Option -DatabaseConnectionString (-cs) nicht verwenden. Name und Portnummer des Computers, auf dem die Konfigurationsdatenbank der Domäne gehostet wird.
-DatabaseConnectionString -cs	database_connection_string	Erforderlich, wenn Sie die Optionen -DatabaseAddress (-da) und -DatabaseServiceName (-ds) nicht verwenden. Verbindungsstring, der zum Herstellen einer Verbindung zur Konfigurationsdatenbank der Domäne verwendet wird. Geben Sie den Namen des Datenbankhosts, -ports und -diensts als Teil des Verbindungsstrings ein. Setzen Sie den Verbindungsstring zwischen Anführungszeichen.
-DatabaseUserName -du	database_user_name	Erforderlich, wenn Sie die Option -TrustedConnection (-tc) nicht verwenden. Konto für die Datenbank, die die Domänenkonfigurationsinformationen enthält.
-DatabasePassword -dp	database_password	Passwort aus der Datenbank für die Domänenkonfiguration des Datenbankbenutzers. Wenn Sie diese Option weglassen, verwendet *infasetup* das in der Umgebungsvariable INFA_DEFAULT_DATABASE_PASSWORD angegebene Passwort. Wird in der Umgebungsvariable kein Wert angegeben, müssen Sie ein Passwort unter Verwendung dieser Option eingeben.

Option	Argument	Beschreibung
-DatabaseType -dt	database_type ORACLE|DB2|MSSQLSERVER|SYBASE	Erforderlich. Typ der Datenbank, in der die Domänenkonfigurationsmetadaten gespeichert werden. Zu den Datenbanktypen gehören: - db2 - oracle - mssqlserver - sybase
-DatabaseServiceName -ds	database_service_name	Erforderlich, wenn Sie die Option -DatabaseConnectionString (-cs) nicht verwenden. Der Name des Datenbankdiensts. Erforderlich für Oracle-, IBM DB2- und Microsoft SQL Server-Datenbanken. Geben Sie die SID für Oracle, den Dienstnamen für IBM DB2 oder den Datenbanknamen für Microsoft SQL Server ein.
-DomainName -dn	domain_name	Erforderlich. Name der Domäne.
-NodeName -nn	node_name	Optional. Name des Knotens. Knotennamen müssen zwischen 1 und 79 Zeichen umfassen und dürfen weder Leerzeichen noch die folgenden Zeichen enthalten:\ / * ? < > " |
-NodeAddress -na	node_host:port	Optional. Hostname und Portnummer für den Computer, auf dem der Knoten gehostet wird. Wählen Sie eine verfügbare Portnummer aus.
-ServiceManagerPort -sp	service_manager_port	Optional. Portnummer, die vom Dienstmanager verwendet wird, um auf eingehende Verbindungsanfragen zu reagieren.
-EnableTLS -tls	enable_tls	Optional. Konfiguriert die sichere Kommunikation für die Dienste in der Informatica-Domäne. Wenn Sie die standardmäßigen, von Informatica bereitgestellten SSL-Zertifikate verwenden, müssen Sie die Schlüsselspeicher- und Truststore-Optionen nicht angeben. Wenn Sie das SSL-Zertifikat nicht verwenden, müssen Sie die Keystore- und Truststore-Optionen angeben. Gültige Werte sind „True“ oder „False“. Standardwert ist „False“. Wenn Sie die Option -tls ohne Wert angeben, verwendet die Informatica-Domäne die sichere Kommunikation zwischen Diensten. Zum Aktivieren der sicheren Kommunikation für die verbundenen Dienste oder Webanwendungen, z. B. das Administrator-Tool, das Analyst-Tool oder den Webdienst-Hub, konfigurieren Sie die sichere Kommunikation separat innerhalb der Anwendungen.

Option	Argument	Beschreibung
-NodeKeystore -nk	node_keystore_directory	Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Erforderlich, wenn Sie Ihre SSL-Zertifikate verwenden. Verzeichnis, das die Schlüsselspeicherdateien enthält. Für die Informatica-Domäne müssen die SSL-Zertifikate im PEM-Format und in JKS (Java Keystore)-Dateien vorliegen. Das Verzeichnis muss Schlüsselspeicherdateien in den Formaten PEM und JKS enthalten. Die Schlüsselspeicherdateien müssen infa_keystore.jks und infa_keystore.pem lauten. Wenn die Schlüsselspeicherdatei, die Sie von der Zertifizierungsstelle erhalten, einen anderen Namen hat, müssen Sie sie in infa_keystore.jks und infa_keystore.pem umbenennen. Sie müssen für alle Knoten in der Domäne dieselben Schlüsselspeicherzertifikate verwenden.
-NodeKeystorePass -nkp	node_keystore_passwor d	Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Erforderlich, wenn Sie Ihre SSL-Zertifikate verwenden. Passwort für die Schlüsselspeicherdatei infa_keystore.jks.
-NodeTruststore -nt	node_truststore_director y	Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Erforderlich, wenn Sie Ihre SSL-Zertifikate verwenden. Verzeichnis, das die Truststore-Dateien enthält. Für die Informatica-Domäne müssen die SSL-Zertifikate im PEM-Format und in JKS-Dateien (Java Keystore) vorliegen. Das Verzeichnis muss Truststore-Dateien in den Formaten PEM und JKS enthalten. Die Truststore-Dateien müssen die Namen infa_truststore.jks und infa_truststore.pem aufweisen. Wenn die Truststore-Datei, die Sie von der Zertifizierungsstelle erhalten haben, einen anderen Namen aufweist, müssen Sie sie in infa_truststore.jks und infa_truststore.pem umbenennen.
-NodeTruststorePass -ntp	node_truststore_passwo rd	Optional, wenn Sie die SSL-Zertifikate von Informatica verwenden. Erforderlich, wenn Sie Ihre SSL-Zertifikate verwenden. Passwort für die infa_truststore.jks-Datei.
-EnableKerberos -krb	enable_kerberos	Optional. Konfiguriert die Informatica-Domäne zur Verwendung der Kerberos-Authentifizierung. Gültige Werte sind „True“ oder „False“. Bei True verwendet die Domäne die Kerberos-Authentifizierung, dann können Sie den Authentifizierungsmodus später nicht ändern. Nachdem Sie die Kerberos-Authentifizierung aktiviert haben, können Sie sie nicht deaktivieren. Standardwert ist „False“. Wenn Sie die Option -krb ohne einen Wert angeben, verwendet die Informatica-Domäne die Kerberos-Authentifizierung.
-ServiceRealmName -srn	realm_name_of_node_sp n	Optional. Name des Kerberos-Bereichs, zu dem die Informatica-Domänendienste gehören. Stellen Sie sicher, dass Sie den gleichen Wert als -urn für die Kerberos-Authentifizierung angeben.

Option	Argument	Beschreibung
-UserRealmName -urn	realm_name_of_user_spn	Optional. Name des Kerberos-Bereichs, zu dem die Informatica-Domänenbenutzer gehören. Stellen Sie sicher, dass Sie den gleichen Wert als -srn für die Kerberos-Authentifizierung angeben.
-KeysDirectory -kd	Infa_keys_directory_location	Optional. Verzeichnis, in dem alle Schlüsseltabellendateien und der Verschlüsselungsschlüssel für die Informatica-Domäne gespeichert werden. Standardwert ist `<Informatica-Installationsverzeichnis>/isp/config/keys`.
-AdminconsolePort -ap	admin_tool_port	Optional. Port für den Zugriff auf Informatica Administrator.
-HttpsPort -hs	admin_tool_https_port	Optional. Portnummer zum Sichern der Verbindung zum Administrator-Tool. Geben Sie diese Portnummer an, wenn Sie HTTPS für einen Knoten konfigurieren möchten. Zum Deaktivieren von HTTPS-Unterstützung für einen Knoten setzen Sie diese Portnummer auf Null.
-KeystoreFile -kf	admin_tool_keystore_file_location	Optional. Schlüsselspeicherdatei, in der die Schlüssel und Zertifikate enthalten sind, die bei Verwendung des SSL-Protokolls erforderlich sind
-KeystorePass -kp	admin_tool_keystore_password	Optional. Ein Volltext-Passwort für die Schlüsselspeicherdatei. Sie können ein Passwort mit der Option -kp oder der Umgebungsvariable INFA_PASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -kp festgelegte Passwort Vorrang.
-LogServiceDirectory -ld	log_service_directory	Optional. Freigegebener Verzeichnispfad, der vom Protokollmanager zum Speichern von Protokollereignisdateien verwendet wird.
-SystemLogDirectory -sld	system_log_directory	Optional. Verzeichnispfad zum Speichern von Systemprotokolldateien. Standard ist <INFA_home>/logs.
-ServerPort -sv	server_shutdown_port	Optional. Vom Dienstmanager verwendete TCP/IP-Portnummer. Der Dienstmanager verwaltet Befehle zum Herunterfahren aus PowerCenter-Komponenten auf diesem Port. Legen Sie diese Portnummer fest, wenn sich auf einem Computer mehrere Knoten befinden oder die Standardportnummer verwendet wird. Standardwert ist 8005.
-AdminconsoleShutdownPort -asp	admin_tool_shutdown_port	Optional. Portnummer, die das Herunterfahren für Informatica Administrator steuert.
-Tablespace -ts	tablespace_name	Erforderlich für eine IBM DB2-Datenbank. Name des Tablespace, in dem sich die Datenbanktabellen für die Domänenkonfiguration befinden.

Option	Argument	Beschreibung
-SchemaName -sc	schema_name <wird nur für MSSQLServer verwendet>	Optional. Name des Microsoft SQL Server-Schemas. Geben Sie einen Schemanamen ein, wenn Sie nicht das Standardschema verwenden.
-DatabaseTlsEnabled -dbtls	database_tls_enabled	Optional. Gibt an, ob die Informatica-Domänendatenbank mit TLS und SSL sicher ist. Setzen Sie diese Option für die sichere Datenbank auf True. Standardwert ist „False“. Wenn die Option -dbtls ohne Wert angegeben wird, verwendet die Informatica-Domäne die sichere Kommunikation mit der Informatica-Domänendatenbank.
-DatabaseTruststorePassword -dbtp	database_truststore_password	Optional. Passwort für die Datenbank-Truststore-Datei für die sichere Datenbank.
-TrustedConnection -tc	trusted_connection <wird nur für MSSQLServer verwendet>	Optional. Stellen Sie eine Verbindung zur Microsoft SQL Server-Datenbank über eine vertrauenswürdige Verbindung her. Die vertrauenswürdige Authentifizierung verwendet die Windows-Sicherheitsanmeldedaten des aktuellen Benutzers, um eine Verbindung zu Microsoft SQL Server herzustellen.
-resetHostPort -rst	resetHostPort	Erforderlich, wenn Sie die Option NodeAddress oder ServiceManager angeben. Setzt die Portnummer des Hosts zurück.
-DatabaseTruststoreLocation -dbtl	database_truststore_location	Optional. Pfad und Dateiname der Truststore-Datei für den Gateway-Knoten.

UpdateKerberosAdminUser

Aktualisiert den Kerberos-Standardadministrator im Domänen-Repository.

Der Befehl UpdateKerberosAdminUser verwendet die folgende Syntax:

```
UpdateKerberosAdminUser

<-KerberosAdminName|-kan> kerberos_admin_name
```

In der folgenden Tabelle werden die *infasetup* UpdateKerberosAdminUser-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-KerberosAdminName -kan	kerberos_admin_name	Erforderlich. Name des Benutzers, der als Standardadministrator ausgewählt werden soll

UpdateKerberosConfig

Verwenden Sie den Befehl „UpdateKerberosConfig“, um den Bereichsnamen oder den Dienst-Bereichsnamen in der Informatica-Konfiguration zu korrigieren. Sie können den Benutzerbereich ändern, zu dem die Informatica-Domänenbenutzer gehören. Sie können den Dienstbereich ändern, zu dem die Informatica-Domänendienste gehören.

Hinweis: Dieser Befehl ändert nicht die Kerberos-Konfiguration. Sie können mit diesem Befehl keine Benutzer von einem Benutzer- oder Dienstbereich in einen anderen Benutzer- oder Dienstbereich migrieren.

Der Befehl „UpdateKerberosConfig“ verwendet die folgende Syntax:

```
UpdateKerberosConfig

[<-ServiceRealmName|-srn>] realm_name_of_node_spn

[<-UserRealmName|-urn>] realm_name_of_user_spn
```

In der folgenden Tabelle werden Optionen und Argumente für „*infasetup* UpdateKerberosConfig“ beschrieben:

Option	Argument	Beschreibung
-ServiceRealmName -srn	realm_name_of_node_spn	Optional. Name des Kerberos-Bereichs, zu dem die Informatica-Domänendienste gehören. Der Dienst-Bereichsname muss derselbe wie der Benutzer-Bereichsname sein.
-UserRealmName -urn	realm_name_of_user_spn	Optional. Name des Kerberos-Bereichs, zu dem die Informatica-Domänenbenutzer gehören. Der Benutzer-Bereichsname muss derselbe wie der Dienst-Bereichsname sein.

UpdateDomainCiphers

Dient zur Aktualisierung der Informatica-Domäne für die Verwendung einer neuen Gültigkeitsliste. Ändert die Whitelist, um Chiffre-Suites in die Gültigkeitsliste aufzunehmen. Ändert die Blacklist, um Chiffre-Suites aus der Gültigkeitsliste zu entfernen.

Überprüfen Sie vor der Ausführung dieses Befehls, ob die folgenden Voraussetzungen erfüllt werden:

- Für die Domäne werden intern sichere Kommunikation bzw. extern sichere Verbindungen mit Webclients verwendet.
- Die Domäne wurde heruntergefahren.
- Sie können den Befehl auf einem Gateway-Knoten in der Domäne ausführen.

Die Gültigkeitsliste mit Chiffre-Suites enthält die von der Informatica-Domäne unterstützten Chiffre-Suites. Beim Ausführen des Befehls „UpdateDomainCiphers“ erstellt die Informatica-Domäne die Gültigkeitsliste mit Chiffre-Suites auf Grundlage der folgenden Listen:

Blacklist

Liste mit Chiffre-Suites, die von der Informatica-Domäne blockiert werden sollen. Wenn Sie der Blacklist eine Chiffre-Suite hinzufügen, entfernt die Informatica-Domäne diese Chiffre-Suite aus der Gültigkeitsliste. Sie können Chiffre-Suites, die sich in der Standardliste befinden, zur Blacklist hinzufügen.

Standardliste

Liste mit Chiffre-Suites, die von der Informatica-Domäne standardmäßig unterstützt werden.

Whitelist

Liste mit Chiffre-Suites, die von der Informatica-Domäne zusätzlich zu denen in der Standardliste unterstützt werden sollen. Wenn Sie der Whitelist eine Chiffre-Suite hinzufügen, fügt die Informatica-Domäne die Chiffre-Suite zur Gültigkeitsliste hinzu. Chiffre-Suites, die sich in der Standardliste befinden, müssen nicht zur Whitelist hinzugefügt werden.

Beachten Sie die folgenden Richtlinien für die Ausführung des Befehls „UpdateDomainCiphers“:

- Beim Ausführen des Befehls erstellen Sie eine neue Gültigkeitsliste, die die bisherige überschreibt.
- Wenn Sie den Befehl ausführen und eine Whitelist oder Blacklist festlegen, überschreibt diese neue Liste die bisherige.
- Die Gültigkeitsliste umfasst die Chiffre-Suites, die sich in der Standardliste und Whitelist befinden, und schließt die Chiffre-Suites in der Blacklist aus.
- Wenn Sie den Befehl ausführen, ohne eine Whitelist oder Blacklist festzulegen, wird mit dem Befehl eine Gültigkeitsliste erstellt, die die Chiffre-Suites aus der Standardliste verwendet.
- Die Gültigkeitsliste muss mindestens eine Chiffre-Suite enthalten, die von TLS v1.1 oder 1.2 unterstützt wird.
- Bei der Gültigkeitsliste muss es sich um eine gültige Chiffre-Suite für Windows, die Java-Laufzeitumgebung und OpenSSL handeln.

Weitere Informationen zum Erstellen von Whitelists und Blacklists für die Aktualisierung der von der Informatica-Domäne verwendeten Gültigkeitsliste finden Sie im *Informatica-Sicherheitshandbuch*.

Für den Befehl „UpdateDomainCiphers“ wird die folgende Syntax verwendet:

```
[<-preview|-p> true|false]

[<-cipherWhiteList|-cwl> ciphersuite1,ciphersuite2,...]

[<-cipherWhiteListFile|-cwlf> whitelist_file_name]

[<-cipherBlackList|-cbl> ciphersuite1,ciphersuite2,...]

[<-cipherBlackListFile|-cblf> blacklist_file_name]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infasetup UpdateDomainCiphers“ beschrieben:

Option	Argument	Beschreibung
-preview -p	True Falsch	Optional. Bei „true“ wird mit dem Befehl die Gültigkeitsliste mit den Chiffre-Suites angezeigt, die von der Domäne verwendet werden wird. Bei „false“ werden mit dem Befehl die Chiffre-Suites für die Informatica-Domäne so aktualisiert, dass die Gültigkeitsliste mit Chiffre-Suites verwendet wird. Standardwert ist „false“.
-cipherWhiteList -cwl	CipherSuiteName01,CiphersuiteName02, ...	Optional. Eine kommagetrennte Liste mit Chiffre-Suites, die Sie in die Gültigkeitsliste aufnehmen möchten. Verwenden Sie den vollständigen Registrierungsnamen der IANA TLS-Chiffre-Suites oder einen regulären Java-Ausdruck. Diese Liste überschreibt die bisherige Whitelist. **Hinweis:** Die Liste muss mindestens eine gültige JRE- oder OpenSSL-Chiffre-Suite enthalten.
-cipherWhiteListFile -cwlf	whitelist_file_location	Optional. Absoluter Dateipfad und Dateiname einer Klartextdatei mit einer kommagetrennten Liste mit Chiffre-Suites, die Sie in die Gültigkeitsliste aufnehmen möchten. Diese Liste überschreibt die bisherige Whitelist. Verwenden Sie den vollständigen Registrierungsnamen der IANA TLS-Chiffre-Suites oder einen regulären Java-Ausdruck. **Hinweis:** Die Liste muss mindestens eine gültige JRE- oder OpenSSL-Chiffre-Suite enthalten.
-cipherBlackList -cbl	CipherSuiteName01,CiphersuiteName02, ...	Optional. Eine kommagetrennte Liste mit Chiffre-Suites, die Sie aus der Gültigkeitsliste entfernen möchten. Verwenden Sie den vollständigen Registrierungsnamen der IANA TLS-Chiffre-Suites oder einen regulären Java-Ausdruck. Diese Liste überschreibt die bisherige Blacklist. **Hinweis:** Die Gültigkeitsliste muss mindestens eine gültige JRE- oder OpenSSL-Chiffre-Suite enthalten.
-cipherBlackListFile -cblf	blacklist_file_location	Optional. Absoluter Dateipfad und Dateiname einer Klartextdatei mit einer kommagetrennten Liste mit Chiffre-Suites, die Sie aus der Gültigkeitsliste entfernen möchten. Verwenden Sie den vollständigen Registrierungsnamen der IANA TLS-Chiffre-Suites oder einen regulären Java-Ausdruck. Diese Liste überschreibt die bisherige Liste. **Hinweis:** Die Gültigkeitsliste muss mindestens eine gültige JRE- oder OpenSSL-Chiffre-Suite enthalten.

UpdateWorkerNode

Aktualisiert die Konnektivitätsinformationen für einen Arbeitsknoten auf dem aktuellen Computer. Führen Sie vor dem Aktualisieren des Arbeitsknotens den infacmd isp ShutDownNode-Befehl aus, um den Knoten herunterzufahren.

Der Befehl „UpdateWorkerNode“ verwendet die folgende Syntax:

```
UpdateWorkerNode
[<-DomainName|-dn> domain_name]
[<-NodeName|-nn> node_name]
[<-NodeAddress|-na> node_host:port]
[<-ServiceManagerPort|-sp> service_manager_port]
[<-EnableTLS|-tls> enable_tls]
[<-NodeKeystore|-nk> node_keystore_directory]
[<-NodeKeystorePass|-nkp> node_keystore_password]
[<-NodeTruststore|-nt> node_truststore_directory]
[<-NodeTruststorePass|-ntp> node_truststore_password]
[<-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]
```

In der folgenden Tabelle werden die Optionen und Argumente für „*infasetup* UpdateWorkerNode“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Domäne.
-NodeName -nn	node_name	Optional. Name des Knotens. Knotennamen müssen zwischen 1 und 79 Zeichen umfassen und dürfen weder Leerzeichen noch die folgenden Zeichen enthalten:\ / * ? < > " |
-NodeAddress -na	node_host:port	Optional. Hostname und Portnummer für den Computer, auf dem der Knoten gehostet wird. Wählen Sie eine verfügbare Portnummer aus.
-ServiceManagerPort -sp	service_manager_port	Optional. Portnummer, die vom Dienstmanager verwendet wird, um auf eingehende Verbindungsanfragen zu reagieren.

Option	Argument	Beschreibung
-EnableTLS -tls	enable_tls	Optional. Konfiguriert die sichere Kommunikation für die Dienste in der Informatica-Domäne. Wenn Sie die standardmäßigen, von Informatica bereitgestellten SSL-Zertifikate verwenden, müssen Sie die Schlüsselspeicher- und Truststore-Optionen nicht angeben. Wenn Sie das SSL-Zertifikat nicht verwenden, müssen Sie die Keystore- und Truststore-Optionen angeben. Gültige Werte sind „True“ oder „False“. Standardwert ist „False“. Wenn Sie die Option -tls ohne Wert angeben, verwendet die Informatica-Domäne die sichere Kommunikation zwischen Diensten. Zum Aktivieren der sicheren Kommunikation für die verbundenen Dienste oder Webanwendungen, z. B. das Administrator-Tool, das Analyst-Tool oder den Webdienst-Hub, konfigurieren Sie die sichere Kommunikation separat innerhalb der Anwendungen.
-ServiceRealmName -srn	realm_name_of_node_spn	Optional. Name des Kerberos-Bereichs, zu dem die Informatica-Domänendienste gehören. Stellen Sie sicher, dass Sie den gleichen Wert als -urn für die Kerberos-Authentifizierung angeben.
-UserRealmName -urn	realm_name_of_user_spn	Optional. Name des Kerberos-Bereichs, zu dem die Informatica-Domänenbenutzer gehören. Stellen Sie sicher, dass Sie den gleichen Wert als -srn für die Kerberos-Authentifizierung angeben.
-KeysDirectory -kd	Infa_keys_directory_location	Optional. Verzeichnis, in dem alle Schlüsseltabellendateien und der Verschlüsselungsschlüssel für die Informatica-Domäne gespeichert werden. Standardwert ist `<Informatica-Installationsverzeichnis>/isp/config/keys`.
-HttpsPort -hs	admin_tool_https_port	Optional. Portnummer zum Sichern der Verbindung zum Administrator-Tool. Geben Sie diese Portnummer an, wenn Sie HTTPS für einen Knoten konfigurieren möchten.
-NodeKeystoreFile -kf	admin_tool_keystore_file_location	Optional. Schlüsselspeicherdatei, in der die Schlüssel und Zertifikate enthalten sind, die bei Verwendung des SSL-Protokolls erforderlich sind
-KeystorePass -kp	admin_tool_keystore_password	Optional. Ein Volltext-Passwort für die Schlüsselspeicherdatei. Sie können ein Passwort mit der Option -kp oder der Umgebungsvariable INFA_PASSWORD einrichten. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -kp festgelegte Passwort Vorrang.
-GatewayAddress -dg	domain_gateway_host:port	Erforderlich. Name und Portnummer des Gateway-Hostcomputers.

Option	Argument	Beschreibung
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-SecurityDomain -sdn	sicherheitsdomäne	Name der Sicherheitsdomäne, die Sie erstellen möchten und zu dem Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Sie können einen Wert für -sdn angeben oder den Standardwert basierend auf dem Authentifizierungsmodus verwenden: - Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Standardwert ist „Native“. Zum Arbeiten mit der LDAP-Authentifizierung müssen Sie den Wert für -sdn angeben. - Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Standardwert ist „Native“ für native Authentifizierung. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-ServerPort -sv	server_shutdown_port	Optional. Vom Dienstmanager verwendete TCP/IP-Portnummer. Der Dienstmanager verwaltet Befehle zum Herunterfahren aus PowerCenter-Komponenten auf diesem Port. Legen Sie diese Portnummer fest, wenn sich auf einem Computer mehrere Knoten befinden oder die Standardportnummer verwendet wird.
-resetHostPort -rst	true | false	Erforderlich, wenn Sie die Option NodeAddress oder ServiceManager angeben. Setzt die Portnummer des Hosts zurück.
-SystemLogDirectory -sld	system_log_directory	Optional. Verzeichnispfad zum Speichern von Systemprotokolldateien. Standard ist <INFA_home>/logs.

UnlockUser

Entsperrt ein natives oder ein LDAP-Benutzerkonto. Wenn Sie ein natives Benutzerkonto entsperren, können Sie außerdem ein neues Passwort für das Benutzerkonto eingeben.

Sie können ein Benutzerkonto entsperren, nachdem Sie die Domäne aus dem Gateway-Knoten herunterfahren.

Sie können ein Benutzerkonto entsperren, nachdem Sie die Domäne heruntergefahren und die Domänendatenbank gestartet haben.

So starten Sie die Domänendatenbank unter Windows:

1. Navigieren Sie zu folgendem Speicherort in der Befehlszeile: `<InformaticaInstallationDir>\h2\bin`.
2. Geben Sie den folgenden Befehl ein: dbmanager.bat startup.

So starten Sie die Domänendatenbank unter UNIX:

1. Navigieren Sie zu folgendem Speicherort in der Befehlszeile: `<InformaticaInstallationDir>/h2/bin`.
2. Geben Sie den folgenden Befehl ein: dbmanager.sh startup.

Der Befehl „infasetup-Befehl UnlockUser“ verwendet folgende Syntax:

```
UnlockUser

<-UserName|-un> user_name

[<-SecurityDomain|-sdn] security domain]

[<-NewPassword|-np] new_password]
```

Die folgende Tabelle beschreibt die infasetup-Optionen und Argumente für UnlockUser:

Option	Argument	Beschreibung
-UserName -un	user_name	Erforderlich. Benutzername des gesperrten Kontos. Bei diesem Wert muss die Groß-/Kleinschreibung beachtet werden.
-SecurityDomain -sdn	sicherheitsdomäne	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch. Optional. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Standardwert ist „Native“.
-NewPassword -np	new_password	Optional. Neues Passwort für das gesperrte native Konto.

ValidateandRegisterFeature

Validiert und registriert die Funktion in der Domäne.

Der Befehl ValidateandRegisterFeature verwendet die folgende Syntax:

```
ValidateandRegisterFeature

<-FeatureFilename|-ff> feature_filename

<-IsUpgrade|-up> is_upgrade
```

In der folgenden Tabelle werden die *infasetup* ValidateandRegisterFeature-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-FeatureFilename -ff	feature_filename	Erforderlich. Speicherort der XML-Datei für das Plug-In.
-IsUpgrade -up	is_upgrade	Erforderlich. Gibt an, ob ein Upgrade des Plug-In auf die angegebene Version in der Funktionsdatei durchgeführt werden soll. Gültige Werte sind „True“ und „False“. Standardwert ist „True“.

KAPITEL 32

Pmcmd-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- Verwenden von pmcmd, 1098
- AbortTask, 1103
- abortworkflow, 1105
- Connect, 1107
- Disconnect, 1108
- Exit, 1109
- GetRunningSessionsDetails, 1109
- GetServiceDetails, 1110
- GetServiceProperties, 1112
- getsessionstatistics, 1113
- GetTaskDetails, 1115
- GetWorkflowDetails, 1117
- Hilfe, 1121
- PingService, 1121
- RecoverWorkflow, 1122
- ScheduleWorkflow, 1124
- SetFolder, 1126
- SetNoWait, 1126
- SetWait, 1127
- ShowSettings, 1127
- StartTask, 1127
- StartWorkflow, 1131
- StopTask, 1135
- StopWorkflow, 1137
- UnscheduleWorkflow, 1139
- UnsetFolder, 1141
- Version, 1141
- WaitTask, 1141
- WaitWorkflow, 1143

Verwenden von pmcmd

pmcmd ist ein Programm zum Kommunizieren mit dem Integration Service. Mit *pmcmd* können Sie einige der Arbeiten ausführen, die Sie auch im Workflow Manager durchführen können, wie z. B. das Starten und Beenden von Arbeitsabläufen und Sitzungen.

Verwenden Sie *pmcmd* in den folgenden Modi:

- **Befehlszeilenmodus.** Sie rufen *pmcmd* jedes Mal auf und beenden es, wenn Sie einen Befehl ausführen. Sie können Skripts zum Planen von Arbeitsabläufen mit der Befehlszeilensyntax schreiben. Jeder im Befehlszeilenmodus geschriebene Befehl muss Verbindungsinformationen zum Integration Service einbeziehen.
- **Interaktiver Modus.** Sie stellen eine aktive Verbindung zum Integration Service her und erhalten sie aufrecht. Dadurch können Sie eine Reihe von Befehlen eingeben.

Sie können Umgebungsvariablen für Benutzernamen und Passwörter mit *pmcmd* verwenden. Sie können Umgebungsvariablen zudem verwenden, um die Art und Weise anzupassen, mit der *pmcmd* Datum und Uhrzeit auf dem Computer anzeigt, auf dem der Integration Service-Prozess ausgeführt wird. Bevor Sie *pmcmd* verwenden, konfigurieren Sie diese Variablen auf dem Computer, auf dem der Integration Service-Prozess ausgeführt wird. Die Umgebungsvariablen gelten für *pmcmd*-Befehle, die auf dem Knoten ausgeführt werden.

Hinweis: Wenn die Domäne eine Domäne für verschiedene Versionen ist, führen Sie *pmcmd* über das Installationsverzeichnis der Integration Service-Version aus.

Ausführen von Befehlen im Befehlszeilenmodus

Im Befehlszeilenmodus wird *pmcmd* jedes Mal aufgerufen und beendet, wenn Sie einen Befehl ausführen. Der Befehlszeilenmodus ist sinnvoll, wenn Sie *pmcmd*-Befehle mit Batchdateien, Skripts oder anderen Programmen ausführen möchten.

Sie können *pmcmd*-Befehle mit Betriebssystem-Planungstools wie *cron* verwenden oder *pmcmd*-Befehle in Shell- oder Perl-Skripts einbetten.

Wenn Sie *pmcmd* im Befehlszeilenmodus ausführen, geben Sie in jedem Befehl Verbindungsinformationen wie Domänenname, Name des Integration Service, Benutzername und Passwort ein. Um beispielsweise den Arbeitsablauf "wf_SalesAvg" im Ordner "SalesEast" zu starten, verwenden Sie folgende Syntax:

```
pmcmd startworkflow -sv MyIntService -d MyDomain -u seller3 -p jackson -f SalesEast
wf_SalesAvg
```

Der Benutzer "seller3" mit dem Passwort "jackson" sendet die Anfrage, um den Arbeitsablauf zu starten.

Wenn Sie eine erforderliche Option nicht oder falsch eingeben, schlägt der Befehl fehl und *pmcmd* gibt einen Nicht-Null-Rückgabewert zurück. Weitere Informationen über alle Rückgabewerte finden Sie unter "pmcmd-Rückgabewerte" auf Seite 1099

So führen Sie pmcmd-Befehle im Befehlszeilenmodus aus:

1. Wechseln Sie an der Eingabeaufforderung zu dem Verzeichnis, in dem sich die ausführbare *pmcmd*-Datei befindet.

   Standardmäßig installiert das PowerCenter-Installationsprogramm *pmcmd* im \server\bin-Verzeichnis.

2. Geben Sie `pmcmd` gefolgt vom Befehlsnamen und den erforderlichen Optionen und Argumenten ein:

   `pmcmd` *`command_name`* `[-option1]` *`argument_1`* `[-option2]` *`argument_2`*`...`

pmcmd-Rückgabewerte

Im Befehlszeilenmodus gibt *pmcmd* die erfolgreiche oder fehlgeschlagene Ausführung eines Befehls durch einen Rückgabewert an. Rückgabewert "0" gibt an, dass der Befehl erfolgreich ausgeführt wurde. Jeder andere Rückgabewert gibt an, dass der Befehl fehlgeschlagen ist.

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

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

In der folgenden Tabelle werden die Rückgabewerte für *pmcmd* beschrieben:

Code	Beschreibung
0	Für alle Befehle gibt ein Rückgabewert von Null an, dass der Befehl erfolgreich ausgeführt wurde. Sie können folgende Befehle im wait- oder nowait-Modus ausführen: starttask, startworkflow, aborttask und abortworkflow. Wenn Sie einen Befehl im wait-Modus ausführen, gibt ein Rückgabewert von Null an, dass der Befehl erfolgreich ausgeführt wurde. Wenn Sie einen Befehl im nowait-Modus ausführen, gibt ein Rückgabewert von Null an, dass die Anfrage erfolgreich an den Integration Service übermittelt wurde und dieser die Anfrage bestätigt hat.
1	Der Integration Service ist nicht verfügbar oder *pmcmd* kann keine Verbindung zum Integration Service herstellen. Es gibt ein Problem mit dem TCP/IP-Hostnamen, der Portnummer oder dem Netzwerk.
2	Der Name der Aufgabe, des Arbeitsablaufs oder des Ordners ist nicht vorhanden.
3	Beim Starten oder Ausführen des Arbeitsablaufs oder der Aufgabe ist ein Fehler aufgetreten.
4	Verwendungsfehler. Sie haben die falschen Optionen an *pmcmd* übergeben.
5	Ein interner *pmcmd*-Fehler ist aufgetreten. Setzen Sie sich mit dem globalen Informatica-Kundensupport in Verbindung.
7	Sie haben einen ungültigen Benutzernamen oder ein ungültiges Passwort verwendet.
8	Sie verfügen nicht über die entsprechenden Berechtigungen zum Ausführen dieser Aufgabe.
9	Die Verbindung zum Integration Service ist beim Senden der Anfrage abgelaufen.
12	Der Integration Service kann die Wiederherstellung nicht starten, da die Sitzung oder der Arbeitsablauf geplant ist, auf ein Ereignis wartet, wartet, initialisiert bzw. angehalten, aktiviert oder ausgeführt wird.
13	Die Benutzername-Umgebungsvariable ist auf einen leeren Wert gesetzt.
14	Die Passwort-Umgebungsvariable ist auf einen leeren Wert gesetzt.
15	Die Benutzername-Umgebungsvariable fehlt.
16	Die Passwort-Umgebungsvariable fehlt.
17	Die Parameterdatei ist nicht vorhanden.
18	Der Integration Service hat die Parameterdatei gefunden, verfügt aber nicht über die Anfangswerte für die Sitzungsparameter, wie beispielsweise $input oder $output.

Code	Beschreibung
19	Der Integration Service kann die Sitzung nicht wiederaufnehmen, da der Arbeitsablauf für eine kontinuierliche Ausführung konfiguriert wurde.
20	Ein Repository-Fehler ist aufgetreten. Stellen Sie sicher, dass der Repository Service und die Datenbank ausgeführt werden und die Anzahl der Verbindungen in der Datenbank nicht überschritten wird.
21	Der Integration Service wird heruntergefahren und akzeptiert keine neuen Anfragen.
22	Der Integration Service kann keine eindeutige Instanz des angegebenen Arbeitsablaufs/der angegebenen Sitzung finden. Geben Sie den Befehl erneut mit dem Namen des Ordners und des Arbeitsablaufs ein.
23	Für die Anfrage stehen keine Daten zur Verfügung.
24	Keine Speicherkapazität.
25	Befehl wird abgebrochen.

Ausführen von Befehlen im interaktiven Modus

Verwenden Sie *pmcmd* im interaktiven Modus zum Starten und Stoppen von Arbeitsabläufen und Sitzungen, ohne ein Skript zu schreiben. Wenn Sie den interaktiven Modus verwenden, geben Sie Verbindungsinformationen wie Domänenname, Name des Integration Service, Benutzername und Passwort ein. Sie können nachfolgende Befehle ausführen, ohne die Verbindungsinformationen für jeden Befehl einzugeben.

Die folgenden Befehle rufen beispielsweise den interaktiven Modus auf, stellen eine Verbindung zum Integration Service "myintservice" her und starten die Arbeitsabläufe "wf_SalesAvg" und "wf_SalesTotal" im Ordner "SalesEast":

```
pmcmd
pmcmd> connect -sv MyIntService -d MyDomain -u seller3 -p jackson
pmcmd> setfolder SalesEast
pmcmd> startworkflow wf_SalesAvg
pmcmd> startworkflow wf_SalesTotal
```

So führen Sie pmcmd-Befehle im interaktiven Modus aus:

1. Wechseln Sie an der Eingabeaufforderung zu dem Verzeichnis, in dem sich die ausführbare *pmcmd*-Datei befindet.

   Standardmäßig installiert das PowerCenter-*Installationsprogramm pmcmd* im \server\bin-Verzeichnis.

2. Geben Sie an der Eingabeaufforderung `pmcmd` ein.

   Dies startet *pmcmd* im interaktiven Modus und zeigt die `pmcmd>`-Eingabeaufforderung an. `pmcmd` muss nicht vor jedem Befehl im interaktiven Modus eingegeben werden.

3. Geben Sie die Verbindungsinformationen für die Domäne und den Integration Service ein. Beispiel:

   ```
   connect -sv MyIntService -d MyDomain -u seller3 -p jackson
   ```

4. Geben Sie einen Befehl und dessen Optionen und Argumente in folgendem Format ein:

   command_name [-option1] *argument_1* [-option2] *argument_2*...

   pmcmd führt den Befehl aus und zeigt die Eingabeaufforderung erneut an.

5. Geben Sie `exit` ein, um eine interaktive Sitzung zu beenden.

Festlegen von Standardwerten

Nachdem Sie eine Verbindung zu einem Integration Service mit *pmcmd* hergestellt haben, können Sie Standardordner oder Bedingungen festlegen, die jedes Mal verwendet werden sollen, wenn der Integration Service einen Befehl ausführt. Wenn Sie beispielsweise eine Reihe von Befehlen oder Aufgaben im selben Ordner eingeben möchten, geben Sie den Namen des Ordners mit dem setfolder-Befehl an. Alle nachfolgenden Befehle verwenden standardmäßig diesen Ordner.

In der folgenden Tabelle werden die Befehle beschrieben, mit denen Sie Standardwerte für nachfolgende Befehle festlegen:

Befehl	Beschreibung
setfolder	Legt einen Ordner als Standardordner fest, in dem alle nachfolgenden Befehle ausgeführt werden sollen.
setnowait	Führt nachfolgende Befehle im nowait-Modus aus. Die *pmcmd*-Eingabeaufforderung ist verfügbar, nachdem der Integration Service den vorangegangenen Befehl erhalten hat. Der nowait-Modus fungiert als Standardmodus.
setwait	Führt nachfolgende Befehle im wait-Modus aus. Die *pmcmd*-Eingabeaufforderung steht nach Abschluss des vorherigen Befehls durch den Integration Service zur Verfügung.
unsetfolder	Kehrt den setfolder-Befehl um.

Sie können mit dem *pmcmd* ShowSettings-Befehl die Standardeinstellungen anzeigen.

Ausführen im wait-Modus

Sie können *pmcmd* im wait- oder nowait-Modus ausführen. Im wait-Modus kehrt *pmcmd* nach Abschluss des Befehls zur Shell oder Eingabeaufforderung zurück. Nachfolgende Befehle können erst ausgeführt werden, wenn der vorherige Befehl abgeschlossen ist.

Wenn Sie beispielsweise folgenden Befehl eingeben, startet *pmcmd* den Arbeitsablauf "wf_SalesAvg" und kehrt erst dann zur Eingabeaufforderung zurück, wenn der Arbeitsablauf abgeschlossen ist:

```
pmcmd startworkflow -sv MyIntService -d MyDomain -u seller3 -p jackson -f SalesEast -
wait wf_SalesAvg
```

Im nowait-Modus kehrt *pmcmd* sofort zur Shell oder Eingabeaufforderung zurück. Sie müssen nicht auf den Abschluss eines Befehls warten, bevor Sie den nächsten Befehl ausführen.

Wenn Sie beispielsweise die folgenden Befehle eingeben, startet *pmcmd* den Arbeitsablauf "wf_SalesTotal" selbst dann, wenn der Arbeitsablauf "wf_SalesAvg" noch ausgeführt wird:

```
pmcmd startworkflow -sv MyIntService -d MyDomain -u seller3 -p jackson -f SalesEast
wf_SalesAvg
pmcmd startworkflow -sv MyIntService -d MyDomain -u seller3 -p jackson -f SalesEast
wf_SalesTotal
```

Standardmäßig führt *pmcmd* Befehle im nowait-Modus aus.

Sie können den wait-Modus im Befehlszeilen- oder interaktiven Modus konfigurieren. Verwenden Sie im Befehlszeilenmodus die Option -wait, um einen Befehl im wait-Modus auszuführen. Verwenden Sie im interaktiven Modus den Befehl setwait oder setnowait, bevor Sie nachfolgende Befehle eingeben.

Scripting von pmcmd-Befehlen

Bei Einsatz von *pmcmd* verwenden Sie möglicherweise regelmäßig einige Befehle mit bestimmten Optionen und Argumenten. Sie verwenden *pmcmd* beispielsweise, um den Status des Integration Service zu überprüfen. In diesem Fall können Sie ein Skript oder eine Batchdatei erstellen, um einen oder mehrere *pmcmd*-Befehle einschließlich der zugehörigen Optionen und Argumente aufzurufen.

Sie können Skripts in Befehlszeilenmodus ausführen. Sie können *pmcmd*-Skripts nicht im interaktiven Modus ausführen.

Das folgende UNIX-Shell-Skript überprüft beispielsweise den Status von Integration Service "testService" und falls dieser ausgeführt wird, werden Details für die Sitzung "s_testSessionTask" abgerufen:

```
#!/usr/bin/bash
# Sample pmcmd script
# Check if the service is alive

pmcmd pingservice -sv testService -d testDomain
if [ "$?" != 0 ]; then

    # handle error

    echo "Could not ping service"

    exit

fi
# Get service properties

pmcmd getserviceproperties  -sv testService -d testDomain
if [ "$?" != 0 ]; then

    # handle error

    echo "Could not get service properties"

    exit

fi
# Get task details for session task "s_testSessionTask" of workflow

# "wf_test_workflow" in folder "testFolder"

pmcmd gettaskdetails -sv testService -d testDomain -u Administrator -p adminPass -folder
testFolder -workflow wf_test_workflow s_testSessionTask
if [ "$?" != 0 ]; then

    # handle error

    echo "Could not get details for task s_testSessionTask"

    exit

fi
```

Eingeben von Befehlsoptionen

pmcmd bietet mehrere Möglichkeiten zur Eingabe bestimmter Befehlsoptionen und -argumente. Verwenden Sie beispielsweise zur Eingabe eines Passworts die folgende Syntax:

```
<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>
```

Um ein Passwort einzugeben, stellen Sie dem Passwort die Option -password oder -p voran:

```
-password ThePassword
or
-p ThePassword
```

Wenn Sie eine Passwort-Umgebungsvariable verwenden, stellen Sie dem Variablennamen die Option -pv oder -passwordvar voran:

```
-passwordvar PASSWORD
or
-pv PASSWORD
```

Wenn eine Befehlsoption Leerzeichen enthält, schließen Sie die Option in einfache oder doppelte Anführungszeichen ein. Verwenden Sie zum Beispiel einfache Anführungszeichen in der folgenden Syntax, um den Ordnernamen einzuschließen:

```
abortworkflow -sv MyIntService -d MyDomain -u seller3 -p jackson -f 'quarterly sales' -
wait wf_MyWorkflow
```

Um einen leeren String zu kennzeichnen, verwenden Sie zwei einfache Anführungszeichen (') oder zwei doppelte Anführungszeichen ("").

AbortTask

Bricht eine Aufgabe ab. Verwenden Sie diesen Befehl nur dann, wenn der Integration Service die Aufgabe bei Verwendung des Befehls stoptask nicht anhalten kann.

Der Befehl AbortTask verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd AbortTask

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

<-workflow|-w> workflow

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

[-wait|-nowait]

taskInstancePath
```

Der Befehl AbortTask verwendet die folgende Syntax im interaktiven Modus:

```
AbortTask

[<-folder|-f> folder]

<-workflow|-w> workflow

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

[-wait|-nowait]

taskInstancePath
```

In der folgenden Tabelle werden *pmcmd* AbortTask-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich im Befehlszeilenmodus. Name des Integration Service. Wird im interaktiven Modus nicht verwendet.
-domain -d	domain	Optional im Befehlszeilenmodus. Domänenname. Wird im interaktiven Modus nicht verwendet.
-timeout -t	timeout	Optional im Befehlszeilenmodus. Zeitraum (in Sekunden), während dem *pmcmd* versucht, eine Verbindung mit dem Integration Service herzustellen. Wird im interaktiven Modus nicht verwendet. Wurde die -timeout-Option weggelassen, verwendet *pmcmd* den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet *pmcmd* den standardmäßigen Timeout-Wert. Die Standardeinstellung ist "180".
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Benutzername-Umgebungsvariable nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Gibt die Benutzername-Umgebungsvariable an. Wird im interaktiven Modus nicht verwendet.
-password -p	passwort	Erforderlich im Befehlszeilenmodus, wenn Sie die Passwort-Umgebungsvariable nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Passwort-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Die Standardeinstellung ist "Native".
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Sicherheitsdomäne-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-folder -f	folder	Erforderlich, wenn der Aufgabenname im Repository nicht eindeutig ist. Name des Ordners, der die Aufgabe enthält.
-workflow -w	arbeitsablauf	Erforderlich. Name des Arbeitsablaufs.

Option	Argument	Beschreibung
-warten -nowait	-	Optional. Konfiguriert den Wartemodus: - warten. Sie können einen neuen *pmcmd*-Befehl erst eingeben, wenn der Integration Service den vorherigen Befehl ausgeführt hat. - nowait. Sie können einen neuen *pmcmd*-Befehl eingeben, wenn der Integration Service den vorherigen Befehl empfangen hat. Als Standardwert wird nowait verwendet.
-runinsname -rn	runInsName	Name der Arbeitsablaufausführungsinstanz, die die abzubrechende Aufgabe enthält. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen.
-wfrunid	workflowRunId	Führen Sie die ID-Nummer (Ausführungs-ID) der Arbeitsablaufausführungsinstanz aus, die die abzubrechende Aufgabe enthält. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen. **Hinweis:** Verwenden Sie diese Option, wenn der Arbeitsablauf keinen eindeutigen Ausführungsinstanznamen aufweist.
-	taskInstancePath	Gibt einen Aufgabennamen und dessen Position im Arbeitsablauf an. Befindet sich die Aufgabe in einem Arbeitsablauf, geben Sie nur den Aufgabennamen ein. Befindet sich die Aufgabe in einem Worklet, geben Sie WorkletName.TaskName ein. Geben Sie taskInstancePath als vollständig qualifizierten String ein.

abortworkflow

Bricht einen Arbeitsablauf ab. Verwenden Sie diesen Befehl nur dann, wenn der Integration Service den Arbeitsablauf bei Verwendung des Befehls stopworkflow nicht anhalten kann.

Der Befehl abortworkflow verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd abortworkflow

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

[-wait|-nowait]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

workflow
```

Der Befehl abortworkflow verwendet die folgende Syntax im interaktiven Modus:

```
abortworkflow

[<-folder|-f> folder]

[-wait|-nowait]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

workflow
```

In der folgenden Tabelle werden *pmcmd* abortworkflow-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich im Befehlszeilenmodus. Name des Integration Service. Wird im interaktiven Modus nicht verwendet.
-domain -d	domain	Optional im Befehlszeilenmodus. Domänenname. Wird im interaktiven Modus nicht verwendet.
-timeout -t	timeout	Optional im Befehlszeilenmodus. Zeitraum (in Sekunden), während dem *pmcmd* versucht, eine Verbindung mit dem Integration Service herzustellen. Wird im interaktiven Modus nicht verwendet. Wurde die -timeout-Option weggelassen, verwendet *pmcmd* den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet *pmcmd* den standardmäßigen Timeout-Wert. Die Standardeinstellung ist "180".
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Benutzername-Umgebungsvariable nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Benutzername-Umgebungsvariable an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.
-password -p	passwort	Erforderlich im Befehlszeilenmodus, wenn Sie die Passwort-Umgebungsvariable nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Passwort-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Die Standardeinstellung ist "Native".
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Sicherheitsdomäne-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.

Option	Argument	Beschreibung
-folder -f	folder	Erforderlich, wenn der Name des Arbeitsablaufs im Repository nicht eindeutig ist. Name des Ordners, der den Arbeitsablauf enthält.
-warten -nowait	-	Optional. Konfiguriert den Wartemodus: - warten. Sie können einen neuen *pmcmd*-Befehl erst eingeben, wenn der Integration Service den vorherigen Befehl ausgeführt hat. - nowait. Sie können einen neuen *pmcmd*-Befehl eingeben, wenn der Integration Service den vorherigen Befehl empfangen hat. Als Standardwert wird nowait verwendet.
-runinsname -rin	runInsName	Name der abzubrechenden Arbeitsablaufausführungsinstanz. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen.
-wfrunid	workflowRunId	Führen Sie die ID-Nummer (Ausführungs-ID) der Arbeitsablaufausführungsinstanz aus, die abgebrochen werden soll. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen. **Hinweis:** Verwenden Sie diese Option, wenn der Arbeitsablauf keinen eindeutigen Ausführungsinstanznamen aufweist.
-	arbeitsablauf	Erforderlich. Name des Arbeitsablaufs.

Connect

Verbindet das *pmcmd*-Programm mit dem Integration Service im interaktiven Modus. Wenn Sie Verbindungsinformationen weglassen, werden Sie von *pmcmd* zur Eingabe der korrekten Daten aufgefordert. Nach erfolgreicher Verbindungsherstellung mithilfe von *pmcmd* können Sie Befehle verwenden, ohne erneut Verbindungsinformationen eingeben zu müssen.

```
Connect

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]
```

Hinweis: Verwenden Sie diesen Befehl ausschließlich im interaktiven *pmcmd*-Modus.

In der folgenden Tabelle werden *pmcmd* Connect-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integration Service.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem *pmcmd* versucht, eine Verbindung mit dem Integration Service herzustellen. Wurde die -timeout-Option weggelassen, verwendet *pmcmd* den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet *pmcmd* den standardmäßigen Timeout-Wert. Die Standardeinstellung ist "180".
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Benutzername-Umgebungsvariable nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Benutzername-Umgebungsvariable an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.
-password -p	passwort	Erforderlich im Befehlszeilenmodus, wenn Sie die Passwort-Umgebungsvariable nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Passwort-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Die Standardeinstellung ist "Native".
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Sicherheitsdomäne-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.

Disconnect

Trennt *pmcmd* vom Integration Service. Das *pmcmd*-Programm wird nicht geschlossen. Verwenden Sie diesen Befehl, wenn Sie eine Trennung von einem Integration Service vornehmen und eine Verbindung zu einem anderen Integration Service im interaktiven Modus herstellen möchten.

Der Befehl Disconnect verwendet folgende Syntax im interaktiven Modus:

```
Disconnect
```

Hinweis: Verwenden Sie diesen Befehl ausschließlich im interaktiven *pmcmd*-Modus.

Exit

Trennt *pmcmd* vom Integration Service und schließt das *pmcmd*-Programm.

Der Befehl Exit verwendet die folgende Syntax im interaktiven Modus:

```
Exit
```

Hinweis: Verwenden Sie diesen Befehl ausschließlich im interaktiven *pmcmd*-Modus.

GetRunningSessionsDetails

Gibt die folgenden Details für alle Sitzungen an, die aktuell auf einem Integration Service ausgeführt werden:

- Integration Service-Status, Startzeit und aktuelle Zeit
- Ordner und Name des Arbeitsablaufs
- Worklet und Sitzungsinstanz
- Bei jeder Ausführung der Sitzung: Aufgabentyp, Startzeit, Ausführungsstatus, erster Fehlercode, zugeordneter Integration Service, Ausführungsmodus und Knotenname
- Für das Mapping in einer laufenden Sitzung: Name des Mappings, Sitzungsprotokolldatei, erster Fehlercode und Fehlermeldung, Anzahl der erfolgreichen und fehlgeschlagenen Quell- und Zielzeilen und der Anzahl der Transformationsfehlermeldungen
- Anzahl der Sitzungen, die im Integration Service ausgeführt werden

Der Befehl GetRunningSessionsDetails verwendet die folgende Syntax im Befehlszeilenmodus.

```
pmcmd GetRunningSessionsDetails

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]
```

Der Befehl GetRunningSessionsDetails verwendet die folgende Syntax im interaktiven Modus:

```
GetRunningSessionsDetails
```

In der folgenden Tabelle werden *pmcmd* GetRunningSessionsDetails-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integration Service.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem *pmcmd* versucht, eine Verbindung mit dem Integration Service herzustellen. Wurde die -timeout-Option weggelassen, verwendet *pmcmd* den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet *pmcmd* den standardmäßigen Timeout-Wert. Die Standardeinstellung ist "180".
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Benutzername-Umgebungsvariable nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Benutzername-Umgebungsvariable an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.
-password -p	passwort	Erforderlich im Befehlszeilenmodus, wenn Sie die Passwort-Umgebungsvariable nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Passwort-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Die Standardeinstellung ist "Native".
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Sicherheitsdomäne-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.

GetServiceDetails

Gibt die folgenden Informationen zu einem Integration Service zurück:

- Name des Integration Service, Status, Startzeit und die aktuelle Zeit
- Für jeden aktiven Arbeitsablauf: Ordnername, Name des Arbeitsablaufs, Version, Ausführungsstatus, erster Fehlercode, Startzeit, Protokolldatei, Ausführungstyp und Benutzer, der den Arbeitsablauf ausführt

- Für jede aktive Aufgabe: Ordnername, Name und Version des Arbeitsablaufs, Name und Version der Aufgabeninstanz, Aufgabentyp, Start- und Endzeit, Ausführungsstatus, erster Fehlercode, Fehlermeldung, zugeordneter Integration Service, Ausführungsmodus, Namen der Knoten, auf denen die Aufgabe ausgeführt wird
- Anzahl der geplanten, aktiven und wartenden Arbeitsabläufe und Sitzungen

Der Befehl GetServiceDetails verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd GetServiceDetails

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[-all|-running|-scheduled]
```

Der Befehl GetServiceDetails verwendet die folgende Syntax im interaktiven Modus:

```
GetServiceDetails

[-all|-running|-scheduled]
```

In der folgenden Tabelle werden *pmcmd* GetServiceDetails-Optionen und Argumente beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integration Service.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem *pmcmd* versucht, eine Verbindung mit dem Integration Service herzustellen. Wurde die -timeout-Option weggelassen, verwendet *pmcmd* den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet *pmcmd* den standardmäßigen Timeout-Wert. Die Standardeinstellung ist "180".
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Benutzername-Umgebungsvariable nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Benutzername-Umgebungsvariable an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.
-password -p	passwort	Erforderlich im Befehlszeilenmodus, wenn Sie die Passwort-Umgebungsvariable nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.

Option	Argument	Beschreibung
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Passwort-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Die Standardeinstellung ist "Native".
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Sicherheitsdomäne-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-all -running -scheduled	-	Optional. Gibt die Arbeitsabläufe an, für die Details zurückgegeben werden sollen: - all. Gibt Statusdetails zu den geplanten und laufenden Arbeitsabläufen zurück. - running. Gibt Statusdetails zu aktiven Arbeitsabläufen zurück. Aktive Arbeitsabläufe, einschließlich laufenden, ausstehenden und ausgesetzten Arbeitsabläufen. - scheduled. Gibt Statusdetails zu den geplanten Arbeitsabläufen zurück. Die Standardeinstellung ist "all".

GetServiceProperties

Gibt die folgenden Informationen über den PowerCenter Integration Service zurück:

- Domäne, in der der PowerCenter Integration Service ausgeführt wird
- Name und Version des PowerCenter Integration Service
- Ob der PowerCenter Integration Service die Ausführung von Debug-Mappings zulässt
- Datenverschiebungsmodus
- Zugeordneter Repository Service
- Aktuelle Zeitstempel und Startzeit
- Name des Rasters
- Namen, Knoten und Codeseiten für die zugeordneten PowerCenter Integration Service-Prozesse
- Betriebsmodus für den PowerCenter Integration Service

Der Befehl GetServiceProperties verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd GetServiceProperties

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>
```

Der Befehl GetServiceProperties verwendet die folgende Syntax im interaktiven Modus:

```
GetServiceProperties
```

In der folgenden Tabelle werden *pmcmd* GetServiceProperties-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des PowerCenter Integration Service.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem *pmcmd* versucht, eine Verbindung mit dem PowerCenter Integration Service herzustellen. Wurde die -timeout-Option weggelassen, verwendet *pmcmd* den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet *pmcmd* den standardmäßigen Timeout-Wert. Die Standardeinstellung ist "180".

getsessionstatistics

Gibt Sitzungsdetails und -statistiken zurück. Der Befehl gibt die folgenden Informationen zurück:

- Ordnername, Name des Arbeitsablaufs, Worklet oder Sitzungsinstanz und Mapping-Name
- Name und Speicherort der Sitzungsprotokolldatei
- Anzahl der erfolgreichen und fehlgeschlagenen Quell- und Zielzeilen
- Anzahl der Transformationsfehler
- Erster Fehlercode und Fehlermeldung
- Aufgabenausführungsstatus
- Name des zugeordneten Integration Service
- Raster und Namen der Knoten, auf denen die Sitzung ausgeführt wird

Der Befehl gibt auch die folgenden Informationen für jede Partition zurück:

- Partitionsname
- Für jede Transformation innerhalb einer Partition: Transformationsinstanz, Transformationsname, Anzahl der angewendeten, betroffenen und zurückgewiesenen Zeilen, Durchsatz, letzter Fehlercode, Start- und Endzeit

Der Befehl getsessionstatistics verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd getsessionstatistics

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]
```

```
[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

<-workflow|-w> workflow

taskInstancePath
```

Der Befehl getsessionstatistics verwendet die folgende Syntax im interaktiven Modus:

```
getsessionstatistics

[<-folder|-f> folder]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

<-workflow|-w> workflow

taskInstancePath
```

In der folgenden Tabelle werden *pmcmd* getsessionstatistics-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integration Service.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem *pmcmd* versucht, eine Verbindung mit dem Integration Service herzustellen. Wurde die -timeout-Option weggelassen, verwendet *pmcmd* den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet *pmcmd* den standardmäßigen Timeout-Wert. Die Standardeinstellung ist "180".
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Benutzername-Umgebungsvariable nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Benutzername-Umgebungsvariable an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.
-password -p	passwort	Erforderlich im Befehlszeilenmodus, wenn Sie die Passwort-Umgebungsvariable nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Passwort-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.

Option	Argument	Beschreibung
-usersecuritydomain -usd	usersecuritydomain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Optional im Befehlszeilenmodus. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Die Standardeinstellung ist "Native".
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Sicherheitsdomäne-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-folder -f	folder	Erforderlich, wenn der Aufgabenname im Repository nicht eindeutig ist. Name des Ordners, der die Aufgabe enthält.
-runinsname -rn	runInsName	Name der Arbeitsablaufausführungsinstanz, die die Aufgabe enthält Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen.
-wfrunid	workflowRunId	Führen Sie die ID-Nummer (Ausführungs-ID) der Arbeitsablaufausführungsinstanz aus, die die Aufgabe enthält. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen. **Hinweis:** Verwenden Sie diese Option, wenn der Arbeitsablauf keinen eindeutigen Ausführungsinstanznamen aufweist.
-workflow -w	arbeitsablauf	Erforderlich. Name des Arbeitsablaufs.
-	taskInstancePath	Erforderlich. Gibt einen Aufgabennamen und dessen Position im Arbeitsablauf an. Befindet sich die Aufgabe in einem Arbeitsablauf, geben Sie nur den Aufgabennamen ein. Befindet sich die Aufgabe in einem Worklet, geben Sie WorkletName.TaskName ein. Geben Sie taskInstancePath als vollständig qualifizierten String ein.

GetTaskDetails

Gibt die folgenden Informationen über eine Aufgabe zurück:

- Ordnername, Name des Arbeitsablaufs, Name der Aufgabeninstanz und Aufgabentyp
- Start- und Endzeit der letzten Ausführung
- Aufgabenausführungsstatus, erster Fehlercode und Fehlermeldung
- Raster und Namen der Knoten, auf denen die Aufgabe ausgeführt wird
- Name des zugeordneten Integration Service
- Aufgabenausführungsmodus

Handelt es sich bei der Aufgabe um eine Sitzung, gibt der Befehl darüber hinaus die folgenden Details zurück:

- Mapping und Name der Sitzungsprotokolldatei
- Erster Fehlercode und Meldung
- Erfolgreiche und fehlgeschlagene Quell- und Zieldateien

- Anzahl der Transformationsfehler

Der Befehl GetTaskDetails verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd GetTaskDetails

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]> <<-user|-u>
username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

<-workflow|-w> workflow

[<-runinsname|-rin> runInsName]

taskInstancePath
```

Der Befehl GetTaskDetails verwendet folgende Syntax im interaktiven Modus:

```
GetTaskDetails

[<-folder|-f> folder]

<-workflow|-w> workflow

[<-runinsname|-rin> runInsName]

taskInstancePath
```

In der folgenden Tabelle werden *pmcmd* GetTaskDetails-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integration Service.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem *pmcmd* versucht, eine Verbindung mit dem Integration Service herzustellen. Wurde die -timeout-Option weggelassen, verwendet *pmcmd* den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet *pmcmd* den standardmäßigen Timeout-Wert. Die Standardeinstellung ist "180".
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Benutzername-Umgebungsvariable nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Benutzername-Umgebungsvariable an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.

Option	Argument	Beschreibung
-password -p	passwort	Erforderlich im Befehlszeilenmodus, wenn Sie die Passwort-Umgebungsvariable nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Passwort-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Die Standardeinstellung ist "Native".
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Sicherheitsdomäne-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-folder -f	folder	Erforderlich, wenn der Aufgabenname im Repository nicht eindeutig ist. Name des Ordners, der die Aufgabe enthält.
-workflow -w	arbeitsablauf	Erforderlich, wenn der Aufgabenname im Repository nicht eindeutig ist. Name des Ordners, der die Aufgabe enthält.
-runinsname -rn	runInsName	Name der Arbeitsablaufausführungsinstanz, die die Aufgabe enthält Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen.
-	taskInstancePath	Erforderlich. Gibt einen Aufgabennamen und dessen Position im Arbeitsablauf an. Befindet sich die Aufgabe in einem Arbeitsablauf, geben Sie nur den Aufgabennamen ein. Befindet sich die Aufgabe in einem Worklet, geben Sie WorkletName.TaskName ein. Geben Sie taskInstancePath als vollständig qualifizierten String ein.

GetWorkflowDetails

Gibt die folgenden Informationen über einen Arbeitsablauf zurück:

- Ordner und Namen der Arbeitsabläufe
- Arbeitsablaufausführungsstatus
- Erster Fehlercode und Fehlermeldung
- Start- und Endzeit
- Name der Protokolldatei
- Arbeitsablaufausführungstyp
- Name des Benutzers, der den Arbeitsablauf zuletzt ausgeführt hat
- Name des zugeordneten Integration Service

Der Befehl GetWorkflowDetails verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd GetWorkflowDetails

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

workflow
```

Der Befehl GetWorkflowDetails verwendet folgende Syntax im interaktiven Modus:

```
GetWorkflowDetails

[<-folder|-f> folder]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

workflow
```

In der folgenden Tabelle werden *pmcmd* GetWorkflowDetails-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integration Service.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem *pmcmd* versucht, eine Verbindung mit dem Integration Service herzustellen. Wurde die -timeout-Option weggelassen, verwendet *pmcmd* den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet *pmcmd* den standardmäßigen Timeout-Wert. Die Standardeinstellung ist "180".
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Benutzername-Umgebungsvariable nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Benutzername-Umgebungsvariable an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.

Option	Argument	Beschreibung
-password -p	passwort	Erforderlich im Befehlszeilenmodus, wenn Sie die Passwort-Umgebungsvariable nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Passwort-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Die Standardeinstellung ist "Native".
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Sicherheitsdomäne-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-folder -f	folder	Erforderlich, wenn der Name des Arbeitsablaufs im Repository nicht eindeutig ist. Name des Ordners, der den Arbeitsablauf enthält.
-runinsname -rin	runInsName	Name der Arbeitsablaufausführungsinstanz Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen.
-wfrunid	workflowRunId	Führen Sie die ID-Nummer (Ausführungs-ID) der Arbeitsablaufausführungsinstanz aus. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen. **Hinweis:** Verwenden Sie diese Option, wenn der Arbeitsablauf keinen eindeutigen Ausführungsinstanznamen aufweist.
-	arbeitsablauf	Name des Arbeitsablaufs.

In der folgenden Tabelle werden die verschiedenen Arbeitsablaufstatus beschrieben:

Name des Status	Beschreibung
Abgebrochen	Der Abbruch des Arbeitsablaufs oder der Aufgabe erfolgt durch den Benutzer im Workflow Monitor oder über *pmcmd*. Der Integration Service beendet den DTM-Prozess und bricht die Aufgabe ab. Sie können einen abgebrochenen Arbeitsablauf wiederherstellen, indem Sie den Arbeitsablauf für die Wiederherstellung aktivieren.
Wird abgebrochen	Der Integration Service ist dabei, den Arbeitsablauf abzubrechen.
Deaktiviert	Die Option "Deaktiviert" wird in den Eigenschaften des Arbeitsablaufs vom Benutzer ausgewählt. Der Integration Service führt den deaktivierten Arbeitsablauf erst aus, wenn die Auswahl der Option "Deaktiviert" aufgehoben wird.
Fehlgeschlagen	Der Arbeitsablauf schlägt im Integration Service fehl, da Fehler aufgetreten sind. Ein fehlgeschlagener Arbeitsablauf kann nicht wiederhergestellt werden.
Vorbereitung zum Ausführen	Der Integration Service wartet auf eine Ausführungssperre für den Arbeitsablauf.

Name des Status	Beschreibung
Wird ausgeführt	Der Integration Service führt den Arbeitsablauf aus.
Geplant	Die Ausführung des Arbeitsablaufs wird vom Benutzer an einem künftigen Datum geplant. Der Integration Service führt den Arbeitsablauf für die Dauer des Plans aus.
Gestoppt	Der Arbeitsablauf oder die Aufgabe wird vom Benutzer im Workflow Monitor oder über *pmcmd* gestoppt. Der Integration Service stoppt die Verarbeitung der Aufgabe und aller anderen Aufgaben im zugehörigen Pfad. Der Integration Service setzt die Ausführung paralleler Aufgaben fort. Sie können einen gestoppten Arbeitsablauf wiederherstellen, indem Sie den Arbeitsablauf für die Wiederherstellung aktivieren.
Anhalgen	Der Integration Service ist dabei, den Arbeitsablauf zu stoppen.
Erfolgreich	Der Integration Service hat den Arbeitsablauf erfolgreich abgeschlossen.
Unterbrochen	Der Integration Service unterbricht den Arbeitsablauf, da eine Aufgabe fehlgeschlagen ist und keine anderen Aufgaben im Arbeitsablauf ausgeführt werden. Dieser Status ist verfügbar, wenn Sie die Option zum Unterbrechen bei Auftreten eines Fehlers ausgewählt haben. Sie können einen ausgesetzten Arbeitsablauf wiederherstellen.
Ausstehend	Eine Aufgabe im Arbeitsablauf schlägt fehl, während andere Aufgaben weiterhin ausgeführt werden. Der Integration Service stoppt die Ausführung der fehlgeschlagenen Aufgabe und fährt mit der Ausführung der Aufgaben in anderen Pfaden fort. Dieser Status ist verfügbar, wenn Sie die Option zum Unterbrechen bei Auftreten eines Fehlers ausgewählt haben.
Beendet	Der Integration Service wird beim Ausführen dieses Arbeitsablaufs oder dieser Aufgabe unerwartet beendet. Sie können einen beendeten Arbeitsablauf wiederherstellen, wenn Sie den Arbeitsablauf für die Wiederherstellung aktivieren.
Wird beendet	Der Integration Service ist dabei, den Arbeitsablauf oder die Aufgabe zu beenden.
Unbekannter Status	Dieser Status wird in den folgenden Situationen angezeigt: - Der Integration Service kann den Status des Arbeitsablaufs oder der Aufgabe nicht bestimmen. - Der Integration Service reagiert nicht auf ein Ping vom Workflow-Monitor. - Der Workflow Monitor kann während des Zeitraums für das Belastbarkeits-Timeout keine Verbindung zum Integration Service herstellen.
Außerplanmäßig	Ein Arbeitsablauf wird vom Benutzer aus dem Plan entfernt.
Wartet	Der Integration Service wartet auf verfügbare Ressourcen, um den Arbeitsablauf oder die Aufgabe auszuführen. Sie können beispielsweise die maximale Anzahl der laufenden Sitzungs- und Befehlsaufgaben, die pro Integration Service-Prozess auf dem Knoten zulässig sind, auf 10 festlegen. Wenn der Integration Service bereits 10 parallele Sitzungen ausführt, weisen alle anderen Arbeitsabläufe und Aufgaben den Status "Wartet" auf, bis der Integration Service wieder ausreichend freie Ressourcen hat, um weitere Aufgaben auszuführen.

Der Befehl GetWorkflowDetails zeigt die letzten Details des Arbeitsablaufausführungstyps an. Arbeitsablaufausführungstypen beziehen sich auf die zum Starten des Arbeitsablaufs verwendete Methode.

In der folgenden Tabelle werden die verschiedenen Arbeitsablaufausführungstypen mit dem Befehl getworkflowdetails beschrieben:

Arbeitsablaufausführungstypen	Beschreibung
Benutzeranfrage	Manuell gestarteter Arbeitsablauf.
Plan	Arbeitsablauf wird zum geplanten Zeitpunkt ausgeführt.

Hilfe

Gibt die Syntax für den angegebenen Befehl zurück. Wenn Sie den Befehlsnamen weglassen, listet *pmcmd* alle Befehle und deren Syntax auf.

Der Befehl Help verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd Help [command]
```

Der Befehl Help verwendet die folgende Syntax im interaktiven Modus:

```
Help [command]
```

In der folgenden Tabelle werden die *pmcmd* Help-Option und das -Argument beschrieben:

Option	Argument	Beschreibung
-	befehl	Optional. Name des Befehls. Wenn Sie den Befehlsnamen weglassen, listet *pmcmd* alle Befehle und deren Syntax auf.

PingService

Stellt sicher, dass der Integration Service ausgeführt wird.

Der Befehl PingService verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd PingService
```

```
<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>
```

Der Befehl PingService verwendet die folgende Syntax im interaktiven Modus:

```
PingService
```

In der folgenden Tabelle werden *pmcmd* PingService-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integration Service.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem *pmcmd* versucht, eine Verbindung mit dem Integration Service herzustellen. Wurde die -timeout-Option weggelassen, verwendet *pmcmd* den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet *pmcmd* den standardmäßigen Timeout-Wert. Die Standardeinstellung ist "180".

RecoverWorkflow

Stellt ausgesetzte Arbeitsabläufe wieder her. Geben Sie zum Wiederherstellen eines Arbeitsablaufs den Namen und Ordner für den Arbeitsablauf ein. Der Integration Service stellt den Arbeitsablauf aus allen unterbrochenen und fehlgeschlagenen Worklets sowie aus allen ausgesetzten und fehlgeschlagenen Befehls-, E-Mail- und Sitzungsaufgaben wieder her.

Der Befehl ArbeitsflussWiederherstellen verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd RecoverWorkflow

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

[<-paramfile> paramfile]

[<-localparamfile|-lpf> localparamfile]

[-wait|-nowait]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

workflow
```

Der Befehl ArbeitsflussWiederherstellen verwendet die folgende Syntax im interaktiven Modus:

```
RecoverWorkflow

[<-folder|-f> folder]
```

```
[<-paramfile> paramfile]

[<-localparamfile|-lpf> localparamfile]

[-wait|-nowait]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

workflow
```

In der folgenden Tabelle werden *pmcmd*-ArbeitsflussWiederherstellen-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integration Service.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem *pmcmd* versucht, eine Verbindung mit dem Integration Service herzustellen. Wurde die -timeout-Option weggelassen, verwendet *pmcmd* den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet *pmcmd* den standardmäßigen Timeout-Wert. Die Standardeinstellung ist "180".
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Benutzername-Umgebungsvariable nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Benutzername-Umgebungsvariable an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.
-password -p	passwort	Erforderlich im Befehlszeilenmodus, wenn Sie die Passwort-Umgebungsvariable nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Passwort-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Die Standardeinstellung ist "Native".
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Sicherheitsdomäne-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.

Option	Argument	Beschreibung
-folder -f	folder	Erforderlich, wenn der Name des Arbeitsablaufs im Repository nicht eindeutig ist. Name des Ordners, der den Arbeitsablauf enthält.
-paramfile	paramfile	Optional. Bestimmt die bei Ausführung einer Aufgabe oder eines Arbeitsablaufs zu verwendende Parameterdatei. Sie überschreibt die konfigurierte Parameterdatei für den Arbeitsablauf oder die Aufgabe.
-localparamfile -lpf	localparamfile	Optional. Gibt die Parameterdatei auf einem lokalen Computer an, die von *pmcmd* beim Start eines Arbeitsablaufs verwendet wird.
-warten -nowait	-	Optional. Konfiguriert den Wartemodus: - warten. Sie können einen neuen *pmcmd*-Befehl erst eingeben, wenn der Integration Service den vorherigen Befehl ausgeführt hat. - nowait. Sie können einen neuen *pmcmd*-Befehl eingeben, wenn der Integration Service den vorherigen Befehl empfangen hat. Als Standardwert wird nowait verwendet.
-runinsname -rin	runInsName	Name der Arbeitsablaufausführungsinstanz, die wiederhergestellt werden soll. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen.
-wfrunid	workflowRunId	Führen Sie die ID-Nummer (Ausführungs-ID) der Arbeitsablaufausführungsinstanz aus, die wiederhergestellt werden soll. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen. **Hinweis:** Verwenden Sie diese Option, wenn der Arbeitsablauf keinen eindeutigen Ausführungsinstanznamen aufweist.
-	arbeitsablauf	Erforderlich. Name des Arbeitsablaufs.

ScheduleWorkflow

Weist den Integration Service an, einen Arbeitsablauf zu planen. Verwenden Sie diesen Befehl zum erneuten Planen eines Arbeitsablaufs, der aus dem Plan entfernt wurde.

Der Befehl ScheduleWorkflow verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd ScheduleWorkflow

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]
```

```
workflow
```

Der Befehl ScheduleWorkflow verwendet folgende Syntax im interaktiven Modus:

```
ScheduleWorkflow

[<-folder|-f> folder]

workflow
```

In der folgenden Tabelle werden *pmcmd* ScheduleWorkflow-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integration Service.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem *pmcmd* versucht, eine Verbindung mit dem Integration Service herzustellen. Wurde die -timeout-Option weggelassen, verwendet *pmcmd* den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet *pmcmd* den standardmäßigen Timeout-Wert. Die Standardeinstellung ist "180".
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Benutzername-Umgebungsvariable nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Benutzername-Umgebungsvariable an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.
-password -p	passwort	Erforderlich im Befehlszeilenmodus, wenn Sie die Passwort-Umgebungsvariable nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Passwort-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Die Standardeinstellung ist "Native".
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Sicherheitsdomäne-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.

Option	Argument	Beschreibung
-folder -f	folder	Erforderlich, wenn der Name des Arbeitsablaufs im Repository nicht eindeutig ist. Name des Ordners, der den Arbeitsablauf enthält.
-	arbeitsablauf	Erforderlich. Name des Arbeitsablaufs.

SetFolder

Legt einen Ordner als Standardordner fest, in dem alle nachfolgenden Befehle ausgeführt werden sollen. Nach Ausgabe dieses Befehls muss kein Ordnername für Arbeitsablauf-, Aufgaben- oder Sitzungsbefehle eingegeben werden. Wenn Sie nach dem Befehl SetFolder in einem Befehl einen Ordnernamen eingeben, überschreibt dieser Ordnername den Namen des Standardordners für ausschließlich diesen Befehl.

Der Befehl SetFolder verwendet folgende Syntax im interaktiven Modus:

```
SetFolder folder
```

Hinweis: Verwenden Sie diesen Befehl ausschließlich im interaktiven *pmcmd*-Modus.

In der folgenden Tabelle werden die *pmcmd* SetFolder-Option und das -Argument beschrieben:

Option	Argument	Beschreibung
-	folder	Erforderlich. Name des Ordners.

SetNoWait

Sie können *pmcmd* im wait- oder nowait-Modus ausführen. Im wait-Modus kehrt *pmcmd* nach Abschluss des Befehls zur Shell oder Eingabeaufforderung zurück. Nachfolgende Befehle können erst ausgeführt werden, wenn der vorherige Befehl abgeschlossen ist. Im nowait-Modus kehrt *pmcmd* sofort zur Shell oder Eingabeaufforderung zurück. Sie müssen nicht auf den Abschluss eines Befehls warten, bevor Sie den nächsten Befehl ausführen.

Der Befehl SetNoWait führt *pmcmd* im nowait-Modus aus. Der nowait-Modus fungiert als Standardmodus.

Der Befehl SetNoWait verwendet die folgende Syntax im interaktiven Modus:

```
SetNoWait
```

Wenn Sie den nowait-Modus einrichten, verwenden Sie nach Ausführung des vorherigen Befehls durch den Integration Service die *pmcmd*-Eingabeaufforderung.

Hinweis: Verwenden Sie diesen Befehl ausschließlich im interaktiven *pmcmd*-Modus.

SetWait

Sie können *pmcmd* im wait- oder nowait-Modus ausführen. Im wait-Modus kehrt *pmcmd* nach Abschluss des Befehls zur Shell oder Eingabeaufforderung zurück. Nachfolgende Befehle können erst ausgeführt werden, wenn der vorherige Befehl abgeschlossen ist. Im nowait-Modus kehrt *pmcmd* sofort zur Shell oder Eingabeaufforderung zurück. Sie müssen nicht auf den Abschluss eines Befehls warten, bevor Sie den nächsten Befehl ausführen.

Der Befehl SetWait führt *pmcmd* im wait-Modus aus. Die *pmcmd*-Eingabeaufforderung steht nach Abschluss des vorherigen Befehls durch den Integration Service zur Verfügung.

Der Befehl SetWait verwendet die folgende Syntax im interaktiven Modus:

```
SetWait
```

Hinweis: Verwenden Sie diesen Befehl ausschließlich im interaktiven *pmcmd*-Modus.

ShowSettings

Gibt den Namen der Domäne, des Integration Service und Repositorys zurück, mit dem *pmcmd* verbunden ist. Angezeigt werden Benutzername, wait-Modus und Standardordner.

Der Befehl ShowSettings verwendet folgende Syntax im interaktiven Modus:

```
ShowSettings
```

Hinweis: Verwenden Sie diesen Befehl ausschließlich im interaktiven *pmcmd*-Modus.

StartTask

Startet eine Aufgabe.

Der Befehl StartTask verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd StartTask

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

<-workflow|-w> workflow

[<-paramfile> paramfile]

[-wait|-nowait]

[<-recovery|-norecovery>]

[<-runinsname|-rin> runInsName]
```

```
taskInstancePath
```

Der Befehl StartTask verwendet die folgende Syntax im interaktiven Modus:

```
pmcmd StartTask

[<-folder|-f> folder]

<-workflow|-w> workflow

<-paramfile> paramfile]

[-wait|-nowait]

[<-recovery|-norecovery>]

[<-runinsname|-rin> runInsName]

taskInstancePath
```

In der folgenden Tabelle werden *pmcmd* StartTask-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integration Service.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem *pmcmd* versucht, eine Verbindung mit dem Integration Service herzustellen. Wurde die -timeout-Option weggelassen, verwendet *pmcmd* den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet *pmcmd* den standardmäßigen Timeout-Wert. Die Standardeinstellung ist "180".
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Benutzername-Umgebungsvariable nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Benutzername-Umgebungsvariable an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.
-password -p	passwort	Erforderlich im Befehlszeilenmodus, wenn Sie die Passwort-Umgebungsvariable nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Passwort-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.

Option	Argument	Beschreibung
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Die Standardeinstellung ist "Native".
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Sicherheitsdomäne-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-folder -f	folder	Erforderlich, wenn der Name des Arbeitsablaufs im Repository nicht eindeutig ist. Name des Ordners, der den Arbeitsablauf enthält.
-workflow -w	arbeitsablauf	Erforderlich. Name des Arbeitsablaufs.
-paramfile	paramfile	Optional. Bestimmt die bei Ausführung einer Aufgabe oder eines Arbeitsablaufs zu verwendende Parameterdatei. Sie überschreibt die konfigurierte Parameterdatei für den Arbeitsablauf oder die Aufgabe.
-warten -nowait	-	Optional. Konfiguriert den Wartemodus: - warten. Sie können einen neuen *pmcmd*-Befehl erst eingeben, wenn der Integration Service den vorherigen Befehl ausgeführt hat. - nowait. Sie können einen neuen *pmcmd*-Befehl eingeben, wenn der Integration Service den vorherigen Befehl empfangen hat. Als Standardwert wird nowait verwendet.

Option	Argument	Beschreibung
-recovery -norecovery	-	Optional. Handelt es sich bei der Aufgabe um eine Sitzung, führt der Integration Service die Sitzung basierend auf der konfigurierten Wiederherstellungsstrategie aus. - recovery. Bei Echtzeitsitzungen, die für die Wiederherstellung aktiviert sind, stellt der Integration Service die fehlgeschlagene Sitzung wieder her und beendet die Ausführung der verbleibenden Aufgaben im Arbeitsablauf. Die Wiederherstellungsoption stimmt mit der Recover Task-Option im Workflow Manager überein. Diese Option ist nicht anwendbar auf Sitzungen, für die keine Wiederherstellung aktiviert wurde. - norecovery. Bei Echtzeitsitzungen, die für die Wiederherstellung aktiviert sind, verarbeitet der Integration Service keine Wiederherstellungsdaten. Der Integration Service löscht vor dem Neustart der Aufgabe den Betriebsstatus sowie die Wiederherstellungsdatei oder -tabelle. Bei Sitzungen, für die keine Wiederherstellung aktiviert wurde, löscht der Integration Service den Betriebsstatus und startet die Aufgabe neu. Die Norecovery-Option stimmt mit der Cold Start Task-Option im Workflow Manager überein. Wenn Sie keine Optionen für Sitzungen bereitstellen, die für die Wiederherstellung aktiviert sind, führt der Integration Service die Sitzung im Recovery-Modus aus. Wenn Sie keine Optionen für Sitzungen bereitstellen, die nicht für die Wiederherstellung aktiviert sind, führt der Integration Service die Sitzung im Norecovery-Modus aus aus.
-runinsname -rn	runInsName	Name der Arbeitsablaufausführungsinstanz, die die zu startende Aufgabe enthält. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen.
-	taskInstancePath	Erforderlich. Gibt einen Aufgabennamen und dessen Position im Arbeitsablauf an. Befindet sich die Aufgabe in einem Arbeitsablauf, geben Sie nur den Aufgabennamen ein. Befindet sich die Aufgabe in einem Worklet, geben Sie WorkletName.TaskName ein. Geben Sie taskInstancePath als vollständig qualifizierten String ein.

Verwenden von Parameterdateien mit starttask

Beim Starten einer Aufgabe können Sie optional das Verzeichnis und den Namen der Parameterdatei eingeben. Der Integration Service führt die Aufgabe mit den in der Datei angegebenen Parametern aus.

UNIX Shell-Benutzer sollten den Parameterdateinamen in einfache Anführungszeichen setzen:

```
-paramfile '$PMRootDir/myfile.txt'
```

Für Benutzer der Windows-Eingabeaufforderung gilt, dass der Parameterdateiname keine Leerzeichen am Anfang oder Ende haben darf. Wenn der Name Leerzeichen enthält, setzen Sie den Dateinamen in doppelte Anführungszeichen:

```
-paramfile "$PMRootDir\my file.txt"
```

Wenn Sie einen *pmcmd*-Befehl schreiben, der eine Parameterdatei enthält, die sich auf einem anderen Computer befindet, verwenden Sie den Backslash (\) mit dem Dollarzeichen ($). Damit wird sichergestellt, dass der Computer, auf dem die Variable definiert ist, die Prozessvariable erweitert.

```
pmcmd starttask -sv MyIntService -d MyDomain -uv USERNAME -pv PASSWORD -f east -w
wSalesAvg -paramfile '\$PMRootDir/myfile.txt' taskA
```

StartWorkflow

Startet einen Arbeitsablauf.

Der Befehl StartWorkflow verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd StartWorkflow

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

[<-startfrom> taskInstancePath]

[<-recovery|-norecovery>]

[<-paramfile> paramfile]

[<-localparamfile|-lpf> localparamfile]

[<-osprofile|-o> OSUser]

[-wait|-nowait]

[<-runinsname|-rin> runInsName]

workflow
```

Der Befehl StartWorkflow verwendet die folgende Syntax im interaktiven Modus:

```
pmcmd StartWorkflow

[<-folder|-f> folder]

[<-startfrom> taskInstancePath [<-recovery|-norecovery>]]

[<-paramfile> paramfile]

[<-localparamfile|-lpf> localparamfile]

[<-osprofile|-o> osProfile]

[-wait|-nowait]

[<-runinsname|-rin> runInsName]

workflow
```

In der folgenden Tabelle werden *pmcmd* StartWorkflow-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integration Service.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem *pmcmd* versucht, eine Verbindung mit dem Integration Service herzustellen. Wurde die -timeout-Option weggelassen, verwendet *pmcmd* den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet *pmcmd* den standardmäßigen Timeout-Wert. Die Standardeinstellung ist "180".
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Benutzername-Umgebungsvariable nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Benutzername-Umgebungsvariable an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.
-password -p	passwort	Erforderlich im Befehlszeilenmodus, wenn Sie die Passwort-Umgebungsvariable nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Passwort-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Die Standardeinstellung ist "Native".
-usersecuritydomainvar -usdv	userSecuritydomainEnv Var	Optional im Befehlszeilenmodus. Sicherheitsdomäne-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-folder -f	folder	Erforderlich, wenn der Name des Arbeitsablaufs im Repository nicht eindeutig ist. Name des Ordners, der den Arbeitsablauf enthält.

Option	Argument	Beschreibung
-startfrom	taskInstancePath	Optional. Startet einen Arbeitsablauf aus einer angegebenen Aufgabe, taskInstancePath. Befindet sich die Aufgabe in einem Arbeitsablauf, geben Sie nur den Aufgabennamen ein. Befindet sich die Aufgabe in einem Worklet, geben Sie WorkletName.TaskName ein. Geben Sie taskInstancePath als vollständig qualifizierten String ein. Wenn Sie keinen Startpunkt angeben, startet der Arbeitsablauf bei der Startaufgabe. Handelt es sich bei der Aufgabe um eine Sitzung, legen Sie die -recovery- oder -norecovery-Option zum Ausführen der Sitzung basierend auf der konfigurierten Wiederherstellungsstrategie fest.
-paramfile	paramfile	Optional. Bestimmt die bei Ausführung einer Aufgabe oder eines Arbeitsablaufs zu verwendende Parameterdatei. Sie überschreibt die konfigurierte Parameterdatei für den Arbeitsablauf oder die Aufgabe.
-recovery -norecovery	-	Optional. Der Integration Service führt die Sitzung basierend auf der konfigurierten Wiederherstellungsstrategie aus. - recovery. Bei Echtzeitsitzungen, die für die Wiederherstellung aktiviert sind, stellt der Integration Service die fehlgeschlagene Sitzung wieder her und beendet die Ausführung der verbleibenden Aufgaben im Arbeitsablauf. Die Recovery-Option stimmt mit der Recover Workflow-Option im Workflow Manager überein. Diese Option ist nicht anwendbar auf Sitzungen, für die keine Wiederherstellung aktiviert wurde. - norecovery. Bei Echtzeitsitzungen, die für die Wiederherstellung aktiviert sind, verarbeitet der Integration Service keine Wiederherstellungsdaten. Der Integration Service löscht vor dem Neustart der Aufgabe den Betriebsstatus sowie die Wiederherstellungsdatei oder -tabelle. Bei Sitzungen, für die keine Wiederherstellung aktiviert wurde, löscht der Integration Service den Betriebsstatus und startet die Aufgabe neu. Die Norecovery-Option stimmt mit der Cold Start Workflow-Option im Workflow Manager überein. Wenn Sie keine Optionen für Sitzungen bereitstellen, die für die Wiederherstellung aktiviert sind, führt der Integration Service die Sitzung im Recovery-Modus aus. Wenn Sie keine Optionen für Sitzungen bereitstellen, die nicht für die Wiederherstellung aktiviert sind, führt der Integration Service die Sitzung im Norecovery-Modus aus aus.
-localparamfile -lpf	localparamfile	Optional. Gibt die Parameterdatei auf einem lokalen Computer an, die von *pmcmd* beim Start eines Arbeitsablaufs verwendet wird.
-osprofile -o	osProfile	Optional. Gibt das dem Arbeitsablauf zugewiesene Betriebssystemprofil an.

Option	Argument	Beschreibung
-warten -nowait	-	Optional. Konfiguriert den Wartemodus: - warten. Sie können einen neuen *pmcmd*-Befehl erst eingeben, wenn der Integration Service den vorherigen Befehl ausgeführt hat. - nowait. Sie können einen neuen *pmcmd*-Befehl eingeben, wenn der Integration Service den vorherigen Befehl empfangen hat. Als Standardwert wird nowait verwendet.
-runinsname -rin	runInsName	Name der zu startenden Arbeitsablaufausführungsinstanz. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen.
-	arbeitsablauf	Erforderlich. Name des Arbeitsablaufs.

Verwenden von Parameterdateien mit startworkflow

Beim Starten eines Arbeitsablaufs können Sie optional das Verzeichnis und den Namen der Parameterdatei eingeben. Der Integration Service führt den Arbeitsablauf mit den in der Datei angegebenen Parametern aus. UNIX Shell-Benutzer sollten den Parameterdateinamen in einfache Anführungszeichen setzen. Für Benutzer der Windows-Eingabeaufforderung gilt, dass der Parameterdateiname keine Leerzeichen am Anfang oder Ende haben darf. Wenn der Name Leerzeichen enthält, setzen Sie den Dateinamen in doppelte Anführungszeichen.

Verwenden Sie Parameterdateien auf den folgenden Computern:

- **Knoten, auf dem Integration Service ausgeführt wird.** Wenn Sie eine Parameterdatei verwenden, die sich auf dem Integration Service-Computer befindet, verwenden Sie die Option -paramfile, um den Speicherort und Namen der Parameterdatei anzugeben.

  Verwenden Sie unter UNIX die folgende Syntax:

  ```
  -paramfile '$PMRootDir/myfile.txt'
  ```

  Verwenden Sie unter Windows die folgende Syntax:

  ```
  -paramfile "$PMRootDir\my file.txt"
  ```

- **Lokaler Rechner.** Wenn Sie eine Parameterdatei verwenden, die sich auf dem Rechner befindet, auf dem *pmcmd* aufrufen wird, übergibt *pmcmd* die Variablen und Werte in der Datei an den Integration Service. Geben Sie beim Erfassen einer lokalen Parameterdatei den absoluten oder relativen Pfad zur Datei an. Verwenden Sie die Option -localparamfile oder -lpf, um den Speicherort und Namen der lokalen Parameterdatei anzugeben.

  Verwenden Sie unter UNIX die folgende Syntax:

  ```
  -lpf 'param_file.txt'

  -lpf 'c:\Informatica\parameterfiles\param file.txt'

  -localparamfile 'c:\Informatica\parameterfiles\param file.txt'
  ```

  Verwenden Sie unter Windows die folgende Syntax:

  ```
  -lpf param_file.txt

  -lpf "c:\Informatica\parameterfiles\param file.txt”

  -localparamfile param_file.txt
  ```

- **Gemeinsam genutzte Netzwerklaufwerke.** Wenn Sie eine Parameterdatei verwenden, die sich auf einem anderen Computer befindet, verwenden Sie den Backslash (\) mit dem Dollarzeichen ($). Damit wird sichergestellt, dass der Computer, auf dem die Variable definiert ist, die Prozessvariable erweitert.

  ```
  -paramfile '\$PMRootDir/myfile.txt'
  ```

StopTask

Hält eine Aufgabe an.

Der Befehl StopTask verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd StopTask

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

[-wait|-nowait]

taskInstancePath
```

Der Befehl StopTask verwendet folgende Syntax im interaktiven Modus:

```
pmcmd StopTask

[<-folder|-f> folder]

<-workflow|-w> workflow

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

[-wait|-nowait]

taskInstancePath
```

In der folgenden Tabelle werden *pmcmd* StopTask-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integration Service.
-domain -d	domain	Optional. Domänenname.

Option	Argument	Beschreibung
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem *pmcmd* versucht, eine Verbindung mit dem Integration Service herzustellen. Wurde die -timeout-Option weggelassen, verwendet *pmcmd* den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet *pmcmd* den standardmäßigen Timeout-Wert. Die Standardeinstellung ist "180".
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Benutzername-Umgebungsvariable nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Benutzername-Umgebungsvariable an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.
-password -p	passwort	Erforderlich im Befehlszeilenmodus, wenn Sie die Passwort-Umgebungsvariable nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Passwort-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Die Standardeinstellung ist "Native".
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Sicherheitsdomäne-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-folder -f	folder	Erforderlich, wenn der Name des Arbeitsablaufs im Repository nicht eindeutig ist. Name des Ordners, der den Arbeitsablauf enthält.
-workflow -w	arbeitsablauf	Erforderlich. Name des Arbeitsablaufs.
-runinsname -rn	runInsName	Name der Arbeitsablaufausführungsinstanz, die die anzuhaltende Aufgabe enthält. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen.
-wfrunid	workflowRunId	Führen Sie die ID-Nummer (Ausführungs-ID) der Arbeitsablaufausführungsinstanz aus, die die anzuhaltende Aufgabe enthält. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen. **Hinweis:** Verwenden Sie diese Option, wenn der Arbeitsablauf keinen eindeutigen Ausführungsinstanznamen aufweist.

Option	Argument	Beschreibung
-warten -nowait	-	Optional. Konfiguriert den Wartemodus: - warten. Sie können einen neuen *pmcmd*-Befehl erst eingeben, wenn der Integration Service den vorherigen Befehl ausgeführt hat. - nowait. Sie können einen neuen *pmcmd*-Befehl eingeben, wenn der Integration Service den vorherigen Befehl empfangen hat. Als Standardwert wird nowait verwendet.
-	taskInstancePath	Erforderlich. Gibt einen Aufgabennamen und dessen Position im Arbeitsablauf an. Befindet sich die Aufgabe in einem Arbeitsablauf, geben Sie nur den Aufgabennamen ein. Befindet sich die Aufgabe in einem Worklet, geben Sie WorkletName.TaskName ein. Geben Sie taskInstancePath als vollständig qualifizierten String ein.

StopWorkflow

Hält einen Arbeitsablauf an.

Der Befehl StopWorkflow verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd StopWorkflow

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

[-wait|-nowait]

workflow
```

Der Befehl StopWorkflow verwendet die folgende Syntax im interaktiven Modus:

```
pmcmd StopWorkflow

[<-folder|-f> folder]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

[-wait|-nowait]

workflow
```

In der folgenden Tabelle werden *pmcmd* StopWorkflow-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integration Service.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem *pmcmd* versucht, eine Verbindung mit dem Integration Service herzustellen. Wurde die -timeout-Option weggelassen, verwendet *pmcmd* den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet *pmcmd* den standardmäßigen Timeout-Wert. Die Standardeinstellung ist "180".
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Benutzername-Umgebungsvariable nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Benutzername-Umgebungsvariable an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.
-password -p	passwort	Erforderlich im Befehlszeilenmodus, wenn Sie die Passwort-Umgebungsvariable nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Passwort-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Die Standardeinstellung ist "Native".
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Sicherheitsdomäne-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-folder -f	folder	Erforderlich, wenn der Name des Arbeitsablaufs im Repository nicht eindeutig ist. Name des Ordners, der den Arbeitsablauf enthält.
-runinsname -rin	runInsName	Name der Arbeitsablaufausführungsinstanz, die angehalten werden soll. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen.

Option	Argument	Beschreibung
-wfrunid	workflowRunId	Führen Sie die ID-Nummer (Ausführungs-ID) der Arbeitsablaufausführungsinstanz aus, die angehalten werden soll. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen. **Hinweis:** Verwenden Sie diese Option, wenn der Arbeitsablauf keinen eindeutigen Ausführungsinstanznamen aufweist.
-warten -nowait	-	Optional. Konfiguriert den Wartemodus: - warten. Sie können einen neuen *pmcmd*-Befehl erst eingeben, wenn der Integration Service den vorherigen Befehl ausgeführt hat. - nowait. Sie können einen neuen *pmcmd*-Befehl eingeben, wenn der Integration Service den vorherigen Befehl empfangen hat. Als Standardwert wird nowait verwendet.
-	arbeitsablauf	Erforderlich. Name des Arbeitsablaufs.

UnscheduleWorkflow

Entfernt einen Arbeitsablauf aus einem Zeitplan.

Der UnscheduleWorkflow-Befehl verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd UnscheduleWorkflow

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

workflow
```

Der UnscheduleWorkflow-Befehl verwendet die folgende Syntax im interaktiven Modus:

```
UnscheduleWorkflow

[<-folder|-f> folder]

workflow
```

In der folgenden Tabelle werden die *pmcmd* UnscheduleWorkflow-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integration Service.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem *pmcmd* versucht, eine Verbindung mit dem Integration Service herzustellen. Wurde die -timeout-Option weggelassen, verwendet *pmcmd* den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet *pmcmd* den standardmäßigen Timeout-Wert. Die Standardeinstellung ist "180".
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Benutzername-Umgebungsvariable nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Benutzername-Umgebungsvariable an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.
-password -p	passwort	Erforderlich im Befehlszeilenmodus, wenn Sie die Passwort-Umgebungsvariable nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Passwort-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Die Standardeinstellung ist "Native".
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Sicherheitsdomäne-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-folder -f	folder	Erforderlich, wenn der Name des Arbeitsablaufs im Repository nicht eindeutig ist. Name des Ordners, der den Arbeitsablauf enthält.
-	arbeitsablauf	Erforderlich. Name des Arbeitsablaufs.

UnsetFolder

Entfernt die Kennzeichnung eines Standardordners. Nachdem Sie diesen Befehl angewendet haben, müssen Sie einen Ordnernamen jedes Mal angeben, wenn Sie einen Befehl für eine Sitzung, einen Arbeitsablauf oder eine Aufgabe eingeben.

Der UnsetFolder-Befehl verwendet die folgende Syntax im interaktiven Modus:

```
UnsetFolder
```

Hinweis: Verwenden Sie diesen Befehl ausschließlich im interaktiven *pmcmd*-Modus.

Version

Zeigt die PowerCenter-Version und Informatica-Handelsmarke sowie Urheberrechtsinformationen an.

Der Version-Befehl verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd Version
```

Der Version-Befehl verwendet die folgende Syntax im interaktiven Modus:

```
Version
```

WaitTask

Weist den Integration Service an, die Aufgabe abzuschließen, bevor die *pmcmd*-Eingabeaufforderung an die Befehlseingabeaufforderung oder Shell zurückgegeben wird.

Der WaitTask-Befehl verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd WaitTask

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

<-workflow|-w> workflow

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

taskInstancePath
```

Der WaitTask-Befehl verwendet die folgende Syntax im interaktiven Modus:

```
WaitTask

[<-folder|-f> folder]

<-workflow|-w> workflow
```

```
[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

taskInstancePath
```

In der folgenden Tabelle werden die *pmcmd* WaitTask-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integration Service.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem *pmcmd* versucht, eine Verbindung mit dem Integration Service herzustellen. Wurde die -timeout-Option weggelassen, verwendet *pmcmd* den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet *pmcmd* den standardmäßigen Timeout-Wert. Die Standardeinstellung ist "180".
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Benutzername-Umgebungsvariable nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Benutzername-Umgebungsvariable an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.
-password -p	passwort	Erforderlich im Befehlszeilenmodus, wenn Sie die Passwort-Umgebungsvariable nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Passwort-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Die Standardeinstellung ist "Native".
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Sicherheitsdomäne-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-folder -f	folder	Erforderlich, wenn der Aufgabenname im Repository nicht eindeutig ist. Name des Ordners, der die Aufgabe enthält.
-workflow -w	arbeitsablauf	Erforderlich. Name des Arbeitsablaufs.

Option	Argument	Beschreibung
-runinsname -rn	runInsName	Name der Arbeitsablaufausführungsinstanz, die die Aufgabe enthält Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen.
-wfrunid	workflowRunId	Führen Sie die ID-Nummer (Ausführungs-ID) der Arbeitsablaufausführungsinstanz aus, die die Aufgabe enthält. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen. **Hinweis:** Verwenden Sie diese Option, wenn der Arbeitsablauf keinen eindeutigen Ausführungsinstanznamen aufweist.
-	taskInstancePath	Erforderlich. Gibt einen Aufgabennamen und dessen Position im Arbeitsablauf an. Befindet sich die Aufgabe in einem Arbeitsablauf, geben Sie nur den Aufgabennamen ein. Befindet sich die Aufgabe in einem Worklet, geben Sie WorkletName.TaskName ein. Geben Sie taskInstancePath als vollständig qualifizierten String ein.

WaitWorkflow

Bewirkt, dass *pmcmd* auf den Abschluss eines Arbeitsablaufs wartet, bevor es nachfolgende Befehle ausführt. Verwenden Sie diesen Befehl in Verbindung mit dem Rückgabewert, wenn Sie *pmcmd* über ein Skript ausführen. Beispielsweise möchten Sie den Status eines kritischen Arbeitsablaufs prüfen, bevor ein anderer Arbeitsablauf gestartet wird. Verwenden Sie den WaitWorkflow-Befehl, um auf den Abschluss des kritischen Arbeitsablaufs zu warten, und überprüfen Sie dann den *pmcmd*-Rückgabewert. Wenn der Rückgabewert 0 ist (erfolgreich), starten Sie den nächsten Arbeitsablauf.

Der WaitWorkflow-Befehl gibt bei Abschluss eines Arbeitsablaufs die Eingabeaufforderung zurück.

Der WaitWorkflow-Befehl verwendet die folgende Syntax im Befehlszeilenmodus:

```
pmcmd WaitWorkflow

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

workflow
```

Der WaitWorkflow-Befehl verwendet die folgende Syntax im interaktiven Modus:

```
WaitWorkflow

[<-folder|-f> folder]

[<-runinsname|-rin> runInsName]
```

```
[-wfrunid workflowRunId]

workflow
```

In der folgenden Tabelle werden die *pmcmd* WaitWorkflow-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-service -sv	service	Erforderlich. Name des Integration Service.
-domain -d	domain	Optional. Domänenname.
-timeout -t	timeout	Optional. Zeitraum (in Sekunden), während dem *pmcmd* versucht, eine Verbindung mit dem Integration Service herzustellen. Wurde die -timeout-Option weggelassen, verwendet *pmcmd* den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT verwendeten Timeout-Wert. Wenn die Umgebungsvariable nicht festgelegt wurde, verwendet *pmcmd* den standardmäßigen Timeout-Wert. Die Standardeinstellung ist "180".
-user -u	username	Erforderlich im Befehlszeilenmodus, wenn Sie die Benutzername-Umgebungsvariable nicht angeben. Benutzername. Wird im interaktiven Modus nicht verwendet.
-uservar -uv	userEnvVar	Gibt die Benutzername-Umgebungsvariable an. Erforderlich im Befehlszeilenmodus, wenn Sie den Benutzernamen nicht angeben. Wird im interaktiven Modus nicht verwendet.
-password -p	passwort	Erforderlich im Befehlszeilenmodus, wenn Sie die Passwort-Umgebungsvariable nicht angeben. Passwort. Wird im interaktiven Modus nicht verwendet.
-passwordvar -pv	passwordEnvVar	Erforderlich im Befehlszeilenmodus, wenn Sie das Passwort nicht angeben. Passwort-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-usersecuritydomain -usd	usersecuritydomain	Optional im Befehlszeilenmodus. Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Wird im interaktiven Modus nicht verwendet. Die Standardeinstellung ist "Native".
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional im Befehlszeilenmodus. Sicherheitsdomäne-Umgebungsvariable. Wird im interaktiven Modus nicht verwendet.
-folder -f	folder	Erforderlich, wenn der Name des Arbeitsablaufs im Repository nicht eindeutig ist. Name des Ordners, der den Arbeitsablauf enthält.
-runinsname -rin	runInsName	Name der Arbeitsablaufausführungsinstanz Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen.

Option	Argument	Beschreibung
-wfrunid	workflowRunId	Führen Sie die ID-Nummer (Ausführungs-ID) der Arbeitsablaufausführungsinstanz aus. Verwenden Sie diese Option, wenn Sie Arbeitsabläufe parallel ausführen. **Hinweis:** Verwenden Sie diese Option, wenn der Arbeitsablauf keinen eindeutigen Ausführungsinstanznamen aufweist.
-	arbeitsablauf	Erforderlich. Name des Arbeitsablaufs.

KAPITEL 33

pmrep-Befehlsreferenz

Dieses Kapitel umfasst die folgenden Themen:

- Verwenden von pmrep, 1148
- AddToDeploymentGroup, 1153
- ApplyLabel, 1155
- AssignIntegrationService, 1157
- AssignPermission, 1158
- BackUp, 1160
- ChangeOwner, 1161
- CheckIn, 1161
- CleanUp, 1162
- ClearDeploymentGroup, 1162
- Connect, 1163
- Create, 1164
- CreateConnection, 1165
- CreateDeploymentGroup, 1168
- CreateFolder, 1169
- CreateLabel, 1171
- Delete, 1171
- DeleteConnection, 1172
- DeleteDeploymentGroup, 1173
- DeleteFolder, 1173
- DeleteLabel, 1173
- DeleteObject , 1174
- DeployDeploymentGroup, 1175
- DeployFolder, 1176
- ExecuteQuery, 1178
- Exit, 1180
- FindCheckout, 1180
- GetConnectionDetails, 1182
- GenerateAbapProgramToFile, 1182
- Hilfe, 1184

- InstallAbapProgram, 1184
- KillUserConnection, 1187
- ListConnections, 1187
- ListObjectDependencies , 1188
- ListObjects, 1190
- ListTablesBySess, 1196
- ListUserConnections, 1197
- MassUpdate, 1197
- ModifyFolder, 1204
- Benachrichtigen, 1205
- ObjectExport, 1205
- ObjectImport , 1207
- PurgeVersion, 1208
- Register, 1211
- RegisterPlugin, 1212
- Wiederherstellen, 1214
- RollbackDeployment , 1216
- Ausführen, 1216
- ShowConnectionInfo, 1217
- SwitchConnection, 1218
- TruncateLog, 1218
- UndoCheckout, 1219
- Unregister, 1220
- UnregisterPlugin, 1221
- UpdateConnection, 1223
- UpdateEmailAddr, 1225
- UpdateSeqGenVals, 1225
- UpdateSrcPrefix, 1227
- UpdateStatistics , 1228
- UpdateTargPrefix, 1228
- Upgrade, 1229
- UninstallAbapProgram, 1230
- Validieren, 1231
- Version, 1234

Verwenden von pmrep

pmrep ist ein Befehlszeilenprogramm, mit dem Sie Repository-Informationen aktualisieren und Repository-Funktionen ausführen können. *pmrep* wird in den bin-Verzeichnissen des PowerCenter Client und der PowerCenter-Dienste installiert.

Verwenden Sie *pmrep* zum Ausführen von Aufgaben zur Repository-Verwaltung, wie z. B. Auflisten von Repository-Objekten, Erstellen und Bearbeiten von Gruppen, Wiederherstellen und Löschen von Repositories und Aktualisieren von Parametern und Sicherheitsinformationen im Zusammenhang mit Sitzungen im PowerCenter Repository.

Beim Verwenden von *pmrep* können Sie Befehle in den folgenden Modi eingeben:

- **Befehlszeilenmodus.** Sie können *pmrep*-Befehle direkt über die Befehlszeile des Systems eingeben. Verwenden Sie den Befehlszeilenmodus, um *pmrep*-Befehle zu schreiben.
- **Interaktiver Modus.** Sie können *pmrep*-Befehle über eine interaktive Eingabeaufforderung eingeben. *pmrep* wird nach Abschluss des Befehls nicht beendet.

Sie können mit Umgebungsvariablen Benutzernamen und Passwörter für *pmrep* festlegen. Konfigurieren Sie vor der Verwendung von *pmrep* diese Umgebungsvariablen. Die Umgebungsvariablen gelten für *pmrep*-Befehle, die auf dem Knoten ausgeführt werden.

Alle*pmrep*-Befehle erfordern eine Verbindung zum Repository. Davon ausgenommen sind folgende Befehle:

- Hilfe
- ListAllPrivileges

Verwenden Sie den*pmrep* Connect-Befehl zum Herstellen einer Verbindung zum Repository, bevor Sie andere *pmrep*-Befehle verwenden.

Hinweis: Wenn die Domäne eine Domäne für verschiedene Versionen ist, führen Sie *pmrep* über das Installationsverzeichnis der Repository Service-Version aus.

Ausführen von Befehlen im Befehlszeilenmodus

Im Befehlszeilenmodus wird *pmrep* jedes Mal aufgerufen und beendet, wenn Sie einen Befehl ausführen. Der Befehlszeilenmodus ist sinnvoll, wenn Sie *pmrep*-Befehle mit Batchdateien, Skripts oder anderen Programmen ausführen möchten.

So führen Sie pmrep-Befehle im Befehlszeilenmodus aus:

1. Ändern Sie an der Eingabeaufforderung das Verzeichnis, in dem sich die ausführbare *pmrep*-Datei befindet.
2. Geben Sie `pmrep` gefolgt vom Befehlsnamen und dessen Optionen und Argumenten ein:

   `pmrep command_name [-option1] argument_1 [-option2] argument_2...`

Ausführen von Befehlen im interaktiven Modus

Interaktiver Modus ruft *pmrep* auf. Sie können eine Reihe von Befehlen an einer *pmrep*-Eingabeaufforderung eingeben, ohne den Vorgang nach jedem Befehl zu beenden.

So führen Sie pmrep-Befehle im interaktiven Modus aus:

1. Geben Sie an der Eingabeaufforderung `pmrep` ein, um den interaktiven Modus aufzurufen.

   Dies startet *pmrep* im interaktiven Modus und zeigt eine `pmrep>`-Eingabeaufforderung an. `pmrep` muss nicht vor jedem Befehl im interaktiven Modus eingegeben werden.

2. Geben Sie einen Befehl und dessen Optionen und Argumente ein.

   Geben Sie an der Eingabeaufforderung Folgendes ein:

   ```
   command_name [-option1] argument_1 [-option2] argument_2...
   ```

   pmrep führt den Befehl aus und zeigt die Eingabeaufforderung erneut an.
3. Geben Sie `exit` ein, um eine interaktive Sitzung zu beenden.

Ausführen von Befehlen im normalen und exklusiven Modus

Der Repository Service wird im normalen oder exklusiven Modus ausgeführt. Führen Sie den Repository Service im exklusiven Modus aus, um Aufgaben durchzuführen, die nur eine Benutzerverbindung zum Repository zulassen.

Führen Sie den Repository Service im exklusiven Modus aus, um die folgenden *pmrep*-Befehle zu verwenden:

- Create
- Delete
- Register
- RegisterPlugin
- Unregister
- UnregisterPlugin

Sie können das Administrator-Tool oder *infacmd* zum Ausführen des Repository Service im exklusiven Modus verwenden.

pmrep-Rückgabewerte

pmrep gibt die erfolgreiche oder fehlgeschlagene Ausführung eines Befehls mit einem Rückgabewert an. Rückgabewert "0" gibt an, dass der Befehl erfolgreich ausgeführt wurde. Rückgabewert "1" gibt an, dass der Befehl fehlgeschlagen ist. Bestimmte Befehle führen mehrere Operationen aus. Mit AddToDeploymentgroup werden einer Bereitstellungsgruppe beispielsweise mehrere Objekte hinzugefügt. In diesen Fällen gibt der Rückgabewert "0" an, dass der Befehl erfolgreich ausgeführt wurde, auch wenn nur bestimmte Objekte erfolgreich bereitgestellt wurden.

Geben Sie sofort nach der Ausführung des Befehls *pmrep* einen der folgenden DOS- oder UNIX-echo-Befehle ein:

- Geben Sie an einer DOS-Shell `echo %ERRORLEVEL%` ein
- Geben Sie an einer UNIX Bourne- oder Korn-Shell `echo $?` ein
- Geben Sie an einer UNIX C-Shell `echo $status` ein

Verwenden von nativen Verbindungsstrings

Einige *pmrep*-Befehle, wie z. B. CreateConnection und Restore, erfordern einen nativen Verbindungsstring.

In der folgenden Tabelle wird die Syntax nativer Verbindungsstrings für die einzelnen unterstützten Datenbanken beschrieben:

Datenbank	Verbindungsstring-Syntax	Beispiel
IBM DB2	*dbname*	mydatabase
Microsoft SQL Server	*servername@dbname*	sqlserver@mydatabase
Oracle	*dbname*.world (identisch mit dem Eintrag TNSNAMES)	oracle.world
Sybase ASE	servername@dbname	sambrown@mydatabase

pmrep-Sripting-Befehle

Bei Einsatz von *pmrep* verwenden Sie möglicherweise regelmäßig einige Befehle mit bestimmten Optionen und Argumenten. Sie können *pmrep* beispielsweise verwenden, um täglich ein Backup eines Produktions-Repositorys durchzuführen. In diesem Fall können Sie eine Skriptdatei erstellen, um einen oder mehrere *pmrep*-Befehle einschließlich der zugehörigen Optionen und Argumente aufzurufen.

Mit der Windows-Batchdatei "`backupproduction.bat`" kann beispielsweise eine Verbindung zu einem Repository mit der Bezeichnung "Produktion" hergestellt und dessen Sicherung durchgeführt werden.

```
backupproduction.bat
REM This batch file uses pmrep to connect to and back up the repository Production on
the server ServerName
@echo off
echo Connecting to repository Production...
c:\PowerCenter\pmrep\pmrep connect -r Production -n Administrator -x Adminpwd -d
MyDomain -h Machine -o 8080
echo Backing up repository Production...
c:\PowerCenter\pmrep\pmrep backup -o c:\backup\Production_backup.rep
```

Sie können Skriptdateien über die Befehlszeilenschnittstelle ausführen. Sie können *pmrep*-Batchdateien nicht im interaktiven Modus ausführen.

Tipps für das Scripting von pmrep-Befehlen

Wenden Sie beim Erstellen und Ausführen von *pmrep*-Skripts die folgenden Tipps an:

- Fügen Sie einen Connect-Befehl als ersten Befehl ein, der von der Skriptdatei aufgerufen wird. Damit können Sie sicherstellen, dass die Aufgaben im richtigen Repository ausgeführt werden.
- Um *pmrep*-Skripts auszuführen, die Verbindungen zu unterschiedlichen Repositories gleichzeitig herstellen, legen Sie die Umgebungsvariable INFA_REPCNX_INFO in jeder Umgebung so fest, dass Name und Dateipfad für die Repository-Verbindungsdatei gespeichert werden. Dies verhindert, dass ein Skript die von einem anderen Skript verwendeten Verbindungsinformationen überschreibt.

Verbindungsuntertypen

Wenn Sie eine Verbindung auflisten oder aktualisieren, können Sie die Verbindungsuntertypen basierend auf dem zugehörigen Verbindungstyp angeben. Der Befehl „pmrep“ listet basierend auf den Repository-Plug-Ins die Verbindungsuntertypen standardmäßig im Repository auf.

In der folgenden Tabelle wird die Liste der Verbindungsuntertypen für den zugehörigen Verbindungstyp angezeigt:

Typ der Verbindung	Verbindungsuntertyp
Relational	Sybase
Relational	Informix (veraltet)
Relational	Microsoft SQL Server
Relational	DB2
Relational	ODBC
Relational	Teradata
Relational	Netezza
Relational	Vertica
Relational	PowerChannel for DB2
Relational	PowerChannel for Oracle
Relational	PowerChannel for MS SQL Server
Relational	PowerChannel for ODBC
Relational	PWX DB2zOS
Relational	PWX DB2i5OS
Relational	PWX DB2LUW
Relational	PWX Oracle
Relational	PWX MSSQLServer
Relational	PWX NRDB Lookup
Relational	Teradata PT Connection
Anwendung	SAP BW
Anwendung	SAP R3
Anwendung	PeopleSoft Oracle
Anwendung	PeopleSoft Sybase

Typ der Verbindung	Verbindungsuntertyp
Anwendung	PeopleSoft Informix
Anwendung	PeopleSoft MsSqlserver
Anwendung	PeopleSoft Db2
Anwendung	Siebel Oracle
Anwendung	Siebel Sybase
Anwendung	Siebel Informix
Anwendung	Siebel MsSqlserver
Anwendung	Siebel Db2
Anwendung	SAP_ALE_IDoc_Reader
Anwendung	SAP Type A
Anwendung	SAP_BWOHS_READER
Anwendung	SAP_ALE_IDoc_Writer
Anwendung	SAP RFC/BAPI Interface
Anwendung	JNDI Connection
Anwendung	JMS Connection
Anwendung	webMethods Broker
Anwendung	webMethods Integration Server
Anwendung	Web Services Consumer
Anwendung	PWX NRDB Batch
Anwendung	PWX NRDB CDC Change
Anwendung	PWX NRDB CDC Real Time
Anwendung	PWX DB2zOS CDC Change
Anwendung	PWX DB2zOS CDC Real Time
Anwendung	PWX DB2i5OS CDC Change
Anwendung	PWX DB2i5OS CDC Real Time
Anwendung	Http Transformation
Anwendung	PWX Oracle CDC Change

Typ der Verbindung	Verbindungsuntertyp
Anwendung	PWX Oracle CDC Real Time
Anwendung	LMAPITarget
Anwendung	Teradata FastExport Connection
Anwendung	PWX MSSQL CDC Change
Anwendung	PWX MSSQL CDC Real Time
Anwendung	PWX DB2LUW CDC Change
Anwendung	PWX DB2LUW CDC Real Time
Anwendung	Salesforce Connection
Anwendung	Hadoop HDFS Connection
FTP	FTP
Externer Ladevorgang	Teradata Mload External Loader
Externer Ladevorgang	Teradata Tpump External Loader
Externer Ladevorgang	DB2 EE External Loader
Externer Ladevorgang	DB2 EEE External Loader
Externer Ladevorgang	Teradata FastLoad External Loader
Externer Ladevorgang	Teradata Warehouse Builder External Loader
Externer Ladevorgang	HP NeoView Java Transporter
Warteschlange	Message Queue
Warteschlange	MSMQ

AddToDeploymentGroup

Fügt Objekte einer Bereitstellungsgruppe hinzu. Verwenden Sie AddToDeploymentGroup zum Hinzufügen von Quelle, Target, Transformation, Mapping, Sitzung, Worklet, Arbeitsablauf, Scheduler, Sitzungskonfiguration und Aufgabenobjekten.

Sie können keine ausgecheckten Objekte zu einer Bereitstellungsgruppe hinzufügen. Sie können Objekte mit Befehlsoptionen angeben oder eine persistente Eingabedatei verwenden. Bei Verwendung einer persistenten Eingabedatei können Sie die Option für den Bereitstellungsgruppennamen eingeben.

Verwenden Sie AddToDeploymentGroup, um wiederverwendbare Eingabeobjekte hinzuzufügen. Wenn Sie nicht wiederverwendbare Eingabeobjekte hinzufügen möchten, müssen Sie eine persistente Eingabedatei verwenden, die kodierte Objekt-IDs enthält.

Wenn AddToDeploymentGroup erfolgreich ausgeführt wird, sendet der Befehl entweder keine Statusinformationen zurück oder er liefert eine Liste von Objekten, die bereits in der Bereitstellungsgruppe vorhanden sind. Wenn der Befehl fehlschlägt, zeigt er die Ursache des Fehlers an.

Der AddToDeploymentGroup-Befehl verwendet die folgende Syntax:

```
addtodeploymentgroup

-p <deployment_group_name>

{{-n <object_name>

  -o <object_type>

  -t <object_subtype>]

  [-v <version_number>]

  [-f <folder_name>]} |

  [-i <persistent_input_file>]}

[-d <dependency_types (all, "non-reusable", or none)>]

[-s dbd_separator]
```

In der folgenden Tabelle werden *pmrep* AddToDeploymentGroup-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-p	deployment_group_name	Erforderlich. Name der Bereitstellungsgruppe, der Objekte hinzugefügt werden.
-n	object_name	Erforderlich beim Hinzufügen eines bestimmten Objekts. Name des Objekts, das Sie der Bereitstellungsgruppe hinzufügen. Der Name eines ausgecheckten Objekts kann nicht eingegeben werden. Bei Verwendung der Option -i kann die Option -n nicht benutzt werden.
-o	object_type	Erforderlich beim Hinzufügen eines bestimmten Objekts. Typ des Objekts, das Sie hinzufügen. Sie können Quelle, Target, Transformation, Mapping, Sitzung, Worklet, Arbeitsablauf, Scheduler, Sitzungskonfiguration, Aufgabe, Cube und Größenordnung festlegen.
-t	object_subtype	Erforderlich bei Verwendung gültiger Subtypen. Der Aufgaben- oder Transformationstyp, den Sie hinzufügen. Weitere Informationen zu gültigen Subtypen finden Sie unter "Auflisten von Objekttypen" auf Seite 1192.
-v	version_number	Optional. Version des hinzuzufügenden Objekts. Standard ist die neueste Version des Objekts. Der Befehl schlägt fehl, wenn Sie eine Versionsnummer für ein nicht versionsgesteuertes Repository angeben.
-f	folder_name	Erforderlich, wenn Sie einen Objektnamen eingeben. Ordner, der das hinzuzufügende Objekt enthält.
-i	persistent_input_file	Eine mit ExecuteQuery, Validate oder ListObjectDependencies generierte Textdatei, die eine Liste der Objektdatensätze mit kodierten IDs enthält. Wenn Sie diesen Parameter verwenden, lässt *pmrep* die Optionen -n, -o und -f nicht zu.

Option	Argument	Beschreibung
-d	dependency_types	Optional. Abhängige Objekte, die der Bereitstellungsgruppe mit dem Objekt hinzugefügt werden können. Geben Sie einen der folgenden Parameter ein: - all. *pmrep* fügt die Objekte und alle abhängigen Objekte, sowohl wiederverwendbare als auch nicht wiederverwendbare, der Bereitstellungsgruppe hinzu. - "non-reusable". *pmrep* fügt die Objekte und die entsprechenden nicht wiederverwendbaren, abhängigen Objekte der Bereitstellungsgruppe hinzu. - Keine. *pmrep* fügt der Bereitstellungsgruppe keine abhängigen Objekte hinzu. Wenn Sie diesen Parameter auslassen, fügt *pmrep* die Objekte und alle abhängigen Objekte der Bereitstellungsgruppe hinzu. **Hinweis:** Schließen Sie Argumente, die Leerzeichen oder nicht-alphanumerische Zeichen enthalten, in doppelte Anführungszeichen ein.
-s	dbd_separator	Optional. Wenn bei einer ODBC-Quelle ein Punkt (.) im Namen vorkommt, legen Sie beim Definieren des Quellobjekts ein anderes Trennzeichen fest. Beispiel: Definieren Sie statt database_name.source_name das Quellobjekt als database_name\source_name, und legen Sie als dbd_separator den umgekehrten Schrägstrich (\) fest.

ApplyLabel

Wendet eine Beschriftung auf ein Objekt oder eine Reihe von Objekten in einem Ordner an. Wenn Sie einen Ordnernamen eingeben, erhalten alle Objekte in diesem Ordner die Beschriftung. Sie können die Beschriftung auf abhängige Objekte anwenden. Wenn Sie die Option `dependency_object_types` verwenden, wendet *pmrep* die Beschriftung auf alle abhängigen Objekte an. Um eine Beschriftung auf ausgewählte abhängige Objekte anzuwenden, trennen Sie jeden Objekttypnamen in der Befehlszeile durch Komma ohne Leerzeichen ab.

Verwenden Sie ApplyLabel, um wiederverwendbare Eingabeobjekte zu beschriften. Wenn Sie nicht wiederverwendbare Eingabeobjekte beschriften möchten, müssen Sie eine persistente Eingabedatei verwenden, die kodierte Objekt-IDs enthält.

Wenn ApplyLabel erfolgreich ist, zeigt *pmrep* entweder keine Statusinformationen oder eine Liste von Objekten an, die bereits über die Beschriftung verfügen. Wenn der Befehl fehlschlägt, zeigt *pmrep* den Grund für den Fehler an.

Der ApplyLabel-Befehl verwendet die folgende Syntax:

```
applylabel

-a <label_name>

{{-n <object_name>

  -o <object_type>

  [-t <object_subtype>]

  [-v <version_number>]

  [-f <folder_name>] } |

  -i <persistent_input_file>}
```

```
[-d <dependency_object_types>]

[-p <dependency_direction (children, parents, or both)>]

[-s (include pk-fk dependency)]

[-g (across repositories)]

[-m (move label)]

[-c <comments>]

[-e dbd_separator]
```

In der folgenden Tabelle werden *pmrep* ApplyLabel-Optionen und Argumente beschrieben:

Option	Argument	Beschreibung
-a	label_name	Erforderlich. Beschriftungsname, der auf das Objekt angewendet werden soll.
-n	object_name	Erforderlich, wenn Sie ein bestimmtes Objekt aktualisieren. Name des Objekts, das die Beschriftung erhalten soll. Sie können keine Objektnamen eingeben, wenn Sie die Option -i verwenden.
-o	object_type	Typ des Objekts, auf das die Beschriftung angewendet werden soll. Sie können Quelle, Target, Transformation, Mapping, Sitzung, Worklet, Arbeitsablauf, Scheduler, Sitzungskonfiguration, Aufgabe, Cube oder Größenordnung festlegen. Erforderlich beim Anwenden einer Beschriftung auf ein bestimmtes Objekt.
-t	object_subtype	Erforderlich. Der Aufgaben- oder Transformationstyp, der beschriftet wird. *pmrep* ignoriert andere Objekttypen. Weitere Informationen zu gültigen Subtypen finden Sie unter "Auflisten von Objekttypen" auf Seite 1192.
-v	version_number	Optional. Version des Objekts, auf das die Beschriftung angewendet werden soll. Der Befehl schlägt fehl, wenn die Version ausgecheckt wurde. Wendet die Beschriftung standardmäßig auf die neueste Version an.
-f	folder_name	Optional. Ordner, der die Objekte enthält. Wenn Sie einen Ordnernamen, jedoch keinen Objektnamen eingeben, wendet *pmrep* die Beschriftung auf alle Objekte im Ordner an. Wenn Sie einen Ordnernamen mit einem Objektnamen eingeben, sucht *pmrep* in dem Ordner nach dem Objekt. Die Option -f kann nicht verwendet werden, wenn Sie die Option -i benutzen.
-i	persistent_input_file	Optional. Name einer Textdatei, die mit ExecuteQuery, ListObjectDependency oder Validate generiert wurde. Enthält eine Liste der Objekte, auf die die Beschriftung angewendet werden soll. Wenn Sie diese Option verwenden, dürfen Sie weder Objektnamen, Objekttyp noch Ordnernamen zur Angabe von Objekten verwenden.

Option	Argument	Beschreibung
-d	dependency_object_types	Optional. Zu beschriftende abhängige Objekttypen. Zu den gültigen abhängigen Objekttypen gehören Shortcuts, Mappings, Mapplets, Sitzungen, Arbeitsabläufe, Worklets, Target-Definitionen, Quelldefinitionen und Fremdschlüssel-Abhängigkeiten. Verwenden Sie diese Option mit der Option -p. Wenn Sie einen Objekttyp eingeben, wird die Beschriftung auf abhängige Objekte dieses Objekttyp angewendet.
-p	dependency_direction	Optional. Über- oder untergeordnete abhängige Objekte, auf die die Beschriftung angewendet werden soll. Sie können übergeordnete oder untergeordnete Objekte bzw. beides festlegen. Wenn Sie die Option -d nicht eingeben, erhalten alle abhängigen Objekte die Beschriftung. Wenn Sie diese Option nicht eingeben, wird die Beschriftung auf das angegebene Objekt angewendet.
-s	-	Optional. Schließen Sie die Objekte mit Primärschlüssel-Fremdschlüssel-Abhängigkeiten unabhängig von der Abhängigkeitsrichtung ein.
-g	-	Optional. Suchen Sie nach Objektabhängigkeiten über Repositories.
-m	-	Optional. Verschieben Sie eine Beschriftung von der aktuellen Version auf die neueste Version eines Objekts. Verwenden Sie dieses Argument, wenn der Beschriftungstyp one_per_object lautet.
-c	Kommentare	Optional. Kommentare zur Beschriftung.
-e	dbd_separator	Optional. Wenn bei einer ODBC-Quelle ein Punkt (.) im Namen vorkommt, legen Sie beim Definieren des Quellobjekts ein anderes Trennzeichen fest. Beispiel: Definieren Sie statt database_name.source_name das Quellobjekt als database_name \source_name, und legen Sie als dbd_separator den umgekehrten Schrägstrich (\) fest.

AssignIntegrationService

Weist den PowerCenter-Integrationsdienst dem angegebenen Arbeitsablauf zu.

Wenn Sie den Arbeitsablauf über den Arbeitsablauf-Manager ausführen und dem Arbeitsablauf im Befehl *pmrep AssignIntegrationService* einen PowerCenter-Integrationsdienst zugeordnet haben, wird der Arbeitsablauf in dem in der Option -i angegebenen PowerCenter-Integrationsdienst ausgeführt.

Wenn Sie den Arbeitsablauf über die Befehlszeile ausführen, wird der Arbeitsablauf in dem im Befehl *pmcmd StartWorkflow* angegebenen PowerCenter-Integrationsdienst ausgeführt. Der Arbeitsablauf wird nicht in dem PowerCenter-Integrationsdienst ausgeführt, den Sie im Befehl *pmrep AssignIntegrationService* angegeben haben.

Für den Befehl „AssignIntegrationService“ wird die folgende Syntax verwendet:

```
assignintegrationservice
-f <folder name>
-n <workflow name>
-i <integration service name>
```

In der folgenden Tabelle werden die Optionen und Argumente für *pmrep* AssignIntegrationService beschrieben:

Option	Argument	Beschreibung
-f	Ordnername	Erforderlich. Name des Ordners, der den Arbeitsablauf enthält. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-n	Name des Arbeitsablaufs	Erforderlich. Name des Arbeitsablaufs.
-i	Name des Integrationsdiensts	Erforderlich. Name des PowerCenter-Integrationsdiensts für den Arbeitsablauf.

AssignPermission

Ermöglicht das Hinzufügen, Entfernen oder Aktualisieren von Berechtigungen bei einem globalen Objekt für einen Benutzer, eine Gruppe oder die Standardgruppe "Andere".

Hinweis: Nur der Administrator oder der aktuelle Eigentümer des Objekts kann Berechtigungen für das Objekt verwalten.

Der AssignPermission-Befehl verwendet die folgende Syntax:

```
AssignPermission

-o <object_type>

[-t <object_subtype>]

-n <object_name>

{-u <user_name> | -g <group_name>}

[-s <security_domain>]

-p <permission>
```

In der folgenden Tabelle werden *pmrep* AssignPermission-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-o	object_type	Erforderlich. Typ des Objekts, für das Sie Berechtigungen verwalten möchten. Sie können Ordner, Beschriftung, Bereitstellungsgruppe, Abfrage oder Verbindung festlegen.
-t	object_subtype	Optional. Typ des Verbindungsobjekts oder der Abfrage. Nicht erforderlich für andere Objekttypen. Weitere Informationen zu gültigen Subtypen finden Sie unter "AssignPermission" auf Seite 1158.
-n	object_name	Erforderlich. Name des Objekts, für das Sie Berechtigungen verwalten möchten. Sie können Sonderzeichen für den Objektnamen verwenden.

Option	Argument	Beschreibung
-u	user_name	Erforderlich, wenn Sie nicht die Option -g verwenden. Name des Benutzers, für den Sie Berechtigungen hinzufügen, entfernen oder aktualisieren möchten. Verwenden Sie die Option -u oder die Option -g, nicht beide.
-g	group_name	Name der Gruppe, für die Sie Berechtigungen hinzufügen, entfernen oder aktualisieren möchten. Geben Sie „Andere“ als Gruppenname an, um Berechtigungen der Standardgruppe „Andere“ zu ändern. Verwenden Sie die Option -u oder die Option -g, aber nicht beide. Sie können Sonderzeichen für den Gruppennamen verwenden.
-s	security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer oder die Gruppe gehört. Standardwert ist „Native“.
-p	permission	Erforderlich. Berechtigungen, die Sie hinzufügen, entfernen oder aktualisieren möchten. Sie weisen Lese-, Schreib- und Ausführungsberechtigungen einem globalen Objekt zu. Verwenden Sie die Zeichen r, w und x, um Lese-, Schreib- und Ausführungsberechtigungen zuzuweisen.

In der folgenden Tabelle werden die Objekttypen und Werte beschrieben, die bei den *pmrep*-Befehlen verwendet werden:

Objekttyp	Objekt-Subtyp
Abfrage	Gemeinsam genutzt
Abfrage	Persönlich
Verbindung	Anwendung
Verbindung	FTP
Verbindung	Loader
Verbindung	Warteschlange
Verbindung	Relational

Beispiel

Sie können Berechtigungen mit der Option -p hinzufügen, entfernen oder aktualisieren.

Um beispielsweise Lese- und Schreibberechtigungen für einen Ordner hinzuzufügen, geben Sie den folgenden Text bei der Eingabeaufforderung ein:

```
pmrep AssignPermission -o folder -n Sales -u Admin -p rw
```

Sie können Berechtigungen für ein Objekt auch aktualisieren. Beispiel: Sie haben einem Ordner eine Leseberechtigung zugewiesen und müssen nun auch die Schreibberechtigung zuweisen. Geben Sie zum Aktualisieren von Berechtigungen den folgenden Text bei der Eingabeaufforderung ein:

```
pmrep AssignPermission -o folder -n Sales -u Admin -p rw
```

Um alle Berechtigungen zu entfernen, geben Sie den folgenden Text bei der Eingabeaufforderung ein:

```
pmrep AssignPermission -o folder -n Sales -u Admin -p ""
```

BackUp

Sichert das Repository in die mit der Option -o angegebene Datei. Sie müssen der Backup-Datei einen Namen zuweisen. Verwenden Sie diesen Befehl, wenn das Repository ausgeführt wird. Sie müssen mit einem Repository verbunden sein, um diesen Befehl verwenden zu können.

Der BackUp-Befehl verwendet die folgende Syntax:

```
backup

-o <output_file_name>

[-d <description>]

[-f (overwrite existing output file)]

[-b (skip workflow and session logs)]

[-j (skip deploy group history)]

[-q (skip MX data)]

[-v (skip task statistics)]
```

In der folgenden Tabelle werden die *pmrep* Backup-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-o	output_file_name	Erforderlich. Name und Pfad der Datei für die Repository-Sicherung. Wenn Sie die Liste der Repository-Backup-Dateien im Administrator-Tool anzeigen, werden nur Dateien mit der Erweiterung .rep aufgeführt.
-d	Beschreibung	Optional. Erstellt eine Beschreibung der Backup-Datei basierend auf der Zeichenfolge, die der Option folgt. Beim Sicherungsprozess werden alle Zeichenfolgen nach 2.000 Zeichen trunkiert.
-f	-	Optional. Überschreibt eine vorhandene Datei mit demselben Namen.
-b	-	Optional. Überspringt während des Backups Tabellen, die sich auf Arbeitsablauf und Sitzungsprotokolle beziehen.
-j	-	Optional. Überspringt während des Backup die Bereitstellungsgruppen-Historie.
-q	-	Optional. Überspringt während des Backups Tabellen, die sich auf MX-Daten beziehen.
-v	-	Optional. Überspringt während des Backups Aufgabenstatistiken.

Verwenden Sie zum Wiederherstellen der Backup-Datei das Administrator-Tool oder den Befehl *pmrep* Restore.

ChangeOwner

Ändert den Namen des Eigentümers für ein globales Objekt.

Hinweis: Nur der Administrator oder der aktuelle Eigentümer des Objekts darf den Eigentümer eines Objekts ändern.

Der ChangeOwner-Befehl verwendet die folgende Syntax:

```
ChangeOwner

-o <object_type>

[-t <object_subtype>]

-n <object_name>

-u <new_owner_name>

[-s <security_domain>]
```

In der folgenden Tabelle werden die *pmrep* ChangeOwner-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-o	object_type	Erforderlich. Typ des Objekts. Sie können Ordner, Beschriftung, Bereitstellungsgruppe, Abfrage oder Verbindung festlegen.
-t	object_subtype	Optional. Typ der Objektabfrage oder des Verbindungsobjekts. Nicht erforderlich für andere Objekttypen. Weitere Informationen zu gültigen Subtypen finden Sie unter "AssignPermission" auf Seite 1158.
-n	object_name	Erforderlich. Name des Objekts Sie können Sonderzeichen für den Objektnamen verwenden.
-u	new_owner_name	Erforderlich. Name des geänderten Eigentümers. Der geänderte Eigentümername muss ein gültiges Benutzerkonto in der Domäne sein.
-s	security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der neue Eigentümer gehört. Standardwert ist „Native".

CheckIn

Checkt ein Objekt ein, das Sie ausgecheckt haben. Wenn Sie ein Objekt einchecken, erstellt das Repository eine neue Version des Objekts und weist ihm eine Versionsnummer zu. Die Versionsnummer ist um eine Zahl höher als die Versionsnummer der letzten eingecheckten Version.

Der CheckIn-Befehl verwendet die folgende Syntax:

```
checkin

-o <object_type>

[-t <object_subtype>]

-n <object_name>

-f <folder_name>
```

```
[-c <comments>]

[-s dbd_separator]
```

In der folgenden Tabelle werden die *pmrep* CheckIn-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-o	object_type	Erforderlich. Typ des einzucheckenden Objekts: Quelle, Target, Transformation, Mapping, Sitzung, Worklet, Arbeitsablauf, Scheduler, Sitzungskonfiguration, Aufgabe, Cube oder Größenordnung.
-t	object_subtype	Optional. Der Typ der einzuscheckenden Aufgabe oder Transformation. Nicht erforderlich für andere Objekttypen. Weitere Informationen zu gültigen Subtypen finden Sie unter "Auflisten von Objekttypen" auf Seite 1192.
-n	object_name	Erforderlich. Name des einzucheckenden Objekts.
-f	folder_name	Erforderlich. Ordner, in dem die neue Objektversion gespeichert werden soll.
-c	Kommentare	Optional. Kommentare zum Einchecken.
-s	dbd_separator	Optional. Wenn bei einer ODBC-Quelle ein Punkt (.) im Namen vorkommt, legen Sie beim Definieren des Quellobjekts ein anderes Trennzeichen fest. Beispiel: Definieren Sie statt database_name.source_name das Quellobjekt als database_name\source_name, und legen Sie als dbd_separator den umgekehrten Schrägstrich (\) fest.

CleanUp

Bereinigt alle von *pmrep* erstellten persistenten Ressourcen. Dieser Befehl bereinigt auch alle Verbindungsinformationen aus vorherigen Sitzungen von *pmrep*. Wird CleanUp in einer Sitzung als erster Befehl aufgerufen, führt dies immer zu einem Fehler.

Wenn Sie CleanUp im interaktiven Modus aufrufen, trennt *pmrep* alle verbundenen Repositories.

Der CleanUp-Befehl verwendet die folgende Syntax:

```
cleanup
```

ClearDeploymentGroup

Löscht alle Objekte aus einer Bereitstellungsgruppe. Verwenden Sie diesen Befehl, um die Bereitstellungsgruppe zu behalten und die Objekte zu entfernen.

Der ClearDeploymentGroup-Befehl verwendet die folgende Syntax:

```
cleardeploymentgroup

-p <deployment_group_name>

[-f (force clear)]
```

In der folgenden Tabelle werden die *pmrep* ClearDeploymentGroup- Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-p	deployment_group_name	Erforderlich. Name der Bereitstellungsgruppe, die Sie löschen möchten.
-f	-	Optional. Entfernen Sie Objekte ohne Bestätigung. Wenn Sie dieses Argument auslassen, werden Sie aufgefordert, das Löschen der Objekte zu bestätigen.

Connect

Stellt die Verbindung zu einem Repository her. Wenn Sie *pmrep* in der Befehlszeile oder im interaktiven Modus zum ersten Mal benutzen, müssen Sie den Connect-Befehl verwenden. Alle Befehle erfordern eine Verbindung zum Repository. Davon ausgenommen sind folgende Befehle:

- Exit
- Hilfe
- ListAllPrivileges

Im Befehlszeilenmodus verwendet *pmrep* die Informationen, die beim letzten Verbindungsaufruf zum Repository verwendet wurden. Wenn *pmrep* ohne erfolgreiche Verbindung aufgerufen wird, führt dies zu einem Fehler. In Befehlszeilenmodus stellt *pmrep* bei jedem Befehl eine Verbindung zum Repository her und trennt diese wieder.

Um *pmrep* zur Ausführung von Aufgaben in mehreren Repositorys in einer einzigen Sitzung zu verwenden, müssen Sie den Connect-Befehl jedes Mal ausführen, wenn Sie zu einem anderen Repository wechseln möchten. Im interaktiven Modus behält *pmrep* die Verbindung bei, bis Sie *pmrep* beenden oder eine neue Verbindung herstellen. Wenn Sie Connect erneut aufrufen, trennt *pmrep* die Verbindung zu ersten Repository und stellt dann eine Verbindung zum zweiten Repository her. Wenn die zweite Verbindung fehlschlägt, bleibt die vorhergehende Verbindung weiterhin getrennt, sodass keine Verbindung zu einem Repository besteht. Wenn Sie einen Befehl ausführen, der eine Verbindung zum Repository benötigt, und Sie nicht mit diesem Repository verbunden sind, verwendet *pmrep* die Verbindungsinformationen der letzten erfolgreichen Verbindung zum Repository aus einer früheren Sitzung von *pmrep*. *pmrep* behält Informationen aus der letzten erfolgreichen Verbindung bei, bis Sie den Cleanup-Befehl verwenden.

Der Befehl „Connect“ verwendet die folgende Syntax:

```
connect

-r <repository_name>

{-d <domain_name> |

 {-h <portal_host_name>

  -o <portal_port_number>}}

[{ <user_name>

[-s <user_security_domain>]

[-x <password> |

 -X <password_environment_variable>]} |

-u <connect_without_user_in_kerberos_mode>]
```

```
[-t <client_resilience>]
```

In der folgenden Tabelle werden die Optionen und Argumente für „*pmrep* Connect“ beschrieben:

Option	Argument	Beschreibung
-r	repository_name	Erforderlich. Name des Repository, zu dem Sie eine Verbindung herstellen möchten.
-d	domain_name	Erforderlich, wenn Sie nicht -h und -o verwenden. Der Name der Domäne für das Repository. Wenn Sie die Option -d verwenden, dürfen Sie nicht die Optionen -h und -o benutzen.
-h	portal_host_name	Erforderlich, wenn Sie nicht -d verwenden. Wenn Sie die Option -h benutzen, müssen Sie auch die Option -o verwenden. Gateway-Hostname.
-o	portal_port_number	Erforderlich, wenn Sie nicht -d verwenden. Wenn Sie die Option -o verwenden, müssen Sie auch die Option -h verwenden. Gateway-Portnummer.
-n	user_name	Optional. Benutzername zum Herstellen einer Verbindung zum Repository.
-s	user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Standardwert ist „Native“.
-x	Passwort	Erforderlich, wenn Sie die Option -n und nicht die Option -X verwenden. Passwort für den Benutzernamen. Beim Passwort wird die Groß- und Kleinschreibung beachtet. Verwenden Sie die Option -x oder -X, aber nicht beide.
-X	password_ environment_variable	Erforderlich, wenn Sie die Option -n und nicht die Option -x verwenden. Passwort-Umgebungsvariable. Verwenden Sie die Option -x oder -X, aber nicht beide.
-u	connect_without _user_ in_kerberos_mode	Erforderlich. Stellt eine Verbindung zu einem Repository-Dienst ohne Benutzernamen und Passwort her, wenn die Informatica-Domäne die Kerberos-Authentifizierung verwendet. Verwenden Sie die Option „-u“, um eine Verbindung zum Repository-Dienst herzustellen, wenn das Repository keinen Inhalt hat.
-t	client_resilience	Optional. Zeit (in Sekunden), in der *pmrep* versucht, eine Verbindung zum Repository herzustellen bzw. erneut herzustellen. Wenn Sie die Option -t auslassen, verwendet *pmrep* den Timeout-Wert, der in der INFA_CLIENT_RESILIENCE_TIMEOUT-Umgebungsvariablen angegeben ist. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Create

Erstellt die Repository-Tabellen in der Datenbank. Bevor Sie die Repository-Tabellen erstellen können, müssen Sie diese Aufgaben abschließen:

- Erstellen und konfigurieren Sie die Datenbank, die das Repository enthalten soll.
- Erstellen Sie den Repository Service im Administrator-Tool oder in *infacmd*.

- Führen Sie den Repository Service im exklusiven Modus im Administrator-Tool oder in *infacmd* aus.
- Stellen Sie eine Verbindung zum Repository in *pmrep* her.

Der Create-Befehl kann nicht verwendet werden, wenn die Repository-Datenbank bereits Repository-Tabellen enthält.

Um den Create-Befehl zu verwenden, müssen Sie über die Berechtigung für den Repository Service in der Domäne verfügen.

Der Create-Befehl verwendet die folgende Syntax:

```
create

-u <domain_user_name>

[-s <domain_user_security_domain>]

[-p <domain_password> |

 -P <domain_password_environment_variable>]

[-g (create global repository)]

[-v (enable object versioning)]
```

In der folgenden Tabelle werden die *pmrep* Create-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-u	domain_user_name	Erforderlich. Benutzername.
-s	domain_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Die Standardeinstellung ist "Native".
-p	domain_password	Optional. Passwort. Verwenden Sie entweder die Option -p oder -P, aber nicht beide. Wenn Sie weder die Option -p noch -P verwenden, werden Sie von *pmrep* aufgefordert, das Passwort einzugeben.
-P	domain_password_ environment_variable	Optional. Passwort-Umgebungsvariable. Verwenden Sie entweder die Option -p oder -P, aber nicht beide. Wenn Sie weder die Option -p noch -P verwenden, werden Sie von *pmrep* aufgefordert, das Passwort einzugeben.
-g	-	Optional. Stuft das Repository zu einem globalen Repository hoch.
-v	-	Optional. Ermöglicht die Objektversionierung für das Repository.

CreateConnection

Erstellt eine Quell- oder Target-Verbindung im Repository. Die Verbindung kann eine relationale, Anwendungs- oder FTP-Verbindung sein. Relationale Datenbankverbindungen für alle relationalen Subtypen benötigen eine Teilmenge aller CreateConnection-Optionen und -Argumente. Zum Beispiel werden die Optionen -z, -d oder -t von Oracle-Verbindungen nicht akzeptiert. Verwenden Sie die Option -k zum Festlegen der Attribute für Anwendungsverbindungen.

Der Befehl „CreateConnection“ verwendet die folgende Syntax:

```
createconnection

-s <connection_type>

-n <connection_name>

[{-u <user_name>

[-p <password> |

-P <password_environment_variable>]}|

-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)]
```

In der folgenden Tabelle werden die Optionen und Argumente für „*pmrep* CreateConnection“ beschrieben:

Option	Argument	Beschreibung
-s	connection_type	Erforderlich. Typ der Verbindung. Folgende Verbindungstypen sind möglich: - Anwendung - FTP - Relational Verwenden Sie zum Erstellen einer Salesforce-Verbindung beispielsweise die folgende Syntax: `-s "salesforce connection"`
-n	connection_name	Erforderlich. Name der Verbindung.

Option	Argument	Beschreibung
-u	user_name	Für bestimmte Verbindungstypen erforderlich. Für die Authentifizierung verwendeter Benutzername.
-p	password	Für bestimmte Verbindungstypen erforderlich. Passwort für die Authentifizierung beim Herstellen einer Verbindung zur relationalen Datenbank. Verwenden Sie die Option -p oder -P, aber nicht beide. Wenn Sie einen Benutzernamen angeben, aber weder -p noch -P verwenden, werden Sie von pmrep zur Eingabe des Passworts aufgefordert.
-P	password_ environment_variable	Optional. Passwort-Umgebungsvariable für die Authentifizierung, wenn Sie eine Verbindung zu der relationalen Datenbank herstellen. Verwenden Sie die Option -p oder -P, aber nicht beide. Wenn Sie weder die Option -p noch -P verwenden, werden Sie von *pmrep* zur Eingabe des Passworts aufgefordert.
-K	connection_to_the_Kerberos_server	Optional. Gibt an, dass die Datenbank, zu der Sie eine Verbindung herstellen, in einem Netzwerk ausgeführt wird, das die Kerberos-Authentifizierung verwendet.
-c	connect_string	Verbindungszeichenfolge, die der Integrationsdienst verwendet, um eine Verbindung zur relationalen Datenbank herzustellen.
-l	code_page	Für bestimmte Verbindungstypen erforderlich. Codepage, die der Verbindung zugeordnet ist.
-r	rollback_segment	Optional. Gültig für Oracle-Verbindungen. Der Name des Rollbacksegments. Datenbanktransaktionen mit Rollbacksegment-Datensätzen, mit denen Sie die Transaktion rückgängig machen können.
-e	connection_ environment_sql	Optional. Geben Sie die SQL-Befehle zum Einrichten der Datenbankumgebung ein, wenn Sie eine Verbindung zur Datenbank herstellen. Der Integrationsdienst führt die Verbindungsumgebungs-SQL bei jeder Verbindungsherstellung mit der Datenbank aus.
-f	transaction_ environment_sql	Optional. Geben Sie die SQL-Befehle zum Einrichten der Datenbankumgebung ein, wenn Sie eine Verbindung zur Datenbank herstellen. Der Integrationsdienst führt die Transaktionsumgebungs-SQL am Anfang jeder Transaktion aus.
-z	packet_size	Optional. Gültig für Sybase ASE- und Microsoft SQL Server-Verbindungen. Optimiert die ODBC-Verbindung zu Sybase ASE und Microsoft SQL Server.
-b	database_name	Optional. Name der Datenbank. Gültig für Sybase ASE- und Microsoft SQL Server-Verbindungen.
-v	server_name	Optionaler Name des Datenbankservers. Gültig für Sybase ASE- und Microsoft SQL Server-Verbindungen.
-d	domain_name	Optional gültig für Microsoft SQL Server-Verbindungen. Der Name der Domäne. Verwendet für Microsoft SQL Server.

Option	Argument	Beschreibung
-t	-	Optional. Gültig für Microsoft SQL Server-Verbindungen. Bei Aktivierung verwendet der Integrationsdienst Windows-Authentifizierung, um auf die Microsoft SQL Server-Datenbank zuzugreifen. Der Name des Benutzers, der den Integrationsdienst startet, muss ein gültiger Windows-Benutzer mit Zugriff auf die Microsoft SQL Server-Datenbank sein.
-a	data_source_name	Optionaler Name der Teradata-ODBC-Datenquelle. Gültig für Teradata-Verbindungen.
-x	-	Aktiviert erweiterte Sicherheit. Gewährt Ihnen Berechtigungen zum Lesen, Schreiben und Ausführen. Öffentlichen und weltweiten Gruppen werden keine Berechtigungen gewährt. Wenn diese Option nicht aktiviert ist, werden allen Gruppen und Benutzern Lese-, Schreib- und Ausführungsberechtigungen gewährt.
-k	connection_attributes	Aktiviert benutzerdefinierte Verbindungsattribute. Attribute weisen das Format <name>=<value>;<name>=<value> auf. **Hinweis:** Fügen Sie vor dem Attributnamen kein Leerzeichen hinzu.
-y	-	Aktiviert den Wert des Providertyps. Sie können die folgenden Providertypen angeben: - 1 für ODBC - 2 für Oledb (Veraltet)
-m	-	Aktiviert das Attribut „DSN verwenden“. Der PowerCenter-Integrationsdienst ruft die Datenbank- und Servernamen aus dem DSN ab.

Festlegen der Datenbank-Codepage

Die Option -l gibt die Codepage für die Datenbankverbindung an. Geben Sie den Namen der Codepage ein, den Sie der Datenbankverbindung zuweisen möchten. Um beispielsweise die US-ASCII-Codepage der Datenbankverbindung zuzuweisen, geben Sie den Codepage-Namen "US-ASCII" ein

Das Ändern der Datenbankverbindungs-Codepage kann zu Dateninkonsistenzen führen, wenn die neue Codepage nicht mit den Codepages der Quell- oder Target-Datenbankverbindung kompatibel ist. Auch wenn Sie den Integration Service für die Datenvalidierung der Codepage konfigurieren, kann das Ändern der Datenbankverbindungs-Codepage zu einem Fehlschlagen von Sitzungen führen, wenn die Codepage der Quelldatenbank-Verbindung nicht Teil der Codepage der Target-Datenbankverbindung ist.

CreateDeploymentGroup

Erstellt eine Bereitstellungsgruppe. Sie können eine dynamische oder statische Bereitstellungsgruppe erstellen. Zum Erstellen einer dynamischen Bereitstellungsgruppe müssen Sie einen Abfragenamen zur Verfügung stellen und angeben, ob es sich um eine private oder öffentliche Abfrage handelt.

Der CreateDeploymentGroup-Befehl verwendet die folgende Syntax:

```
createdeploymentgroup

-p <deployment_group_name>
```

```
[-t <deployment_group_type (static or dynamic)>]

[-q <query_name>]

[-u <query_type (shared or personal)>]

[-c <comments>]
```

In der folgenden Tabelle werden die *pmrep* CreateDeploymentGroup-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-p	deployment_group_name	Erforderlich. Der Name der zu erstellenden Bereitstellungsgruppe.
-t	deployment_group_type	Optional. Erstellen Sie eine statische Gruppe, oder verwenden Sie eine Abfrage zum dynamischen Erstellen der Gruppe. Sie können statisch oder dynamisch angeben. Der Standardwert ist statisch.
-q	query_name	Erforderlich, wenn die Bereitstellungsgruppe dynamisch ist. Wird jedoch ignoriert, wenn die Gruppe statisch ist. Name der Abfrage, die der Bereitstellungsgruppe zugeordnet ist.
-u	query_type	Erforderlich, wenn die Bereitstellungsgruppe dynamisch ist. Wird jedoch ignoriert, wenn die Gruppe statisch ist. Typ der Abfrage zum Erstellen einer Bereitstellungsgruppe. Sie können die gemeinsame oder persönliche Nutzung festlegen.
-c	Kommentare	Optional. Kommentare zu der neuen Bereitstellungsgruppe.

CreateFolder

Erstellt einen Ordner im Repository.

Der CreateFolder-Befehl verwendet die folgende Syntax:

```
createfolder

-n <folder_name>

[-d <folder_description>]

[-o <owner_name>]

[-a <owner_security_domain>]

[-s (shared_folder)]

[-p <permissions>]

[-f <active | frozendeploy | frozennodeploy>]
```

In der folgenden Tabelle werden die *pmrepCreateFolder*-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-n	folder_name	Erforderlich. Ordnername.
-d	folder_description	Optional. Beschreibung des Ordners, der im Repository Manager angezeigt wird. Wenn die Ordnerbeschreibung Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie sie in Anführungszeichen.
-o	owner_name	Optional. Eigentümer des Ordners. Jeder Benutzer im Repository kann Eigentümer des Ordners sein. Der Standardeigentümer ist der Benutzer, der den Ordner erstellt hat.
-a	owner_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Eigentümer gehört. Standardwert ist "Native".
-s	-	Optional. Stellt den Ordner zur gemeinsamen Nutzung zur Verfügung.
-p	Berechtigungen	Optional. Zugriffsberechtigungen für den Ordner. Wenn dies ausgelassen wird, weist der Repository Service Standardberechtigungen zu.
-f	active frozendeploy frozennodeploy	Optional. Ändert den Ordnerstatus auf einen der folgenden Status: - active. Dieser Status ermöglicht Benutzern das Auschecken versionsgesteuerter Objekte im Ordner. - frozendeploy (Eingefroren, Ersetzen bei Bereitstellung zulassen). Dieser Status verhindert, dass Benutzer Objekte im Ordner auschecken. Bei der Bereitstellung im Ordner werden neue Versionen der Objekte erstellt. - frozennodeploy (Eingefroren, Ersetzen bei Bereitstellung nicht zulassen). Dieser Status verhindert, dass Benutzer Objekte im Ordner auschecken. Sie können in diesem Ordner keine Objekte bereitstellen.

Hinweis: Mit dem AssignPermission-Befehl können Sie in einem Ordner Berechtigungen hinzufügen, entfernen oder aktualisieren.

Zuweisen von Berechtigungen

Sie können Eigentümer-, Gruppen- und Repository-Berechtigungen durch Eingabe von drei Ziffern zuweisen, wenn Sie die Option -p verwenden. Die erste Ziffer entspricht den Eigentümerberechtigungen, die zweite entspricht den Berechtigungen der Gruppe, der der Benutzer angehört, und die dritte bezieht sich auf alle anderen Berechtigungen.

Geben Sie für jeden Berechtigungssatz eine Zahl ein. Jede Berechtigung ist einer Zahl zugeordnet. Verwenden Sie 4 für Leseberechtigung, 2 für Schreibberechtigung und 1 für Ausführungsberechtigung. Um Berechtigungen zuweisen, geben Sie 4, 2, 1 oder die Summe der entsprechenden Zahlen ein.

Wenn Sie beispielsweise Standardberechtigungen zuweisen möchten, verwenden Sie die folgende Befehlssyntax:

```
-p 764
```

Mit dieser Syntax erhält der Ordnereigentümer die Berechtigung zum Lesen, Schreiben und Ausführen (7 = 4+2+1). Die Gruppe des Eigentümers hat Lese- und Schreibberechtigungen (6 = 4+2). Alle anderen haben Leseberechtigung.

Der Befehl gibt die Meldung "createfolder erfolgreich abgeschlossen" oder "createfolder fehlgeschlagen" zurück. Die Erstellung schlägt möglicherweise aus folgenden Gründen fehl:

- Der Ordner ist bereits vorhanden.
- Der Eigentümer existiert nicht oder gehört nicht zur Gruppe.

CreateLabel

Erstellt eine Beschriftung, die Sie zum Zuordnen von Objektgruppen während der Entwicklung verwenden. Sie können eine Beschriftung jedem versionsgesteuerten Objekt bzw. jeder Objektgruppe in einem Repository zuordnen.

Der CreateLabel-Befehl verwendet die folgende Syntax:

```
createlabel

-a <label_name>

[-c <comments>]
```

In der folgenden Tabelle werden die *pmrep* CreateLabel-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-a	label_name	Erforderlich. Name der Beschriftung, die Sie erstellen.
-c	Kommentare	Optional. Kommentare zur Beschriftung.

Delete

Löscht die Repository-Tabellen aus der Repository-Datenbank.

Bevor Sie den Delete-Befehl verwenden können, müssen Sie eine Verbindung zum Repository herstellen und einen Benutzernamen und ein Passwort oder eine Passwort-Umgebungsvariable eingeben.

Wenn Sie den Delete-Befehl verwenden, muss der Repository Service im exklusiven Modus ausgeführt werden. Sie können die Ausführung des Repository Service im exklusiven Modus im Administrator-Tool konfigurieren oder den Befehl *infacmd* UpdateRepositoryService verwenden.

Der Delete-Befehl verwendet die folgende Syntax:

```
delete

[-x <repository_password_for_confirmation> |

 -X <repository_password_environment_variable_for_confirmation>]

[-f (forceful delete: unregisters local repositories and deletes)]
```

In der folgenden Tabelle werden die *pmrep* Delete-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-x	repository_password_for_ confirmation	Optional. Passwort. Sie können die Option -x oder -X Option verwenden, aber nicht beide. Wenn Sie weder die Option -x noch -X verwenden, werden Sie von *pmrep* aufgefordert, zur Bestätigung das Passwort einzugeben.
-X	repository_password_ environment_variable_for_ confirmation	Optional. Passwort-Umgebungsvariable. Sie können die Option -x oder -X Option verwenden, aber nicht beide. Wenn Sie weder die Option -x noch -X verwenden, werden Sie von *pmrep* aufgefordert, zur Bestätigung das Passwort einzugeben.
-f	-	Optional. Löscht ein globales Repository und hebt die Registrierung lokaler Repositories auf. Alle registrierten lokalen Repositories müssen ausgeführt werden.

DeleteConnection

Löscht eine relationale Verbindung aus dem Repository.

Der DeleteConnection-Befehl verwendet die folgende Syntax:

```
deleteconnection

-n <connection_name>

[-f (force delete)]

[-s <connection type application, relational, ftp, loader or queue>]
```

In der folgenden Tabelle werden die *pmrep* DeleteConnection-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-n	connection_name	Erforderlich. Name der zu löschenden Verbindung.
-f	-	Optional. Verbindung wird ohne weitere Bestätigung gelöscht.
-s	Verbindungstypanwendung, relational, FTP, Loader oder Warteschlange	Optional. Typ der Verbindung. Folgende Verbindungstypen sind möglich: - Anwendung - FTP - Loader - Warteschlange - Relational Standardwert ist relational.

DeleteDeploymentGroup

Löscht eine Bereitstellungsgruppe. Wenn Sie eine statische Bereitstellungsgruppe löschen, entfernen Sie auch alle Objekte aus der Bereitstellungsgruppe.

Der DeleteDeploymentGroup-Befehl verwendet die folgende Syntax:

```
deletedeploymentgroup

-p <deployment_group_name>

[-f (force delete)]
```

In der folgenden Tabelle werden die *pmrep* DeleteDeploymentGroup-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-p	deployment_group_name	Erforderlich. Name der zu löschenden Bereitstellungsgruppe.
-f	-	Optional. Löscht die Bereitstellungsgruppe ohne Bestätigung. Wenn Sie dieses Argument auslassen, werden Sie von *pmrep* vor dem Löschen der Bereitstellungsgruppe aufgefordert, dies zu bestätigen.

DeleteFolder

Löscht einen Ordner aus dem Repository.

Der DeleteFolder-Befehl verwendet die folgende Syntax:

```
deletefolder

-n <folder_name>
```

In der folgenden Tabelle werden die *pmrep* DeleteFolder-Option und das Argument beschrieben:

Option	Argument	Beschreibung
-n	folder_name	Erforderlich. Name des Ordners.

DeleteLabel

Löscht eine Beschriftung und entfernt die Beschriftung aus allen Objekte, die sie verwenden. Wenn die Beschriftung gesperrt ist, schlägt das Löschen fehl.

Der DeleteLabel-Befehl verwendet die folgende Syntax:

```
deletelabel

-a <label_name>

[-f (force delete)]
```

In der folgenden Tabelle werden die *pmrep* DeleteLabel-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-a	label_name	Erforderlich. Name der zu löschenden Beschriftung.
-f	-	Optional. Löschen der Beschriftung ohne Bestätigung. Wenn Sie dieses Argument auslassen, werden Sie durch den Befehl aufgefordert, das Löschen der Beschriftung zu bestätigen.

DeleteObject

Löscht ein Objekt. Verwenden Sie DeleteObject zum Löschen von Quellen, Targets, benutzerdefinierten Funktionen, Mapplets, Mappings, Sitzungen, Worklets oder Arbeitsabläufen.

Der DeleteObject-Befehl verwendet die folgende Syntax:

```
DeleteObject

-o <object_type>

-f <folder_name>

-n <object_name>

[-s dbd_separator]
```

In der folgende Tabelle werden die *pmrep* DeleteObject-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-o	object_type	Erforderlich. Typ des Objekts, das Sie löschen: Quelle, Target, Mapplet, Mapping, Sitzung, "benutzerdefinierte Funktion", Worklet, Arbeitsablauf.
-f	folder_name	Erforderlich. Name des Ordners, der das Objekt enthält.
-n	object_name	Erforderlich. Name des zu löschenden Objekts. Wenn Sie eine Quelldefinition löschen, müssen Sie den Datenbanknamen voranstellen. Beispiel: DBD.sourcename.
-s	dbd_separator	Optional. Wenn bei einer ODBC-Quelle ein Punkt (.) im Namen vorkommt, legen Sie beim Definieren des Quellobjekts ein anderes Trennzeichen fest. Beispiel: Definieren Sie statt database_name.source_name das Quellobjekt als database_name\source_name, und legen Sie als dbd_separator den umgekehrten Schrägstrich (\) fest.

Hinweis: Sie können den DeleteObject-Befehl bei einem nicht versionsgesteuerten Repository ausführen. Wenn Sie den DeleteObject-Befehl bei einem versionsgesteuerten Repository ausführen, gibt *pmrep* den folgenden Fehler zurück:

```
This command is not supported because the versioning is on for the repository
<Repository name>.
Failed to execute DeleteObject
```

DeployDeploymentGroup

Stellt eine Bereitstellungsgruppe bereit. Sie können mit diesem Befehl eine Bereitstellungsgruppe innerhalb eines Repositorys oder in ein anderes Repository kopieren.

Zum Verwenden dieses Befehls müssen Sie eine Steuerdatei mit allen Spezifikationen erstellen, die der Assistent zum Kopieren benötigt. Die Steuerdatei ist eine XML-Datei, die von der Datei depcntl.dtd definiert ist.

Wenn *pmrep* nicht sofort Objektsperren im Target-Repository abrufen kann, wartet er standardmäßig unbegrenzt darauf, die Sperren abzurufen.

Sie können mit den Bereitstellungs-Steuerdatei-Parametern ein Bereitstellungs-Timeout festlegen. Das Bereitstellungs-Timeout ist der Zeitraum (in Sekunden), den *pmrep* auf das Abrufen von Sperren wartet. Bei dem Wert 0 schlägt die Bereitstellung fehl, wenn *pmrep* nicht sofort Sperren abrufen kann. Der Standardwert ist -1, wodurch *pmrep* angewiesen wird, unbegrenzt auf das Abrufen von Sperren zu warten.

Drücken Sie während des Bereitstellungsvorgangs oder während *pmrep* auf das Abrufen von Objektsperren wartet die Tastenkombination Strg+C, um die Bereitstellung abzubrechen.

Der BereitstellungsGruppeBereitstellen-Befehl verwendet die folgende Syntax:

```
deploydeploymentgroup

-p <deployment_group_name>

-c <control_file_name>

-r <target_repository_name>

[-n <target_repository_user_name>

[-s <target_repository_user_security_domain>]

  [-x <target_repository_password> |

   -X <target_repository_password_environment_variable>]

  [-d <target_domain_name> |

   {-h <target_portal_host_name>

    -o <target_portal_port_number>}]] (only if target is in a different domain)

[-l <log_file_name>]
```

In der folgenden Tabelle werden die *pmrep* BereitstellungsGruppeBereitstellen-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-p	deployment_group_name	Erforderlich. Name der bereitzustellenden Gruppe.
-c	control_file_name	Erforderlich. Name der XML-Datei, die die Spezifikationen des Assistenten zum Kopieren enthält. Die Bereitstellungs-Steuerdatei ist erforderlich.
-r	target_repository_name	Erforderlich. Name des Target-Repositorys, in dem Sie die Bereitstellungsgruppe kopieren.

Option	Argument	Beschreibung
-n	target_repository_user_name	Erforderlich, wenn Sie die Bereitstellungsgruppe in ein anderes Repository kopieren. Anmeldebenutzername für das Target-Repository.
-s	target_repository_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Die Standardeinstellung ist "Native".
-x	target_repository_password	Optional. Anmelde-Passwort für das Target-Repository. Verwenden Sie die Option -x oder -X, aber nicht beide. Wenn Sie die Bereitstellungsgruppe in ein anderes Repository kopieren und keine der beiden Optionen -x oder -X verwenden, werden Sie von *pmrep* zur Eingabe des Passworts aufgefordert.
-X	target_repository_password_environment_variable	Optional. Anmelde-Passwort-Umgebungsvariable für das Target-Repository. Verwenden Sie die Option -x oder -X, aber nicht beide. Wenn Sie die Bereitstellungsgruppe in ein anderes Repository kopieren und keine der beiden Optionen -x oder -X verwenden, werden Sie von *pmrep* zur Eingabe des Passworts aufgefordert.
-d	target_domain_name	Erforderlich, wenn Sie die Bereitstellungsgruppe in ein anderes Repository kopieren, ohne die Optionen -h und -o zu verwenden. Name der Domäne für das Repository.
-h	target_portal_host_name	Erforderlich, wenn Sie die Bereitstellungsgruppe in ein anderes Repository kopieren, ohne die Option -d zu verwenden. Name des Computers für den Knoten, der als Host für die Domäne des Target-Repositorys eingesetzt wird.
-o	target_portal_port_number	Erforderlich, wenn Sie die Bereitstellungsgruppe in ein anderes Repository kopieren, ohne die Option -d zu verwenden. Portnummer für den Knoten, der als Host für die Domäne des Target-Repositorys eingesetzt wird.
-l	log_file_name	Optional. Protokolldatei, die die einzelnen Bereitstellungsschritte aufzeichnet. Wenn Sie diese Option auslassen, gibt *pmrep* die Bereitstellungsschritte im Befehlszeilenfenster aus.

DeployFolder

Stellen einen Ordner bereit. Sie können mit diesem Befehl einen Ordner innerhalb eines Repositorys oder in ein anderes Repository kopieren.

Zum Verwenden dieses Befehls müssen Sie eine Steuerdatei mit allen Spezifikationen erstellen, die der Assistent zum Kopieren benötigt. Die Steuerdatei ist eine XML-Datei, die von der Datei depcntl.dtd definiert ist.

Wenn *pmrep* nicht sofort Objektsperren im Target-Repository abrufen kann, wartet er standardmäßig unbegrenzt darauf, die Sperren abzurufen.

Sie können mit den Bereitstellungs-Steuerdatei-Parametern ein Bereitstellungs-Timeout festlegen. Das Bereitstellungs-Timeout ist der Zeitraum (in Sekunden), den *pmrep* auf das Abrufen von Sperren wartet. Bei

dem Wert 0 schlägt die Bereitstellung fehl, wenn *pmrep* nicht sofort Sperren abrufen kann. Der Standardwert ist -1, wodurch *pmrep* angewiesen wird, unbegrenzt auf das Abrufen von Sperren zu warten.

Drücken Sie während des Bereitstellungsvorgangs oder während *pmrep* auf das Abrufen von Objektsperren wartet die Tastenkombination Strg+C, um die Bereitstellung abzubrechen.

Der DeployFolder-Befehl verwendet die folgende Syntax:

```
deployfolder

-f <folder_name>

-c <control_file_name>

-r <target_repository_name>

[-n <target_repository_user_name>

[-s <target_repository_user_security_domain>]

 [-x <target_repository_password> |

  -X <target_repository_password_environment_variable>]

 [-d <target_domain_name> |

   {-h <target_portal_host_name>

    -o <target_portal_port_number>}]] (only if target is in a different domain)

[-l <log_file_name>]
```

In der folgenden Tabelle werden die *pmrep* DeployFolder-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-f	folder_name	Erforderlich. Name des bereitzustellenden Ordners.
-c	control_file_name	Erforderlich. Name der XML-Datei, die die Spezifikationen des Assistenten zum Kopieren enthält.
-r	target_repository_name	Erforderlich. Name des Target-Repositorys, in das Sie den Ordner kopieren.
-n	target_repository_user_name	Erforderlich, wenn Sie den Ordner in ein anderes Repository kopieren. Anmeldebenutzername für das Target-Repository.
-s	target_repository_user_ security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Die Standardeinstellung ist "Native".
-x	target_repository_user_ passwort	Optional. Anmelde-Passwort für das Target-Repository. Verwenden Sie die Option -x oder -X, aber nicht beide. Wenn Sie den Ordner in ein anderes Repository kopieren und keine der beiden Optionen -x oder -X verwenden, werden Sie von *pmrep* zur Eingabe des Passworts aufgefordert.
-X	target_repository_password_ environment_variable	Optional. Anmelde-Passwort-Umgebungsvariable für das Target-Repository. Verwenden Sie die Option -x oder -X, aber nicht beide. Wenn Sie den Ordner in ein anderes Repository kopieren und keine der beiden Optionen -x oder -X verwenden, werden Sie von *pmrep* zur Eingabe des Passworts aufgefordert.

Option	Argument	Beschreibung
-d	target_domain_name	Erforderlich, wenn Sie den Ordner in ein anderes Repository kopieren, ohne die Optionen -h und -o zu verwenden. Name der Domäne für das Repository.
-h	target_portal_host_name	Erforderlich, wenn Sie den Ordner in ein anderes Repository kopieren, ohne die Option -d zu verwenden. Name des Computers für den Knoten, der als Host für die Domäne des Target-Repositorys eingesetzt wird.
-o	target_portal_port_number	Erforderlich, wenn Sie den Ordner in ein anderes Repository kopieren, ohne die Option -d zu verwenden. Portnummer für den Knoten, der als Host für die Domäne des Target-Repositorys eingesetzt wird.
-l	log_file_name	Optional. Protokolldatei, die die einzelnen Bereitstellungsschritte aufzeichnet. Wenn Sie diese Option auslassen, gibt *pmrep* die Bereitstellungsschritte im Befehlszeilenfenster aus.

ExecuteQuery

Führt eine Abfrage aus. Sie können angeben, ob das Ergebnis angezeigt oder in eine persistente Eingabedatei geschrieben werden soll. Wenn die Abfrage erfolgreich ist, wird die Gesamtanzahl der qualifizierten Datensätze geliefert.

Verwenden Sie die persistente Eingabedatei mit den Befehlen ApplyLabel, AddToDeploymentGroup, MassUpdate und Validate.

Der ExecuteQuery-Befehl verwendet die folgende Syntax:

```
executequery

-q <query_name>

[-t <query_type (shared or personal)>]

[-u <output_persistent_file_name>]

[-a (append)]

[-c <column_separator]

[-r <end-of-record_separator>]

[-l <end-of-listing_indicator>]

[-b (verbose)]

[-y (print database type)]

[-n (do not include parent path)]

[-s <dbd_separator>]
```

In der folgenden Tabelle werden die *pmrep* ExecuteQuery-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-q	query_name	Erforderlich. Name der auszuführenden Abfrage.
-t	query_type	Optional. Typ der auszuführenden Abfrage. Sie können festlegen, ob es sich um öffentliche oder private Abfragen handelt. Wenn nicht anders angegeben, sucht *pmrep* zuerst in allen privaten Abfragen nach dem entsprechenden Abfragenamen. Danach werden die öffentlichen Abfragen durchsucht.
-u	persistent_output_file_name	Optional. Senden Sie das Abfrageergebnis in eine Textdatei. Wenn Sie keinen Dateinamen eingeben, wird das Abfrageergebnis in "stdout" ausgegeben.
-a	-	Optional. Hängt die Abfrageergebnisse an die persistente Ausgabedatei an. Wenn Sie diese Option nicht eingeben, überschreibt *pmrep* den Inhalt der Datei.
-c	column_separator	Optional. Zeichen oder Zeichenfolgen, mit denen Spalten mit Objektmetadaten getrennt werden. Verwenden Sie ein Zeichen oder eine Zeichenfolge, die nicht in Repository-Objektnamen verwendet wird. Wenn ein Repository-Objektname Leerzeichen enthält, sollten Sie kein Leerzeichen als Spaltentrenner verwenden. Wenn Sie diese Option auslassen, verwendet *pmrep* ein einzelnes Leerzeichen.
-r	end-of-record_separator	Optional. Zeichen oder Zeichenfolgen, die das Ende von Objektmetadaten kennzeichnen. Verwenden Sie ein Zeichen oder eine Zeichenfolge, die nicht in Repository-Objektnamen verwendet wird. Wenn Sie diese Option auslassen, verwendet *pmrep* eine neue Zeile.
-l	end-of-listing_indicator	Optional. Zeichen oder Zeichenfolgen, die das Ende der Objektliste kennzeichnen. Geben Sie ein Zeichen oder eine Zeichenfolge ein, die nicht in Repository-Objektnamen verwendet wird. Wenn Sie diese Option auslassen, verwendet *pmrep* einen Punkt.
-b	-	Optional. Verbose. Zeigt neben den Mindestinformationen weitere Informationen zu den Objekten an. Wenn Sie diese Option auslassen, druckt *pmrep* ein reduziertes Format, einschließlich Objekttyp, wiederverwendbare oder nicht wiederverwendbare Wörter, Objektname und -pfad. Verbose-Format enthält den Objektstatus, die Versionsnummer, den Ordnernamen und ausgecheckte Informationen. Das Kurzformat für globale Objekte, z. B. Beschriftung, Abfrage, Bereitstellungsgruppe und Verbindung, enthält den Objekttyp und den Objektnamen. Verbose-Format enthält den Beschriftungstyp, den Abfragetyp, den Bereitstellungsgruppen-Typ, den Erstellernamen sowie den Zeitpunkt der Erstellung.
-y	-	Optional. Zeigt den Datenbanktyp von Quellen und Zielen an.

Option	Argument	Beschreibung
-n	-	Optional. Schließt im Abfrageergebnis nicht den vollständigen übergeordneten Pfad der nicht wiederverwendbaren Objekte ein. Wenn Sie beispielsweise diese Option verwenden und das Ergebnis enthält eine nicht wiederverwendbare Transformation, druckt *pmrep* transformation_name statt mapping_name.transformation_name. Diese Option kann die Leistung von *pmrep* erhöhen.
-s	dbd_separator	Optional. Wenn bei einer ODBC-Quelle ein Punkt (.) im Namen vorkommt, legen Sie beim Definieren des Quellobjekts ein anderes Trennzeichen fest. Beispiel: Definieren Sie statt database_name.source_name das Quellobjekt als database_name \source_name, und legen Sie als dbd_separator den umgekehrten Schrägstrich (\) fest.

Exit

Beendet den interaktiven Modus von *pmrep*.

Bei jeder Befehlseingabe wird *pmrep* vom Befehlszeilenmodus aufgerufen und beendet.

Der Exit-Befehl verwendet die folgende Syntax:

```
exit
```

FindCheckout

Zeigt eine Liste der ausgecheckten Objekte im Repository an. Die Auflistung enthält die ausgecheckten Einträge, außer wenn Sie "alle Benutzer" eingeben.

Wenn Sie einen Objekttyp auswählen, können Sie ausgecheckte Objekte in einem bestimmten Ordner oder in allen Ordnern auflisten. Wenn Sie keinen Objekttyp angeben, gibt *pmrep* alle ausgecheckten Objekte im Repository zurück.

Der FindCheckout-Befehl verwendet die folgende Syntax:

```
findcheckout

[-o <object_type>]

[-f <folder_name>]

[-u (all_users)]

[-c <column_separator>]

[-r <end-of-record_separator>]

[-l <end-of-listing_indicator>]

[-b (verbose)]

[-y (print database type)]
```

```
[-s <dbd_separator>]
```

In der folgenden Tabelle werden die *pmrep* FindCheckout-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-o	object_type	Aufzulistender Objekttyp. Sie können Quelle, Ziel, Umwandlung, Mapping, Sitzung, Worklet, Arbeitsablauf, Scheduler, Sitzungskonfiguration, Aufgabe, Cube oder Größenordnung festlegen. Wenn Sie diese Option nicht verwenden, ignoriert *pmrep* die Optionen -f und -u und der Befehl gibt alle ausgecheckten Objekte im Repository zurück.
-f	folder_name	Optional, wenn Sie einen Objekttyp angeben. Gibt eine Liste der ausgecheckten Objekte für den Objekttyp im angegebenen Ordner zurück. Standardmäßig werden Objekte für den Objekttyp ordnerübergreifend aufgelistet.
-u	-	Optional. Listen Sie die ausgecheckten Objekte aller Benutzer auf. Standardmäßig werden ausgecheckte Objekte des aktuellen Benutzers aufgelistet.
-c	column_separator	Optional. Zeichen oder Zeichenfolgen, mit denen Spalten mit Objektmetadaten getrennt werden. Verwenden Sie ein Zeichen oder eine Zeichenfolge, die nicht in Repository-Objektnamen verwendet wird. Wenn ein Repository-Objektname Leerzeichen enthält, sollten Sie kein Leerzeichen als Spaltentrenner verwenden. Wenn Sie diese Option auslassen, verwendet *pmrep* ein einzelnes Leerzeichen.
-r	end-of-record_separator	Optional. Zeichen oder Zeichenfolgen, die das Ende von Objektmetadaten kennzeichnen. Verwenden Sie ein Zeichen oder eine Zeichenfolge, die nicht in Repository-Objektnamen verwendet wird. Standardmäßig wird für eine neue Zeile /n verwendet.
-l	end-of-listing_indicator	Optional. Zeichen oder Zeichenfolgen, die das Ende der Objektliste kennzeichnen. Verwenden Sie ein Zeichen oder eine Zeichenfolge, die nicht in Repository-Objektnamen verwendet wird. Wenn Sie diese Option auslassen, verwendet *pmrep* einen Punkt.
-b	-	Optional. Verbose. Zeigt neben den Mindestinformationen weitere Informationen zu den Objekten an. Wenn Sie diese Option auslassen, druckt *pmrep* ein reduziertes Format, einschließlich Objekttyp, wiederverwendbare oder nicht wiederverwendbare Wörter, Objektname und -pfad. Verbose-Format enthält die Versionsnummer und den Ordnernamen. Das Kurzformat für globale Objekte wie Beschriftung, Abfrage, Bereitstellungsgruppe und Verbindung enthält den Objekttyp und den Objektnamen. Verbose-Format enthält den Erstellernamen und den Zeitpunkt der Erstellung.

Option	Argument	Beschreibung
-y	-	Optional. Zeigt den Datenbanktyp von Quellen und Zielen an.
-s	dbd_separator	Optional. Wenn bei einer ODBC-Quelle ein Punkt (.) im Namen vorkommt, legen Sie beim Definieren des Quellobjekts ein anderes Trennzeichen fest. Beispiel: Definieren Sie statt database_name.source_name das Quellobjekt als database_name \source_name, und legen Sie als dbd_separator den umgekehrten Schrägstrich (\) fest.

GetConnectionDetails

Listet die Eigenschaften und Attribute eines Verbindungsobjekts als Name-Wert-Paar auf.

Für die Verwendung des GetConnectionDetails-Befehls benötigen Sie die Leseberechtigung für das Verbindungsobjekt.

Der GetConnectionDetails-Befehl verwendet die folgende Syntax:

```
getconnectiondetails

-n <connection_name>

-t <connection_type>
```

In der folgenden Tabelle werden die *pmrep* GetConnectionDetails-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-n	connection_name	Erforderlich. Name der Verbindung, für die Details aufgelistet werden sollen.
-t	connection_type	Erforderlich. Typ der Verbindung. Folgende Verbindungstypen sind möglich: - Application - FTP - Loader - Warteschlange - Relational

GenerateAbapProgramToFile

Generiert das ABAP-Programm für ein Mapping mit SAP-Tabelle als Quelle und speichert das Programm als Datei. Der GenerateAbapProgramToFile-Befehl generiert das ABAP-Programm für ein Mapping im PowerCenter Repository. Das generierte Programm wird als Datei gespeichert. Sie können den GenerateAbapProgramToFile-Befehl für Mappings verwenden, die als Quelle SAP-Tabellen benutzen.

Die Benennungskonvention für die Datei lautet *mappingname_<version>_<program_mode>.ab4*. Sie müssen den Pfad und den Dateinamen in doppelte Anführungszeichen einschließen. Nachdem Sie das ABAP-

Programm generiert und in eine Datei gespeichert haben, verwenden Sie den InstallAbapProgram-Befehl, um es auf einem SAP-System zu installieren.

Der GenerateAbapProgramToFile-Befehl verwendet die folgende Syntax:

```
generateabapprogramtofile

-s <folder_name>

-m <mapping_name>

[-v <version_number>]

[-l <log_filename>]

-u <user_name>

-x <password>

-c <connect_string>

-t <client>

[-y <language>]

-p <program_mode (file, stream)>

-f <output_file_location>

{-e (enable override)

-o <override_name> }

[-a (authority check)]

[-n (use namespace)]
```

In der folgenden Tabelle werden die pmrep GenerateAbapProgramToFile-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-s	folder_name	Erforderlich. Der Name des Ordners, der das Mapping enthält, für das das ABAP-Programm generiert werden muss.
-m	mapping_name	Erforderlich. Name des Mappings.
-v	version_number	Optional. Versionsnummer des Mappings. Standardmäßig ist die neueste Version.
-l	log_filename	Optional. Name der Protokolldatei, in die die Informationen oder Fehlermeldungen geschrieben werden. Standardmäßig wird die Protokolldatei in dem Verzeichnis erstellt, in dem Sie den Befehl ausführen.
-u	user_name	Erforderlich. Benutzername für die SAP-Quellsystemverbindung. Muss ein Benutzer sein, für den Sie eine Quellsystemverbindung erstellt haben.
-x	passwort	Erforderlich. Passwort für den Benutzernamen. Verwenden Sie das Befehlszeilenprogramm pmpasswd zum Verschlüsseln des Benutzerpasswords.
-c	connect_string	Erforderlich. In der Datei `sapnwrfc.ini` definierter DEST-Eintrag für eine Verbindung mit einem bestimmten SAP-Anwendungsserver oder für eine Verbindung, die den SAP-Lastenausgleich verwendet.

Option	Argument	Beschreibung
-t	Client	Erforderlich. SAP-Clientnummer.
-y	Sprache	Optional. SAP-Anmeldesprache. Muss mit der Codepage des PowerCenter Client kompatibel sein. Standardwert ist die Sprache des SAP-Systems.
-p	program_mode (file, stream)	Erforderlich. Modus, in denen der PowerCenter-Integrationsdienst Daten aus dem SAP-System extrahiert. Wählen Sie die Datei oder den Stream aus.
-f	output_file_location	Erforderlich. Speicherort im lokalen Rechner, auf dem Sie die ABAP-Programmdatei speichern möchten.
-e	-	Optional. Überschreibt den standardmäßigen Namen der ABAP-Programmdatei.
-o	override_name	Erforderlich, wenn Sie das Überschreiben aktivieren. ABAP-Programmdateiname.
-a	-	Optional. Fügt dem ABAP-Programm Autoritätsprüfungen hinzu.
-n	-	Optional. Hängt dem ABAP-Programmnamen einen Namespace an, den Sie bei SAP registriert haben.

Beispiel

Im folgenden Beispiel wird ein ABAP-Programm generiert und in einer Datei gespeichert:

```
generateabapprogramtofile -s folder_name -m mapping_name -l logfile_name -u user_name -x
password -c connect_string -t 800 -y EN -p stream -e -o program_name -n -a -f "C:
\<informatica_installation_dir>\ABAP_prog"
```

Hilfe

Gibt die Syntax für den angegebenen Befehl zurück. Wenn Sie keinen Befehl angeben, wird die Syntax für alle *pmrep*-Befehle angezeigt.

Verwenden Sie für den Help-Befehl eine der folgenden Syntaxstrukturen:

```
help [command]
-help [command]
```

InstallAbapProgram

Installiert ein ABAP-Programm in das SAP-System. Verwenden Sie den InstallAbapProgram-Befehl, um das ABAP-Programm zu generieren und direkt auf dem SAP-System zu installieren. Sie können mit diesem Befehl ein ABAP-Programm aus einer Datei auf dem SAP-System installieren. Sie können den InstallAbapProgram-Befehl für Mappings verwenden, die SAP-Tabellen als Quelle nutzen.

Der InstallAbapProgram-Befehl ruft die Mapping-Informationen über das PowerCenter Repository für ein Mapping ab und generiert das ABAP-Programm. Der Befehl installiert das generierte ABAP-Programm in das SAP-System. Wenn Sie das ABAP-Programm zum ersten Mal auf dem SAP-System installieren, generiert der

Befehl einen Programmnamen. Nachfolgende Installationen verwenden den gleichen Programmnamen, wenn Sie den gleichen Programmmodus nutzen.

Wenn Sie ein ABAP-Programm über eine Datei auf dem SAP-System installieren, müssen Sie den vollständigen Pfad und den Dateinamen des zu installierenden ABAP-Programms zur Verfügung stellen. Schließen Sie den Pfad und den Dateinamen in doppelte Anführungszeichen ein. Sie müssen den Ordnernamen und die Mapping-Informationen angeben, für die das ABAP-Programm generiert wurde. Der InstallAbapProgram-Befehl ruft die Beschreibung des Mappings ab und hängt sie an das ABAP-Programm an, wenn es auf dem SAP-System installiert wird.

Der InstallAbapProgram-Befehl verwendet die folgende Syntax:

```
installabapprogram

-s <folder_name>

-m <mapping_name>

[-v <version_number>]

[-l <log_filename>]

-u <user_name>

-x <password>

-c <connect_string>

-t <client>

[-y <language>]

{-f <input_file_name> |

-p <program_mode (file, stream)>

{-e (enable override)

-o <override_name> }

[-a (authority check)]

[-n (use namespace)]}

[-d <development_class_name>]
```

In der folgenden Tabelle werden die pmrep InstallAbapProgram-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-s	folder_name	Erforderlich. Der Name des Ordners, der das Mapping enthält, für das das ABAP-Programm generiert werden muss. Bei Installation über eine Datei der Name des Ordners, der das Mapping enthält, für das Sie das ABAP-Programm generiert haben.
-m	mapping_name	Erforderlich. Name des Mappings. Bei Installation über eine Datei der Name des Mappings, für das Sie das ABAP-Programm generiert haben.
-v	version_number	Optional. Versionsnummer des Mappings. Standardmäßig ist die neueste Version. Bei Installation über eine Datei die Version des Mappings, für das Sie das ABAP-Programm generiert haben.

Option	Argument	Beschreibung
-l	log_filename	Optional. Name der Protokolldatei, in die die Informationen oder Fehlermeldungen geschrieben werden. Standardmäßig wird die Protokolldatei in dem Verzeichnis gespeichert, in dem Sie den Befehl ausführen.
-u	user_name	Erforderlich. Benutzername für die SAP-Quellsystemverbindung. Muss ein Benutzer sein, für den Sie eine Quellsystemverbindung erstellt haben.
-x	passwort	Erforderlich. Passwort für den Benutzernamen. Verwenden Sie das Befehlszeilenprogramm pmpasswd zum Verschlüsseln des Benutzerpasswords.
-c	connect_string	Erforderlich. In der Datei `sapnwrfc.ini` definierter DEST-Eintrag für eine Verbindung mit einem bestimmten SAP-Anwendungsserver oder für eine Verbindung, die den SAP-Lastenausgleich verwendet.
-t	Client	Erforderlich. SAP-Clientnummer.
-y	Sprache	Optional. SAP-Anmeldesprache. Muss mit der Codepage des PowerCenter Client kompatibel sein. Standardwert ist die Sprache des SAP-Systems.
-f	input_file_name	Erforderlich, wenn Sie das ABAP-Programm mit einer Datei installieren. Name der ABAP-Programmdatei, von der aus Sie das ABAP-Programm in das SAP-System installieren möchten.
-p	program_mode (file, stream)	Erforderlich, wenn Sie das ABAP-Programm direkt auf dem SAP-System generieren und installieren. Optional, wenn Sie das ABAP-Programm mit einer Datei installieren. Modus, in denen der PowerCenter-Integrationsdienst Daten aus dem SAP-System extrahiert. Wählen Sie die Datei oder den Stream aus.
-e	-	Optional, wenn Sie das ABAP-Programm direkt auf dem SAP-System generieren und installieren. Überschreibt den standardmäßigen Namen der ABAP-Programmdatei.
-o	override_name	Erforderlich, wenn Sie das Überschreiben aktivieren. ABAP-Programmdateiname.
-a	-	Optional, wenn Sie das ABAP-Programm direkt auf dem SAP-System generieren und installieren. Fügt dem ABAP-Programm Autoritätsprüfungen hinzu.
-n	-	Optional, wenn Sie das ABAP-Programm direkt auf dem SAP-System generieren und installieren. Hängt dem ABAP-Programmnamen einen Namespace an, den Sie bei SAP registriert haben.
-d	development_class_name	Optional. Paket oder der Name der Entwicklungsklasse, in der der PowerCenter-Repository-Dienst das ABAP-Programm installiert. Standardentwicklungsklasse ist $TMP.

Beispiele

Das folgende Beispiel installiert das ABAP-Programm direkt auf dem SAP-System:

```
installabapprogram -s folder_name -m mapping_name -l logfile_name -u user_name -x
password -c connect_string -t 800 -y EN -p file -e -o zabc -a -n -d development_class
```

Das folgende Beispiel installiert das ABAP-Programm von einer Datei auf dem SAP-System:

```
installabapprogram -s folder_name -m mapping_name -l logfile_name -u user_name -x
password -c connect_string -t 800 -y EN -p file -v 1 -f "C:
\mapping_name_version_file.ab4"
```

KillUserConnection

Beendet Benutzerverbindungen zum Repository. Sie können Benutzerverbindungen basierend auf dem Benutzernamen oder der Verbindungs-ID beenden. Sie können auch alle Benutzerverbindungen zum Repository beenden.

Der KillUserConnection-Befehl verwendet die folgende Syntax:

```
killuserconnection

{-i <connection_id> |

-n <user_name> |

-a (kill all)}
```

In der folgenden Tabelle werden die *pmrep* KillUserConnection-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-i	connection_id	Repository-Verbindungs-ID.
-n	user_name	Benutzername.
-a	-	Beendet alle Verbindungen.

ListConnections

Listet alle Verbindungsobjekte im Repository und deren jeweilige Verbindungstypen auf. Folgende Verbindungstypen sind möglich:

- Anwendung
- FTP
- Loader
- Warteschlange
- Relational

Der ListConnections-Befehl verwendet die folgende Syntax:

```
listconnections

[-t (output includes connection subtype)]
```

In der folgenden Tabelle wird die *pmrep* ListConnections-Option beschrieben:

Option	Argument	Beschreibung
-t	-	Optional. Zeigt den Verbindungs-Subtyp an. Bei einer relationalen Verbindung gehören beispielsweise zu den Verbindungs-Subtypen Oracle, Sybase und Microsoft SQL Server. Sie können nur den Subtyp für Verbindungen anzeigen, für die Sie eine Leseberechtigung haben.

ListObjectDependencies

Listet Abhängigkeitsobjekte für wiederverwendbare und nicht wiederverwendbaren Objekte auf. Wenn Sie Abhängigkeiten für nicht wiederverwendbare Objekte auflisten möchten, müssen Sie eine persistente Eingabedatei verwenden, die Objekt-IDs enthält. Sie können diese Datei erstellen, indem Sie eine Abfrage ausführen und den Befehl zum Erstellen einer Textdatei auswählen.

ListObjectDependencies akzeptiert eine persistente Eingabedatei und kann eine persistente Ausgabedatei erstellen. Diese Dateien haben das gleiche Format. Wenn Sie eine Ausgabedatei erstellen, verwenden Sie diese als Eingabe für die *pmrep*-Befehle ApplyLabel, AddToDeploymentGroup oder Validate.

ListObjectDependencies gibt die Anzahl der Datensätze zurück, wenn der Befehl erfolgreich ausgeführt wird.

Der ListObjectDependencies-Befehl verwendet die folgende Syntax:

```
listobjectdependencies

{{-n <object_name>

  -o <object_type>

  [-t <object_subtype>]

  [-v <version_number>]

  [-f <folder_name>] } |

   -i <persistent_input_file>}

[-d <dependency_object_types>]

[-p <dependency_direction (children, parents, or both)>]

[-s (include pk-fk dependency)]

[-g (across repositories)]

[-u <persistent_output_file_name>

  [-a (append)]]

[-c <column_separator>]

[-r <end-of-record_separator>]

[-l <end-of-listing_indicator>]

[-b (verbose)]

[-y (print database type)]

[-e <dbd_separator>]
```

In der folgenden Tabelle werden die *pmrep* ListObjectDependencies-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-n	object_name	Erforderlich. Name eines bestimmten Objekts, für das Abhängigkeiten aufgelistet werden sollen.
-o	object_type	Erforderlich. Objekttyp, für den Abhängigkeiten aufgelistet werden sollen. Sie können Quelle, Ziel, Umwandlung, Mapping, Sitzung, Worklet, Arbeitsablauf, Scheduler, Sitzung, Sitzungskonfiguration, Aufgabe, Cube und Größenordnung festlegen.

Option	Argument	Beschreibung
-t	object_subtype	Typ der Transformation oder Aufgabe. Ignoriert bei anderen Objekttypen. Weitere Informationen zu gültigen Subtypen finden Sie unter "Auflisten von Objekttypen" auf Seite 1192.
-v	version_number	Optional. Listen Sie abhängige Objekte für eine andere Objektversion als die neueste Version auf. Sie müssen diese Option nur bei versionsgesteuerten Repositories verwenden. Sie wird nicht auf nicht versionsgesteuerte Repositories angewendet.
-f	folder_name	Ordner, der den Objektnamen enthält. Ordner ist erforderlich, wenn Sie nicht die Option -i verwenden.
-i	persistent_input_file	Optional. Textdatei von Objekten, die mit den Befehlen ExecuteQuery oder Validate generiert wurde. Sie müssen diese Datei verwenden, wenn Sie Abhängigkeiten für nicht wiederverwendbare Objekte auflisten möchten. Wenn Sie diese Option nutzen, können Sie nicht die Optionen -n, -o und -f zur Angabe von Objekten verwenden.
-d	dependency_object_types	Optional. Typ der aufzulistenden abhängigen Objekte. Sie können alle oder einen bzw. mehrere Objekttypen eingeben. Die Stanardeinstellung ist "ALL". Wenn die Option für alle Objekte ausgewählt ist, listet *pmrep* alle unterstützten abhängigen Objekte auf. Wenn Sie eine oder mehrere Objekte auswählen, dann listet *pmrep* abhängige Objekte für diese Typen auf. Um mehrere Objekttypen einzugeben, trennen Sie diese durch Kommas ohne Leerzeichen ab.
-p	dependency_direction	Erforderlich, wenn Sie nicht die Option -s verwenden. Übergeordnete oder untergeordnete abhängige Objekte, die aufgelistet werden sollen. Sie können übergeordnete oder untergeordnete Objekte bzw. beides festlegen. Wenn Sie die Option -p nicht verwenden, listet *pmrep* keine übergeordneten und untergeordneten Abhängigkeiten auf.
-s	-	Erforderlich, wenn Sie die Option -p nicht verwenden. Schließen Sie das Objekt mit Primärschlüssel-Fremdschlüssel-Abhängigkeiten unabhängig von der Abhängigkeitsrichtung ein. Wenn Sie die Option -s nicht verwenden, listet *pmrep* keine Primärschlüssel-Fremdschlüssel-Abhängigkeiten auf.
-g	-	Optional. Suchen Sie nach Objektabhängigkeiten über Repositories.
-u	persistent_output_file_name	Senden Sie das Abhängigkeitsergebnis in eine Textdatei. Verwenden Sie die Datei als Eingabe in die *pmrep*-Befehle ApplyLabel, AddToDeploymentGroup oder Validate. Standardmäßig wird das Abfrageergebnis an "stdout" gesendet. Sie können bei dieser Option nicht die Optionen -b und -c verwenden.
-a	-	Hängen Sie das Ergebnis an die persistente Ausgabedatei an, statt diese zu überschreiben.
-c	column_separator	Zeichen oder Zeichenfolgen, mit denen Spalten mit Objektmetadaten getrennt werden. Verwenden Sie ein Zeichen oder eine Zeichenfolge, die nicht in Repository-Objektnamen verwendet wird. Wenn ein Repository-Objektname Leerzeichen enthält, sollten Sie kein Leerzeichen als Spaltentrenner verwenden. Sie können diese Option nicht zusammen mit der Option -u verwenden. Wenn Sie diese Option auslassen, verwendet *pmrep* ein einzelnes Leerzeichen.

Option	Argument	Beschreibung
-r	end-of-record_separator	Zeichen oder Zeichenfolgen, die das Ende von Objektmetadaten kennzeichnen. Verwenden Sie ein Zeichen oder eine Zeichenfolge, die nicht in Repository-Objektnamen verwendet wird. Standardmäßig wird für eine neue Zeile /n verwendet.
-l	end-of-listing_indicator	Zeichen oder Zeichenfolgen, die das Ende der Objektliste kennzeichnen. Geben Sie ein Zeichen oder eine Zeichenfolge ein, die nicht in Repository-Objektnamen verwendet wird. Wenn Sie diese Option auslassen, verwendet *pmrep* einen Punkt.
-b	-	Verbose. Zeigt neben den Mindestinformationen weitere Informationen zu den Objekten an. Wenn Sie diese Option auslassen, zeigt *pmrep* ein reduziertes Format an, einschließlich Objekttyp, wiederverwendbare oder nicht wiederverwendbare Wörter, Objektname und -pfad. Verbose-Format enthält die Versionsnummer und den Ordnernamen. Das Kurzformat für globale Objekte, z. B. Beschriftung, Abfrage, Bereitstellungsgruppe und Verbindung, enthält den Objekttyp und den Objektnamen. Verbose-Format enthält den Erstellernamen und den Zeitpunkt der Erstellung. Sie können diese Option nicht zusammen mit der Option -u verwenden.
-y	-	Optional. Zeigt den Datenbanktyp von Quellen und Zielen an.
-e	dbd_separator	Optional. Wenn bei einer ODBC-Quelle ein Punkt (.) im Namen vorkommt, legen Sie beim Definieren des Quellobjekts ein anderes Trennzeichen fest. Beispiel: Definieren Sie statt database_name.source_name das Quellobjekt als database_name\source_name, und legen Sie als dbd_separator den umgekehrten Schrägstrich (\) fest.

ListObjects

Gibt eine Liste von Objekten im Repository zurück. Wenn Sie Objekte auflisten, gibt *pmrep* Objektmetadaten zurück. Verwenden Sie die folgenden Auflistungsoperationen:

- **Auflisten von Objekttypen**. Definieren Sie die aufzulistenden Objekte.
- **Auflisten von Ordnern**. Listen Sie alle Ordner im Repository auf.
- **Auflisten von Objekten**. Listen Sie wiederverwendbare und nicht wiederverwendbare Objekte im Repository oder in einem Ordner auf.

Verwenden Sie ListObjects in einem Shell-Skript, um Objektmetadaten zurückzugeben und Metadaten zu parsen. Verwenden Sie anschließend die geparsten Daten in einem anderen *pmrep*-Befehl.

Verwenden Sie zum Beispiel ListObjects, um alle Sequenzgenerator-Transformationen im Repository aufzulisten. Erstellen Sie ein Shell-Skript, das ListObjects verwendet, um die Informationen der Sequenzgenerator-Transformation zurückzugeben, parsen Sie die von ListObjects zurückgegebenen Daten und verwenden Sie UpdateSeqGenVals, um die Sequenzwerte zu aktualisieren.

pmrep gibt jedes Objekt in einem Datensatz und gibt die Metadaten für jedes einzelne Objekt in einer Spalte zurück. Die Datensätze werden standardmäßig durch eine neue Zeile getrennt. Sie können die Zeichen eingeben, die zum Trennen von Datensätzen und Spalten verwendet werden. Sie können zudem die Zeichen eingeben, die das Ende einer Liste kennzeichnen.

Tipp: Wenn Sie Zeichen zum Trennen von Datensätzen und Spalten und zum Kennzeichnen des Listenendes eingeben, verwenden Sie Zeichen, die nicht in Repository-Objektnamen benutzt werden. Dies hilft bei der Verwendung eines Shell-Skripts zum Parsen der Objektmetadaten.

Der ListObjects-Befehl verwendet die folgende Syntax:

```
listobjects

-o <object_type>

[-t <object_subtype>]

[-f <folder_name>]

[-c <column_separator>]

[-r <end-of-record_indicator>]

[-l <end-of-listing_indicator>]

[-b (verbose)]

[-y (print database type)]

[-s <dbd_separator>]
```

In der folgenden Tabelle werden die *pmrep* ListObject-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-o	object_type	Erforderlich. Aufzulistender Objekttyp. - Wenn Sie Ordner eingeben, muss keine andere Option eingeschlossen werden. *pmrep* ignoriert die Optionen -t und -f. - Wenn Sie andere Objekte als Ordner eingeben, müssen Sie die Option -f einschließen. - Wenn Sie Transformation oder Aufgabe eingeben, müssen Sie die Option -f einschließen. Optional können Sie die Option -t einschließen. Weitere Informationen über Objekttypen, die mit ListObjects verwendet werden können, finden Sie unter "Auflisten von Objekttypen" auf Seite 1192.
-t	object_subtype	Optional. Aufzulistender Transformations- oder Aufgabentyp. Wenn Sie Transformation oder Aufgabe als Objekttyp eingeben, können Sie diese Option einschließen, um einen bestimmten Typ zurückzugeben. Weitere Informationen über Objekttypen, die mit ListObjects verwendet werden können, finden Sie unter "Auflisten von Objekttypen" auf Seite 1192.
-f	folder_name	Erforderlich, wenn Sie andere Objekte als Ordner auflisten. Zu suchender Ordner. Verwenden Sie diese Option bei allen Objekttypen außer Bereitstellungsgruppe, Ordner, Beschriftung und Abfrage.
-c	column_separator	Optional. Zeichen oder Zeichenfolgen, mit denen Spalten mit Objektmetadaten getrennt werden. Verwenden Sie ein Zeichen oder eine Zeichenfolge, die nicht in Repository-Objektnamen verwendet wird. Wenn ein Repository-Objektname Leerzeichen enthält, sollten Sie kein Leerzeichen als Spaltentrenner verwenden. Wenn Sie diese Option auslassen, verwendet *pmrep* ein einzelnes Leerzeichen.

Option	Argument	Beschreibung
-r	end-of-record_indicator	Optional. Zeichen oder Zeichenfolgen, die das Ende von Objektmetadaten kennzeichnen. Verwenden Sie ein Zeichen oder eine Zeichenfolge, die nicht in Repository-Objektnamen verwendet wird. Standardmäßig wird für eine neue Zeile /n verwendet.
-l	end_of_listing_indicator	Optional. Zeichen oder Zeichenfolgen, die das Ende der Objektliste kennzeichnen. Geben Sie ein Zeichen oder eine Zeichenfolge ein, die nicht in Repository-Objektnamen verwendet wird. Wenn Sie diese Option auslassen, verwendet *pmrep* einen Punkt.
-b	-	Optional. Verbose. Zeigen Sie neben den Mindestinformationen weitere Informationen zu den Objekten an. Wenn Sie diese Option auslassen, zeigen Sie ein reduziertes Format an, einschließlich Objekttyp, wiederverwendbare oder nicht wiederverwendbare Wörter, Objektname und -pfad. Verbose-Format enthält den Objektstatus, die Versionsnummer, den Ordnernamen und ausgecheckte Informationen. Das Kurzformat für globale Objekte, z. B. Beschriftung, Abfrage, Bereitstellungsgruppe und Verbindung, enthält den Objekttyp und den Objektnamen. Verbose-Format enthält den Beschriftungstyp, den Abfragetyp, den Bereitstellungsgruppen-Typ, den Erstellernamen sowie den Zeitpunkt der Erstellung.
-y	-	Optional. Zeigt den Datenbanktyp von Quellen und Zielen an.
-s	dbd_separator	Optional. Wenn bei einer ODBC-Quelle ein Punkt (.) im Namen vorkommt, legen Sie beim Definieren des Quellobjekts ein anderes Trennzeichen fest. Beispiel: Definieren Sie statt database_name.source_name das Quellobjekt als database_name\source_name, und legen Sie als dbd_separator den umgekehrten Schrägstrich (\) fest.

Auflisten von Objekttypen

Verwenden Sie die Option object_type, um die aufzulistenden Objekte zu definieren. Der Befehl listet die neuesten Versionen oder ausgecheckten Versionen von Objekten auf, einschließlich Shortcuts jedoch ausschließlich der Objekte gemäß der Regeln für Objekttypen.

In der folgenden Tabelle werden die Objekttypen und Regeln beschrieben, die bei ListObjects verwendet werden:

Objekttyp	Regel
Deploymentgroup	Listet Bereitstellungsgruppen im Repository auf.
Folder	Listet Ordner im Repository auf.
Beschriften	Listet Beschriftungen im Repository auf.
Mapplet	Listet Mapplets mit der neuesten oder ausgecheckten Version in einem Ordner auf, einschließlich Shortcuts jedoch ausschließlich der Instanzen wiederverwendbarer Mapplets.

Objekttyp	Regel
Mapping	Listet Mappings mit der neuesten oder ausgecheckten Version in einem Ordner auf, einschließlich Shortcuts jedoch ausschließlich der Instanzen wiederverwendbarer Mapplets.
Abfrage	Listet Abfragen im Repository auf.
Scheduler	Listet wiederverwendbare und nicht wiederverwendbare Scheduler mit der neuesten oder ausgecheckten Version in einem Ordner auf.
Sitzung	Listet wiederverwendbare und nicht wiederverwendbare Sitzungen mit der neuesten oder ausgecheckten Version in einem Ordner auf, ausschließlich der Instanzen wiederverwendbarer Sitzungen.
Sitzungskonfig	Listet die Sitzungskonfigurationen mit der neuesten oder ausgecheckten Version in einem Ordner auf.
Quelle	Listet Quellen mit der neuesten oder ausgecheckten Version in einem Ordner auf, einschließlich Shortcuts jedoch ausschließlich der Quellinstanzen.
Target	Listet Targets mit der neuesten oder ausgecheckten Version in einem Ordner auf, einschließlich Shortcuts jedoch ausschließlich von Target-Instanzen.
Aufgabe	Listet wiederverwendbare und nicht wiederverwendbare Aufgaben mit der neuesten oder ausgecheckten Version in einem Ordner auf.
Transformation	Listet wiederverwendbare und nicht wiederverwendbare Transformationen mit der neuesten oder ausgecheckten Version in einem Ordner auf, einschließlich Shortcuts und ausschließlich der Instanzen wiederverwendbarer Transformationen.
"Benutzerdefinierte Funktion"	Listet benutzerdefinierte Funktionen im Repository auf.
Arbeitsablauf	Listet die Arbeitsabläufe mit der neuesten oder ausgecheckten Version in einem Ordner auf.
Worklet	Listet wiederverwendbare und nicht wiederverwendbare Worklets mit der neuesten oder ausgecheckten Version in einem Ordner auf, ausschließlich der Instanzen wiederverwendbarer Worklets.

In der folgenden Tabelle werden die Objekttypen und Werte beschrieben, die bei den *pmrep*-Befehlen verwendet werden:

Objekttyp	Subtypwert	Beschreibung
Aufgabe	zuweisung	Zuweisung
Aufgabe	befehl	Befehl
Aufgabe	kontrolle	Kontrolle
Aufgabe	entscheidung	Entscheidung
Aufgabe	email	E-Mail

Objekttyp	Subtypwert	Beschreibung
Aufgabe	event_raise	Event-Raise
Aufgabe	event_wait	Event-Wait
Aufgabe	start	Start
Aufgabe	timer	Timer
Transformation	aggregator	Aggregator
Transformation	application_source_qualifier	Anwendungsquellqualifikator
Transformation	app_multi-group_source_qualifier	Anwendungs-Mehrfachgruppen-Quellenqualifikator
Transformation	custom_transformation	Custom
Transformation	custom_transformation	HTTP
Transformation	custom_transformation	SQL
Transformation	custom_transformation	Union
Transformation	custom_transformation	XML-Generator
Transformation	custom_transformation	XML-Parser
Transformation	expression	Ausdruck
Transformation	external_procedure	Externe Prozedur
Transformation	filter	Filter
Transformation	input_transformation	Eingabe
Transformation	java	Java
Transformation	joiner	Joiner
Transformation	lookup_procedure	Lookup
Transformation	mq_source_qualifier	MQ-Quellqualifikator
Transformation	normalizer	Normalizer
Transformation	output_transformation	Ausgabe
Transformation	rang	Rang
Transformation	router	Router
Transformation	sequenz	Sequenzgenerator
Transformation	sortierer	Sortierer

Objekttyp	Subtypwert	Beschreibung
Transformation	source_qualifier	Quellqualifikator
Transformation	stored_procedure	Gespeicherte Prozedur
Transformation	transaction_control	Transaktionssteuerung
Transformation	update_strategy	Update-Strategie
Transformation	xml_source_qualifier	XML-Quellqualifikator

Auflisten von Ordnern

Verwenden Sie ListObjects, um jeden Ordner im Repository zurückzugeben. Wenn Sie als Objekttyp `Ordner` eingeben, ignoriert *pmrep* den Subtyp und den Ordnernamen.

Zum Auflisten aller Ordner im Repository verwenden Sie beispielsweise die folgende Syntax:

```
listobjects -o folder
```

Alternativ können Sie einen anderen Spaltentrenner und Listenende-Indikator eingeben:

```
ListObjects -o folder -c "**" -l #
```

Auflisten von Objekten

Verwenden Sie ListObjects, um wiederverwendbare und nicht wiederverwendbare Objekte im Repository oder in einem Ordner aufzulisten. *pmrep* enthält keine Instanzen wiederverwendbarer Objekte. Wenn Sie Objekte auflisten, müssen Sie den Ordnernamen für alle Objekte einschließen, die einem Ordner zugeordnet sind.

pmrep gibt ggf. den Namen des Objekts mit dem Pfad zurück. Wenn beispielsweise ein Mapping oder Mapplet eine Transformation enthält, gibt *pmrep mapping_name.transformation_name* oder *mapplet_name.transformation_name* zurück.

Weitere Informationen zu einer Liste der Umwandlungs- oder Aufgaben-Rückgabewerte finden Sie unter "Auflisten von Objekttypen" auf Seite 1192.

Um beispielsweise alle Transformationstypen in einem Ordner aufzulisten, geben Sie den folgenden Text bei der Eingabeaufforderung ein:

```
listobjects -o transformation -f myfolder
```

pmrep gibt die folgenden Informationen zurück:

```
stored_procedure reusable sp_sproc1
expression reusable exp1
stored_procedure non-reusable mapping1.sp_nsproc
sequence non-reusable smallmapplet.seqgen_empid
.listobjects completed successfully.
```

Um alle Transformationen einer gespeicherten Prozedur aufzulisten, geben Sie den folgenden Text bei der Eingabeaufforderung ein:

```
listobjects -o transformation -t stored_procedure -f myfolder
```

pmrep gibt die folgenden Informationen zurück:

```
stored_procedure reusable sp_sproc1
stored_procedure non-reusable mapping1.sp_nsproc
.listobjects completed successfully.
```

Um alle Sitzungen in einem Ordner aufzulisten, geben Sie den folgenden Text bei der Eingabeaufforderung ein:

```
listobjects -o session -f myfolder
```

pmrep gibt die folgenden Informationen zurück:

```
session reusable s_sales_by_CUSTID
session non-reusable wf_sales.s_sales_Q3
session non-reusable wf_orders.wl_shirt_orders.s_shirt_orders
.listobjects completed successfully.
```

ListTablesBySess

Gibt eine Liste von Quellen und Targets zurück, die in einer Sitzung verwendet wurden. Wenn Sie Quellen oder Targets auflisten, gibt *pmrep* Quell- oder Target-Instanznamen im Fenster zurück. Verwenden Sie ListTablesBySess in einem Shell-Skript mit anderen *pmrep*-Befehlen. Sie können beispielsweise ein Shell-Skript erstellen, das ListTablesBySess zum Zurückgeben von Quellinstanznamen und Updatesrcprefix zum Aktualisieren des Quelleneigentümer-Namens verwendet.

Wenn Sie ListTablesBySess verwenden, gibt *pmrep* die Quell- und Target-Instanznamen wie sie in den Sitzungseigenschaften erscheinen zurück. Wenn beispielsweise das Mapping ein Mapplet mit einer Quelle enthält, gibt *pmrep* den Quellinstanznamen in folgendem Format zurück:

```
mapplet_name.source_name
```

Der ListTablesBySess-Befehl verwendet die folgende Syntax:

```
listtablesbysess

-f <folder_name>

-s [<qualifying_path>.]<session_name>

-t <object_type_listed> (source or target)
```

In der folgenden Tabelle werden die *pmrep* ListTablesBySess-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-f	folder_name	Erforderlich. Name des Ordners, der die Sitzung enthält.
-s	session_name	Erforderlich. Name der Sitzung mit den Quellen oder Targets. Sie können einen wiederverwendbaren oder nicht wiederverwendbaren Sitzungsnamen eingeben. Sie können jedoch keine Instanz eines wiederverwendbaren Sitzungsnamens eingeben. Um einen nicht wiederverwendbaren Sitzungsnamen in einem Arbeitsablauf einzugeben, geben Sie den Arbeitsablaufnamen und den Sitzungsnamen im Format *workflow_name.session_name* ein.
-t	object_type_listed	Erforderlich. Geben Sie Quelle zum Auflisten von Quellen oder Target zum Auflisten von Targets ein.

Um beispielsweise alle Quellen in einer wiederverwendbaren Sitzung aufzulisten, geben Sie den folgenden Text bei der Eingabeaufforderung ein:

```
listtablesbysess -f myfolder -s s_reus_sess1 -t source
```

pmrep gibt die folgenden Informationen zurück:

```
ITEMS
mapplet1.ORDERS
Shortcut_To_ITEM_ID
listtablesbysess completed successfully.
```

Wenn das Mapping ein Mapplet mit einer Quelle beinhaltet, enthält *pmrep* den Mapplet-Namen mit der Quelle, z. B. mapplet1.ORDERS.

Sie können beispielsweise alle Targets in einer nicht wiederverwendbaren Sitzung in einem Arbeitsablauf auflisten:

```
listtablesbysess -f myfolder -s wf_workkflow1.s_nrsess1 -t target
```

pmrep gibt die folgenden Informationen zurück:

```
target1_inst
ORDERS_BY_CUSTID
Shortcut_To_tgt2_inst
listtablesbysess completed successfully.
```

ListUserConnections

Listet die Informationen für jeden, mit dem Repository verbundenen Benutzer auf.

Der ListUserConnections-Befehl verwendet die folgende Syntax:

```
listuserconnections
```

MassUpdate

Aktualisiert Sitzungseigenschaften für eine Reihe von Sitzungen, die angegebene Bedingungen erfüllen. Sie können alle Sitzungen in einem Ordner oder einer Liste von Sitzungen aktualisieren. Um eine Liste von Sitzungen zu aktualisieren, erstellen Sie eine persistente Eingabedatei. Die Liste kann eine bestimmte Liste von Sitzungen oder Bedingungen wie Namensmuster oder Eigenschaftswert enthalten. Verwenden Sie ExecuteQuery, um eine persistente Eingabedatei zu generieren.

Wenn Sie MassUpdate ausführen, können Sie Informationen wie den Ordnernamen, die Anzahl der Sitzungen, die erfolgreich aktualisiert wurden oder fehlgeschlagen sind, und die Namen der aktualisierten Sitzungen anzeigen. Sie können den Status der Aktualisierung im Befehlszeilenfenster oder in einer vom Befehl generierten Protokolldatei anzeigen. Geben Sie den Namen und Pfad für die Protokolldatei ein, wenn Sie den Befehl ausführen. Standardmäßig wird die Protokolldatei in dem Verzeichnis gespeichert, in dem Sie den Befehl ausführen.

Verwenden Sie MassUpdate zum Aktualisieren einer Sitzungseigenschaft über mehrere Sitzungen, wenn eine PowerCenter Version einen Standardwert ändert.

Hinweis: Abhängige Sitzungseigenschaften können nicht aktualisiert werden.

Bevor Sie die Sitzungen aktualisieren, können Sie MassUpdate auch in einem Testmodus ausführen, um Änderungen anzuzeigen. Ein Beispiel einer Protokolldatei finden Sie auf “Beispiel-Protokolldatei” auf Seite 1203.

Der MassUpdate-Befehl verwendet die folgende Syntax:

```
pmrep massupdate

-t <session_property_type (session_property, session_config_property,
transformation_instance_attribute, session_instance_runtime_option)>

-n <session_property_name>

-v <session_property_value>

[-w <transformation_type>]

{-i <persistent_input_file> | -f <folder_name> }

[-o <condition_operator (equal, unequal, less, greater)>]

[-l <condition_value>]

[-g <update_session_instance_flag>]

[-m <test_mode>]

[-u <output_log_file_name>]
```

In der folgenden Tabelle werden die *pmrep* MassUpdate-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-t	session_property_type	Erforderlich. Zu aktualisierender Sitzungseigenschaftstyp. Es gibt folgende Typen von Sitzungseigenschaften: - session_property - session_config_property - transformation_instance_attribute - session_instance_runtime_option
-n	session_property_name	Erforderlich. Name des zu aktualisierenden Attributs oder der zu aktualisierenden Eigenschaft.
-v	session_property_value	Erforderlich. Wert (gefolgt von einem Semikolon), den Sie der Eigenschaft zuweisen möchten. Verwenden Sie zum Zuweisen eines Werts zur Eigenschaft beispielsweise folgende Syntax: `-v "IgnoreNULLInExpressionComparison=Yes;"` **Hinweis:** Setzen Sie den Sitzungseigenschaftswert in doppelte Anführungszeichen.
-w	transformation_type	Erforderlich, wenn Sie ein Umwandlungsinstanzattribut aktualisieren. Zu aktualisierender Umwandlungstyp. Sie können die folgenden Umwandlungstypen aktualisieren: Aggregat, Joiner, Lookup, Rang, Sortierer, Quelldefinition und Zieldefinition.
-i	persistent_input_file	Erforderlich, wenn Sie die Option -f nicht verwenden. Name der Datei, die die ausgewählte Liste der zu aktualisierenden Sitzungen enthält. Sie können mit dem *pmrep* ExecuteQuery-Befehl eine Abfrage ausführen und diese Datei generieren. MassUpdate gibt einen Fehler zurück, wenn Sie ein Objekt angeben, das keine Sitzung ist. Sie müssen die Option -i oder die Option -f verwenden, aber nicht beide.

Option	Argument	Beschreibung
-f	folder_name	Erforderlich, wenn Sie nicht die Option -i verwenden. Name des Ordners. Verwenden Sie diesen, um alle Sitzungen in einem Ordner zu aktualisieren. Sie müssen die Option -i oder die Option -f verwenden, aber nicht beide.
-o	condition_operator	Erforderlich, wenn Sie condition_value verwenden. Teil der Bedingung, die den Sitzungssatz definiert. Das Attribut einer Sitzung oder Sitzungsinstanz wird aktualisiert, wenn die Bedingung erfüllt ist. Sie können die folgenden Bedingungsoperatoren verwenden, um eine Zeichenfolge zu aktualisieren: gleich oder ungleich. Sie können die folgenden Bedingungsoperatoren verwenden, um eine Ganzzahl zu aktualisieren: gleich, ungleich, kleiner oder größer.
-l	condition_value	Erforderlich, wenn Sie einen Bedingungsoperator verwenden. Teil der Bedingung. Die Bedingung wird wie folgt angezeigt: <session_property_value> <condition operator> <condition_value>
-g	update_session_instance_flag	Erforderlich, wenn Sie die Laufzeitoption einer Sitzungsinstanz aktualisieren. Optional bei folgenden Sitzungseigenschaftstypen: Sitzungseigenschaft, Sitzungskonfigurationsattribut und Umwandlungsinstanzattribut. Aktualisiert Sitzungsinstanzen. Sie können ein Attribut in einer Sitzungsinstanz aktualisieren, wenn die Sitzungsinstanz das Attribut überschreibt.
-m	test_mode	Optional. Führt MassUpdate im Testmodus aus. Zeigen Sie Sitzungen an, auf die sich der Befehl auswirkt, bevor Sie Änderungen vornehmen. Sie können die folgenden Details im Befehlszeilenfenster anzeigen: - Sitzungsname - Sitzungstyp: wiederverwendbar oder nicht wiederverwendbar - Aktueller Wert der Sitzungseigenschaft - Sitzungen, bei denen das Attribut den gleichen Wert hat und auf die der Befehl keine Auswirkung hat.
-u	output_log_file_name	Optional. Name der Protokolldatei, die den Status der Aktualisierung und Basisinformationen zu Sitzungen und Sitzungsinstanzen speichert. Vorherige Attributwerte werden ebenfalls in diese Datei geschrieben. Wenn Sie diese Option nicht verwenden, werden die Details im Befehlszeilenfenster angezeigt.

Der MassUpdate-Befehl gibt die Meldung "massupdate erfolgreich abgeschlossen" oder "Ausführen von massupdate fehlgeschlagen" zurück. Die Aktualisierung kann aus folgenden Gründen fehlschlagen:

- Sie haben keinen für den Attributnamen gültigen Attributwert angegeben.
- Sie haben den korrekten Namen der Sitzungseigenschaft zusammen mit dem falschen Sitzungseigenschafts-Typ angegeben.
- Sie haben die Option -v, die mit einem Semikolon endet, beim Aktualisieren eines Sitzungseigenschaftswert nicht angegeben.
- Sie haben während der Aktualisierung eines Transformationsinstanz-Attributs die Option -w nicht angegeben.

- Sie haben während der Aktualisierung einer Sitzungsinstanz-Laufzeitoption die Option -g nicht angegeben.
- Sie verfügen nicht über die Repository Services-Administratorrolle.

Sitzungseigenschafts-Typen

Wenn Sie MassUpdate ausführen, geben Sie den Sitzungseigenschafts-Typ und den Namen an. Sie legen folgende Sitzungseigenschafts-Typen fest:

- Sitzungseigenschaften
- Sitzungskonfigurationsattribute
- Transformationsinstanzattribute
- Sitzungsinstanz-Laufzeitoptionen

Hinweis: Sie müssen die Sitzungseigenschaft in Anführungszeichen einschließen.

In der folgenden Tabelle werden die aktualisierbaren Sitzungseigenschaften und die Sitzungseigenschafts-Typen aufgelistet:

Sitzungseigenschaft	Sitzungseigenschafts-Typ
$Quellenverbindungswert	session_property
$Target-Verbindungswert	session_property
Zusätzliche gleichzeitige Pipelines für die Erstellung des Lookup-Cache	session_config_property
Größe des Aggregator-Datencaches	transformation_instance_attribute Das Argument transformation_type muss Aggregator sein.
Aggregator-Index - Cache-Größe	transformation_instance_attribute Das Argument transformation_type muss Aggregator sein.
Temporäre Sequenz für Pushdown zulassen	session_property
Temporäre Ansicht für Pushdown zulassen	session_property
Cache-Verzeichnis	transformation_instance_attribute Das Argument transformation_type muss Aggregator, Joiner oder Rang sein.
Cache-LOOKUP()-Funktion	session_config_property
Leistungsdaten erfassen	session_property
Commit-Intervall	session_property
Commit-Typ	session_property
Constraintbasierte Lastreihenfolge	session_config_property
Benutzerdefinierte Eigenschaften	session_config_property
DateTime-Format-String	session_config_property

Sitzungseigenschaft	Sitzungseigenschafts-Typ
Standard-Pufferblockgröße	session_config_property
Diese Aufgabe deaktivieren	session_instance_runtime_option
DTM-Puffergröße	session_property
Hohe Präzision aktivieren	session_property
Prüflast aktivieren	session_property
Übergeordnetes Objekt schlägt fehl, wenn diese Aufgabe nicht ausgeführt wird	session_instance_runtime_option
Übergeordnetes Objekt schlägt fehl, wenn diese Aufgabe fehlschlägt	session_instance_runtime_option
Inkrementelle Aggregation	session_property
Ist aktiviert	session_config_property
Java Klassenpfad	session_property
Joiner-Daten-Cachegröße	transformation_instance_attribute Das Argument transformation_type muss Joiner sein.
Joiner-Index-Cachegröße	transformation_instance_attribute Das Argument transformation_type muss Joiner sein.
Zeilensequenzielle Pufferlänge	session_config_property
Lookup-Cache-Verzeichnisname	transformation_instance_attribute Das Argument transformation_type muss Lookup-Prozedur sein.
Lookup-Daten-Cachegröße	transformation_instance_attribute Das Argument transformation_type muss Lookup-Prozedur sein.
Lookup-Index-Cachegröße	transformation_instance_attribute Das Argument transformation_type muss Lookup-Prozedur sein.
Maximal zulässige Speicherkapazität für automatische Speicherattribute	session_config_property
Maximaler Prozentsatz der zulässigen Gesamtspeicherkapazität für automatische Speicherattribute	session_config_property
Bei Fehler vor oder nach SQL	session_config_property
Bei Befehlsaufgabenfehler vor Sitzung	session_config_property
Bei Fehler in gespeicherter Prozedur	session_config_property

Sitzungseigenschaft	Sitzungseigenschafts-Typ
Ausgabedateiverzeichnis	transformation_instance_attribute Das Argument transformation_type muss Target-Definition sein.
Tracing überschreiben	session_config_property
Name der Parameterdatei	session_property
Zeitstempel für Kompatibilität vor 85	session_config_property
Zuvor erstellter Lookup-Cache	session_config_property
Pushdown-Optimierung	session_property
Rang-Daten-Cachegröße	transformation_instance_attribute Das Argument transformation_type muss Rang sein.
Rang-Index-Cachegröße	transformation_instance_attribute Das Argument transformation_type muss Rang sein.
Wiederherstellungsstrategie	session_property
Ablehnungsdateiverzeichnis	transformation_instance_attribute Das Argument transformation_type muss Target-Definition sein.
Transaktionen bei Fehlern rückgängig machen	session_property
Sitzungsprotokoll speichern nach	session_config_property
Sitzungsprotokolldatei-Verzeichnis	session_property
Erneuter Sitzungsversuch bei Deadlock	session_property
Sitzungs-Sortier-Reihenfolge	session_property Wenn der Integration Service im Unicode-Modus ausgeführt wird, können Sie die Sortierreihenfolge für das Sortieren von Zeichendaten in der Sitzung auswählen. Sie können die folgenden Werte für die Sortierreihenfolge konfigurieren: - 0. BINARY - 2. SPANISH - 3. TRADITIONAL_SPANISH - 4. DANISH - 5. SWEDISH - 6. FINNISH
Sortierer-Cachegröße	transformation_instance_attribute Das Argument transformation_type muss Sortierer sein.
Quelldateiverzeichnis	transformation_instance_attribute Das Argument transformation_type muss Quelldefinition sein.
Stoppen bei Fehlern	session_config_property

Sitzungseigenschaft	Sitzungseigenschafts-Typ
Quellzeilen behandeln als	session_property
Eingabe-Link behandeln als AND	session_instance_runtime_option
Rückwärtskompatible Sitzungsprotokolldatei schreiben	session_property

Regeln und Richtlinien für MassUpdate

Verwenden Sie die folgenden Regeln und Richtlinien, wenn Sie MassUpdate ausführen:

- Wenn der Knoten, auf dem der Repository Service-Prozess ausgeführt wird, über begrenzte Speicherkapazität verfügt, deaktivieren Sie das Repository Agent Caching vor dem Ausführen von MassUpdate oder starten Sie den Repository Service nach dem Ausführen von MassUpdate.
- Sie können wiederverwendbare und nicht wiederverwendbare Sitzungen aktualisieren.
- Sie können nach dem Ausführen von MassUpdate Eigenschaftswerte nicht mehr umkehren.
- Ausgecheckte Sitzungen können nicht aktualisiert werden.
- Sitzungen in eingefrorenen Ordner können nicht aktualisiert werden.

Beispiel-Protokolldatei

Der folgende Text zeigt ein Beispiel einer Protokolldatei, die von*pmrep* MassUpdate generiert wurde:

```
cases_auto,s_test_ff,reusable,0
s_test_ff was successfully checked out.

------------------------------------------------------------------------------
11/10/2008 11:12:55 ** Saving... Repository test_ver_MU, Folder cases_auto
------------------------------------------------------------------------------
Session s_test_ff updated.
Checking-in saved objects...done
------------------------------------------------------------------------------

cases_auto,wf_non_reusable_test_ff.s_test_ff_non_reusable,non-reusable,0
wf_non_reusable_test_ff was successfully checked out.

------------------------------------------------------------------------------
11/10/2008 11:12:57 ** Saving... Repository test_ver_MU, Folder cases_auto
------------------------------------------------------------------------------
Validating the flow semantics of Workflow wf_non_reusable_test_ff...
...flow semantics validation completed with no errors.

Validating tasks of Workflow wf_non_reusable_test_ff...
...Workflow wf_non_reusable_test_ff tasks validation completed with no errors.

Workflow wf_non_reusable_test_ff updated.
Checking-in saved objects...done
------------------------------------------------------------------------------

Massupdate Summary:
Number of reusable sessions that are successfully updated: 1.
Number of non-reusable sessions that are successfully updated: 1.
Number of session instances that are successfully updated: 0.
Number of reusable sessions that fail to be updated: 0.
Number of non-reusable sessions that fail to be updated: 0.
Number of session instances that fail to be updated: 0.
------------------------------------------------------------------------------
```

ModifyFolder

Ändert Ordnereigenschaften. Sie ändern einen Ordner in einem nicht versionsgesteuerten Repository.

Der Befehl gibt "ModifyFolder erfolgreich abgeschlossen" oder "ModifyFolder fehlgeschlagen" zurück. Die Änderung schlägt möglicherweise aus folgenden Gründen fehl:

- Der Ordner existiert nicht.
- Die neue Eigentümer existiert nicht oder gehört nicht zur Gruppe.
- Ein Ordner mit dem neuen Ordnernamen ist bereits vorhanden.

Der ModifyFolder-Befehl verwendet die folgende Syntax:

```
modifyFolder

-n <folder_name>

[-d <folder_description>]

[-o <owner_name>]

[-a <owner_security_domain>]

[-s (shared folder)]

[-p <permissions>]

[-r <new_folder_name>]

[-f <folder_status> (active, frozendeploy, or frozennodeploy)]

[-u <os_profile>]
```

In der folgenden Tabelle werden die *pmrepModifyFolder* -Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-n	folder_name	Erforderlich. Neuer Ordnername.
-d	folder_description	Optional. Beschreibung des Ordners, der im Repository angezeigt wird.
-o	owner_name	Optional. Aktueller Eigentümer des Ordners. Jeder Benutzer im Repository kann Eigentümer des Ordners sein. Standardeigentümer ist der aktuelle Benutzer.
-a	owner_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Eigentümer gehört. Die Standardeinstellung ist "Native".
-s	shared_folder	Optional. Stellt den Ordner zur gemeinsamen Nutzung zur Verfügung.
-p	Berechtigungen	Optional. Zugriffsberechtigungen für den Ordner. Wenn dies ausgelassen wird, verwendet der Repository Service vorhandene Berechtigungen.
-r	new_folder_name	Optional. Neuer Name des Ordners.

Option	Argument	Beschreibung
-f	folder_status	Optional. Ändern Sie den Ordnerstatus auf einen der folgenden Status: - active. Dieser Status ermöglicht Benutzern das Auschecken versionsgesteuerte Objekte im Ordner. - frozendeploy (Eingefroren, Ersetzen bei Bereitstellung zulassen). Dieser Status verhindert, dass Benutzer Objekte im Ordner auschecken. Bei der Bereitstellung im Ordner werden neue Versionen der Objekte erstellt. - frozennodeploy (Eingefroren, Ersetzen bei Bereitstellung nicht zulassen). Dieser Status verhindert, dass Benutzer Objekte im Ordner auschecken. Sie können in diesem Ordner keine Objekte bereitstellen.
-u	os_profile	Optional. Weist dem Ordner ein Betriebssystemprofil zu.

Benachrichtigen

Sendet Benachrichtigungsmeldungen an Benutzer, die mit einem Repository verbunden sind, oder an Benutzer, die mit allen von einem Repository Service verwalteten Repositories verbunden sind.

Der Notify-Befehl verwendet die folgende Syntax:

```
notify

-m <message>
```

In der folgenden Tabelle werden *pmrep* Notify-Option und -Argument beschrieben:

Option	Argument	Beschreibung
-m	message	Erforderlich. Meldung, die gesendet werden soll.

Der Befehl gibt "Notify erfolgreich abgeschlossen" oder "Ausführen von Notify fehlgeschlagen" zurück. Die Benachrichtigung schlägt möglicherweise aus folgenden Gründen fehl:

- Die von Ihnen eingegebene Meldung ist ungültig.
- Die Verbindung zum Repository Service wurde nicht hergestellt.
- Der Repository Service konnte Benutzer nicht benachrichtigen.

ObjectExport

Exportiert Objekte in eine XML-Datei, die in der Datei powrmart.dtd definiert ist. Sie exportieren ein Objekt nach Name. Wenn Sie ein Objekt eingeben, müssen Sie den Namen des Ordners eingeben, der das Objekt enthält. Wenn Sie keine Versionsnummer eingeben, exportieren Sie die neueste Version des Objekts.

Verwenden Sie eine persistente Eingabedatei, um mehrere Objekte anzugeben, die gleichzeitig exportiert werden sollen. Sie können diese Datei mit den *pmrep*-Befehlen ExecuteQuery, Validate oder ListObjectDependencies erstellen. Wenn Sie die persistente Eingabedatei verwenden, benutzen Sie keine anderen Parameter zur Angabe von Objekten.

Wenn Sie ein Mapping exportieren, exportiert PowerCenter standardmäßig das Mapping mit den zugehörigen Instanzen. Wenn Sie abhängige Objekte einschließen möchten, müssen Sie die entsprechenden *pmrep*-Optionen hinzufügen. Optional können Sie wiederverwendbare und nicht wiederverwendbare abhängige Objekte, durch Shortcuts referenzierte Objekte sowie zugehörige Objekte in einer Primärschlüssel-Fremdschlüssel-Beziehung einschließen.

Zum Exportieren von Mapping-Abhängigkeiten müssen Sie die Optionen -b und -r verwenden.

Der ObjectExport-Befehl verwendet die folgende Syntax:

```
objectexport

{{-n <object_name>

 -o <object_type>

 [-t <object_subtype>]

 [-v <version_number>]

 [-f <folder_name>]} |

 -i <persistent_input_file>}

[-m (export pk-fk dependency)]

[-s (export objects referred by shortcut)]

[-b (export non-reusable dependents)]

[-r (export reusable dependents)]

-u <xml_output_file_name>

[-l <log_file_name>]

[-e dbd_separator]
```

In der folgenden Tabelle werden die *pmrep* ObjectExport-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-n	object_name	Erforderlich, wenn Sie nicht die Option -i verwenden. Der Name eines bestimmten Objekts, das exportiert werden soll. Wenn Sie diese Option nicht eingeben, exportiert *pmrep* alle aktuellen oder ausgecheckten Objekte im Ordner. Verwenden Sie die Option -n oder -i, aber nicht beide.
-o	object_type	Objekttyp des Objektnamens. Sie können Quelle, Target, Transformation, Mapping, Mapplet, Sitzung, Worklet, Arbeitsablauf, Scheduler, Sitzungskonfiguration oder Aufgabe festlegen. Bei Verwendung dieser Option kann die Option -i nicht benutzt werden.
-t	object_subtype	Typ der Transformation oder Aufgabe. Dieses Argument wird bei anderen Objekttypen ignoriert. Weitere Informationen zu gültigen Subtypen finden Sie unter "Auflisten von Objekttypen" auf Seite 1192.
-v	version_number	Optional. Exportiert die Version des eingegebenen Objekts.
-f	folder_name	Name des Ordners, der das zu exportierende Objekt enthält. Wenn Sie keinen Objektnamen eingeben, exportiert *pmrep* alle Objekte in diesem Ordner. Bei Verwendung dieser Option kann die Option -i nicht benutzt werden.

Option	Argument	Beschreibung
-i	persistent_input_file	Erforderlich, wenn Sie die Option -n nicht verwenden. Textdateiliste der Objekte, die mit ExecuteQuery, Validate oder ListObjectDependencies generiert wurden. Sie enthält Objektdatensätze mit kodierten IDs. Wenn Sie diesen Parameter verwenden, können Sie die Optionen -n, -o und -f nicht benutzen.
-m	-	Erforderlich zum Exportieren abhängiger Objekte. Exportiert Primärschlüssel-Tabellendefinitionen beim Exportieren von Quellen und Targets mit Fremdschlüsseln.
-s	-	Erforderlich zum Exportieren abhängiger Objekte. Exportiert das ursprüngliche, vom Shortcut referenzierte Objekt.
-b	-	Erforderlich zum Exportieren abhängiger Objekte. Exportiert vom Objekt benutzte, nicht wiederverwendbare Objekte.
-r	-	Erforderlich zum Exportieren abhängiger Objekte. Exportiert vom Objekt benutzte, wiederverwendbare Objekte.
-u	xml_output_file_name	Erforderlich. Name der XML-Datei, die die Objektinformationen enthalten soll.
-l	log_file_name	Optional. Protokolldatei, die alle Exportschritte aufzeichnet. Wenn Sie diese Option auslassen, werden im Fenster Statusmeldungen ausgegeben.
-e	dbd_separator	Optional. Wenn bei einer ODBC-Quelle ein Punkt (.) im Namen vorkommt, legen Sie beim Definieren des Quellobjekts ein anderes Trennzeichen fest. Beispiel: Definieren Sie statt database_name.source_name das Quellobjekt als database_name\source_name, und legen Sie als dbd_separator den umgekehrten Schrägstrich (\) fest.

Beispiele

Das folgende Beispiel exportiert ein Mapping mit dem Namen "Map", das in folder1 gespeichert ist, in eine Datei mit dem Namen map.xml:

```
objectexport  -n map -o mapping -f folder1 -u map.xml
```

Das folgende Beispiel exportiert die Objekte in einer persistenten Eingabedatei mit dem Namen persistent_input.xml in eine Datei mit dem Namen map.xml:

```
objectexport  -i persistent_input.txt -u map.xml
```

Hinweis: Wenn Sie eine manuell erstellte persistente Eingabedatei verwenden, wird folgende Meldung angezeigt, da Sie als kodierte ID "none" eingegeben haben: IDs sind ungültig. Versuch mit Namen für [none,folder1,map,mapping,none,1].

ObjectImport

Importiert Objekte aus einer XML-Datei. Dieser Befehl erfordert eine Steuerdatei, um die zu importierenden Objekte und die Konfliktlösungsmethode festzulegen. Die Steuerdatei ist eine XML-Datei, die durch die Datei impcntl.dtd definiert wird.

Der ObjectImport-Befehl verwendet die folgende Syntax:

```
objectimport

-i <input_xml_file_name>

-c <control_file_name>

[-l <log_file_name>]

[-p (retain persistent value)]
```

In der folgenden Tabelle werden die *pmrep* ObjectImport-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-i	input_XML_file_name	Erforderlich. Name der zu importierenden XML-Datei.
-c	control_file_name	Erforderlich. Name der Steuerdatei, die Importoptionen definiert.
-l	log_file_name	Optional. Protokolldatei, die alle Exportschritte aufzeichnet. Wenn Sie diese Option auslassen, werden im Fenster Statusmeldungen ausgegeben.
-p	-	Optional. Behält persistente Werte für Mapping-Variablen bei.

Hinweis: Der ObjectImport-Befehl erstellt keinen Ordner, wenn der eingegebene Ordnername nicht im Repository existiert.

PurgeVersion

Bereinigt Objektversionen von der Repository-Datenbank. Sie können Versionen gelöschter Objekte und aktiver Objekte bereinigen. Ein Objekt ist ein gelöschtes Objekt, wenn die neueste Version eingecheckt ist und den Gelöscht-Versionsstatus aufweist. Andere Objekte sind aktive Objekte.

Wenn Sie Versionen gelöschter Objekte bereinigen, werden alle Versionen bereinigt. Die gelöschten Objekte müssen eingecheckt werden. Sie können Versionen für alle gelöschten Objekte bereinigen oder für Objekte, die vor einem angegebenen Endzeitpunkt gelöscht wurden. Sie können die Endzeit als Datum und Uhrzeit, nur als Datum oder als Anzahl von Tagen vor dem aktuellen Datum festlegen.

Wenn Sie Versionen aktiver Objekte bereinigen, können Sie Bereinigungskriterien angeben. Sie können die Anzahl der beizubehaltenden Versionen festlegen und frühere Version bereinigen oder Sie bereinigen Versionen, die älter sind als ein festgelegter Cutoff-Zeitpunkt. Sie können weder eine ausgecheckte Version noch die aktuellste eingecheckte Version bereinigen.

Wenn Sie Versionen eines Verbundobjekts bereinigen, achten Sie darauf, welche Versionen der abhängigen Objekte bereinigt werden.

Mit der Option -k können Sie die Objekte, die nicht bereinigt werden, sowie den Grund dafür anzeigen, warum Objektversionen nicht bereinigt werden. Sie verfügen beispielsweise nicht über die Berechtigung zum Bereinigen einer Objektversion. Sie können Objektversionen, die zu einer Bereitstellungsgruppe gehören, nicht bereinigen.

Der PurgeVersion-Befehl verwendet die folgende Syntax:

```
purgeversion
{-d <all | time_date | num_day> |
{-n <last_n_versions_to_keep> |
 -t <time_date | num_day>}}
```

```
[-f <folder_name>]
[-q <query_name>]
[-o <output_file_name>]
[-p (preview purged objects only)]
[-b (verbose)]
[-c (check deployment group reference)]
[-s dbd_separator]
[-k (log objects not purged)]
```

In der folgenden Tabelle werden die *pmrep* PurgeVersion-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-d	alle time_date num_day	Erforderlich, wenn Sie weder -n noch -t verwenden. Bereinigt alle Versionen der eingecheckten gelöschten Objekte. Sie können `all` für alle gelöschten Objekte festlegen oder eine Endzeit angeben, um alle Versionen von Objekten zu bereinigen, die vor diesem Zeitpunkt gelöscht wurden. Legen Sie den Endzeitpunkt im Format MM/DD/YYYY HH24:MI:SS, im Format MM/DD/YYYY oder als Anzahl an Tagen vor dem aktuellen Datum fest. Wenn Sie eine Anzahl an Tagen angeben, muss der Wert eine Ganzzahl größer 0 sein.
-n	last_n_versions_to_keep	Erforderlich, wenn Sie -d oder -t nicht verwenden. Anzahl der neuesten eingecheckten Objektversionen, die für ein aktives Objekt beibehalten werden sollen. Der Wert muss eine Ganzzahl größer 0 sein. Geben Sie beispielsweise 6 ein, um alle Versionen außer den letzten sechs eingecheckten Versionen zu bereinigen. Wenn das Objekt ausgecheckt ist, wird auch die ausgecheckte Version beibehalten. **Hinweis:** Nachdem Sie Objektversionen bereinigt haben, können Sie diese nicht mehr abrufen. Um sicherzustellen, dass Sie zu früheren Versionen zurückkehren können, sollten Sie nicht alle Versionen eines Objekts bereinigen.
-t	purge_cutoff_time	Erforderlich, wenn Sie -d oder -n nicht verwenden. Cutoff-Zeitpunkt für das Bereinigen von Objektversionen von aktiven Objekten. Bereinigt Versionen, die vor dem Cutoff-Zeitpunkt eingecheckt wurden. Sie können den Cutoff-Zeitpunkt zum Bereinigen im Format MM/DD/YYYY HH24:MI:SS, im Format MM/DD/YYYY oder als Anzahl an Tagen vor dem aktuellen Datum festlegen. Wenn Sie eine Anzahl an Tagen angeben, muss der Wert eine Ganzzahl größer 0 sein. Wenn Sie die Option -t verwenden, behalten Sie die neueste eingecheckte Version, auch wenn diese nach dem Cutoff-Zeitpunkt zum Bereinigen eingecheckt wurde.
-f	folder_name	Optional. Ordner, auf dem Objektversionen bereinigt werden. Wenn Sie keinen Ordner festlegen, bereinigen Sie Objektversionen auf allen Ordnern im Repository.
-q	query_name	Optional. Abfrage zum Bereinigen von Objektversionen von einem bestimmten Abfrageergebnissatz. **Hinweis:** Wenn Sie die Option -d verwenden, bereinigen Sie alle Versionen der gelöschten Objekte. Um die neueren Versionen der gelöschten Objekte beizubehalten und ältere Versionen zu bereinigen, können Sie eine Abfrage definieren, die die gelöschten Objekte zurückgibt, und dann die Option -q zusammen mit -n, -t oder beidem verwenden.
-o	outputfile_name	Optional. Ausgabedatei zum Speichern von Informationen zu bereinigten Objektversionen.

Option	Argument	Beschreibung
-p	-	Optional. Zeigt eine Vorschau des PurgeVersion-Befehls an. *pmrep* zeigt die Bereinigungsergebnisse an, ohne die Objektversionen tatsächlich zu bereinigen.
-b	-	Optional. Zeigt oder speichert Bereinigungsinformationen im Verbose-Modus. Verbose-Modus bietet ausführliche Informationen zu Objektversionen, einschließlich Repository-Name, Ordner-Name, Versionsnummer und Status. Sie können die Option -b mit -o und -p verwenden.
-c	-	Optional. Prüft Bereitstellungsgruppen im Repository auf Verweise zu den Objektversionen, die in einer Bereinigungsvorschau zurückgegeben werden. Wenn in einer Bereinigungsvorschau eine Objektversion in einer Bereitstellungsgruppe enthalten ist, zeigt *pmrep* eine Warnung an. Wenn Sie die Option -c mit der Option -p verwenden, listet der Befehl Objekte auf, die bereinigt werden. Anschließend werden die Objektversionen aufgelistet, die in Bereitstellungsgruppen enthalten sind. Wenn Sie die Option -c ohne die Option -p verwenden, bereinigt der Befehl keine Objektversionen, die zu Bereitstellungsgruppen gehören. **Hinweis:** Die Option -c kann sich negativ auf die Leistung auswirken.
-s	dbd_separator	Optional. Wenn bei einer ODBC-Quelle ein Punkt (.) im Namen vorkommt, legen Sie beim Definieren des Quellobjekts ein anderes Trennzeichen fest. Beispiel: Definieren Sie statt database_name.source_name das Quellobjekt als database_name \source_name, und legen Sie als dbd_separator den umgekehrten Schrägstrich (\) fest.
-k	-	Optional. Listet alle Objektnamen und Versionen auf, die nicht bereinigt werden, obwohl sie den Bereinigungskriterien entsprechen. Die Option -k listet auch den Grund dafür auf, warum die Objektversionen nicht bereinigt werden. Beispiel: Eine Objektversion wird nicht bereinigt, wenn Sie nicht über ausreichende Berechtigungen zum Löschen des Objekts verfügen. **Hinweis:** Eine Objektversion wird nicht bereinigt, wenn sie zu einer Bereitstellungsgruppe gehört. Wenn ein Objekt zu mehr als einer Bereitstellungsgruppe gehört, wird als Ursache für die Nichtbereinigung des Objekts die erste Bereitstellungsgruppe angeführt.

Beispiele

Das folgende Beispiel bereinigt sämtliche Versionen aller gelöschten Objekte im Repository:

```
pmrep purgeversion -d all
```

Hinweis: Eine optimale Leistung erreichen Sie, indem Sie auf Ordnerebene bereinigen oder Bereinigungskriterien verwenden, die die Anzahl der gelöschten Objektversionen reduzieren. Vermeiden Sie das Bereinigen aller gelöschten Objekte oder aller älteren Versionen auf Repository-Ebene.

Das folgende Beispiel bereinigt alle Objekte im Ordner folder1, mit Ausnahme der neuesten eingescheckten Objektversion:

```
pmrep purgeversion -n 1 -f folder1
```

Das folgende Beispiel zeigt eine Bereinigungsvorschau aller Objektversionen an, die vor Mittag des 5. Januar 2005 eingescheckt wurden, und gibt die Ergebnisse in der Datei mit dem Namen purge_output.txt aus:

```
pmrep purgeversion -t '01/05/2005 12:00:00' -o purge_output.txt -p
```

Register

Registriert ein lokales Repository bei einem verbundenen globalen Repository. Sie müssen eine Verbindung zum globalen Repository herstellen, bevor Sie das lokale Repository registrieren.

Außerdem müssen Sie den Repository Service für das lokale Repository im exklusiven Modus ausführen. Sie können die Ausführung des Repository Service im exklusiven Modus im Administrator-Tool konfigurieren oder den Befehl *infacmd* UpdateRepositoryService verwenden.

Der Befehl gibt "Register erfolgreich abgeschlossen" oder "Ausführen von Register fehlgeschlagen" zurück. Die Registrierung schlägt möglicherweise aus folgenden Gründen fehl:

- Die Verbindung zum Repository Service wurde nicht hergestellt.
- Das lokale Repository wird nicht im exklusiven Modus ausgeführt.
- Der Repository Service konnte Informationen zum globalen Repository nicht initialisieren.
- Der Repository Service konnte das lokale Repository nicht bei dem globalen Repository registrieren.

Der Register-Befehl verwendet die folgende Syntax:

```
register
-r <local_repository_name>
-n <local_repository_user_name>
[-s <local_repository_user_security_domain>]
[-x <local_repository_password> |
-X <local_repository_password_environment_variable>]
[-d <local_repository_domain_name> |
{-h <local_repository_portal_host_name>
-o <local_repository_portal_port_number>}] (if local repository is in a different domain)
```

In der folgenden Tabelle werden die *pmrep* Register-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-r	local_repository_name	Erforderlich. Name des zu registrierenden lokalen Repository.
-n	local_repository_user_name	Erforderlich. Lokaler Benutzernamen.
-s	local_repository_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Die Standardeinstellung ist "Native".
-x	local_repository_password	Optional. Anmelde-Passwort für das lokale Target-Repository. Verwenden Sie die Option -x oder -X, aber nicht beide. Wenn Sie weder die Option -x noch -X verwenden, werden Sie von *pmrep* aufgefordert, das Passwort einzugeben.
-X	repository_password_environment_variable	Optional. Anmelde-Passwort-Umgebungsvariable für das lokale Target-Repository. Verwenden Sie die Option -x oder -X, aber nicht beide. Wenn Sie weder die Option -x noch -X verwenden, werden Sie von *pmrep* aufgefordert, das Passwort einzugeben.

Option	Argument	Beschreibung
-d	local_repository_domain_name	Erforderlich, wenn sich das lokale Repository in einer anderen Domäne befindet und Sie nicht die Optionen -h und -o verwenden. Name der Informatica-Domäne für das Repository.
-h	local_repository_portal_host_name	Erforderlich, wenn sich das lokale Repository in einer anderen Domäne befindet und Sie nicht die Option -d verwenden. Computername der Domäne, auf der das lokale Repository gespeichert ist. Wenn Sie diese Option verwenden, müssen Sie auch die Option -o benutzen.
-o	local_repository_portal_port_number	Erforderlich, wenn sich das lokale Repository in einer anderen Domäne befindet und Sie nicht die Option -d verwenden. Portnummer der Domäne, auf der das lokale Repository gespeichert ist. Wenn Sie diese Option verwenden, müssen Sie auch die Option -h verwenden.

RegisterPlugin

Registriert ein externes Plug-In in einem Repository. Das Registrieren eines Plug-Ins fügt dessen Funktionalität dem Repository hinzu. Verwenden Sie den RegisterPlugin-Befehl zum Aktualisieren vorhandener Plug-Ins.

Wenn Sie diesen Befehl verwenden, muss der Repository Service im exklusiven Modus ausgeführt werden. Sie können die Ausführung des Repository Service im exklusiven Modus im Administrator-Tool konfigurieren oder den Befehl *infacmd* UpdateRepositoryService verwenden.

Der RegisterPlugin-Befehl verwendet die folgende Syntax:

```
registerplugin

-i <input_registration_file_name_or_path>

[-e (update plug-in)]

[-l <NIS_login>

  {-w <NIS_password> |

  -W <NIS_password_environment_variable>}

  [-k (CRC check on security library)]]

[-N (is native plug-in)]
```

In der folgenden Tabelle werden die *pmrep* RegisterPlugin-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-i	input_registration_file_name_or_path	Erforderlich. Name oder Pfad der Registrierungsdatei für das Plug-In.
-e	-	Optional. Aktualisieren Sie ein vorhandenes Plug-In. Nicht anwendbar bei Authentifizierungsmodulen.

Option	Argument	Beschreibung
-l	NIS login	Optional. Registriert Sicherheitsmodul-Komponenten. Stellen Sie die NIS-Anmeldung des Benutzers zur Verfügung, der ein externes Sicherheitsmodul registriert. Wenn das Plug-In ein Authentifizierungsmodul enthält, müssen Sie den externen Anmeldenamen angeben, andernfalls schlägt die Registrierung fehl. Diese Anmeldung wird als Administrator-Benutzername im Repository verwendet. Verwenden Sie diese Option nicht für andere Plug-Ins.
-w	NIS password	Optional. Verwenden Sie dies zum Registrieren von Authentifizierungsmodul-Komponenten. Passwort für externes Verzeichnis des Benutzers, der das Modul registriert. Wenn das Plug-In ein Authentifizierungsmodul enthält, müssen Sie das Benutzerpasswort des externen Verzeichnisses angeben, andernfalls schlägt die Registrierung fehl. Verwenden Sie diese Option nicht für andere Plug-Ins. Verwenden Sie die Option -w oder -W, aber nicht beide. Wenn Sie kein Passwort oder keine Passwort-Umgebungsvariable angeben, werden Sie von *pmrep* aufgefordert, das Passwort einzugeben.
-W	NIS_password_environment_variable	Optional. Verwenden Sie dies zum Registrieren von Authentifizierungsmodul-Komponenten. Passwort-Umgebungsvariable für externes Verzeichnis des Benutzers, der das Modul registriert. Wenn das Plug-In ein Authentifizierungsmodul enthält, müssen Sie das Benutzerpasswort des externen Verzeichnisses angeben, andernfalls schlägt die Registrierung fehl. Verwenden Sie diese Option nicht für andere Plug-Ins. Verwenden Sie die Option -w oder -W, aber nicht beide. Wenn Sie kein Passwort oder keine Passwort-Umgebungsvariable angeben, werden Sie von *pmrep* aufgefordert, das Passwort einzugeben.
-k	-	Optional. Speichert das CRC der Plug-In-Bibliothek im Repository. Wenn der Repository Service das Modul lädt, führt dieses eine CRC-Prüfung in der Bibliothek aus.
-N	-	Registriert ein Plug-In. Erforderlich, wenn die folgenden Bedingungen gegeben sind: - Sie führen ein PowerCenter-Upgrade aus. - Das PowerCenter-Upgrade hat keine neue Repository-Version. - Das Plug-In enthält aktualisierte Funktionen. - Das Plug-In wird standardmäßig bei einer neuen PowerCenter-Installation registriert. Weitere Informationen zu Plug-Ins, die beim Upgrade registriert werden müssen, finden Sie im *PowerCenter Release-Handbuch*.

Registrieren eines Sicherheitsmoduls

Wenn Sie Benutzer und Passwörter für ein Repository mit einem externen Verzeichnisdienst verwalten möchten, müssen Sie das Sicherheitsmodul bei dem Repository registrieren. Verwenden Sie den Registerplugin-Befehl zum Registrieren des Sicherheits-Plug-Ins.

Beispiel

Sie verwalten PowerCenter für eine Organisation, die ein zentralisiertes LDAP NIS zur Benutzerauthentifizierung hat. Bei der Ausführung eines PowerCenter-Upgrades entscheiden Sie sich, LDAP für die Benutzerauthentifizierung zu verwenden. Das Upgrade installiert das LDAP-Sicherheitsmodul im Repository-Sicherheitsordner. Nachdem der Connect-Befehl eine Verbindung zum Repository hergestellt hat, führt der Administrator den *pmrep*-Befehl zum Registrieren des neuen externen Moduls bei dem Repository aus:

```
pmrep registerplugin -i security/ldap_authen.xml -l adminuser -w admnpass
```

Die Optionen -l für den Anmeldenamen und -w für das Anmelde-Passwort enthalten die gültigen NIS-Anmeldeinformationen für den Benutzer, der den *pmrep*-Befehl ausführt. Nach der Registrierung müssen Sie diesen Anmeldenamen und das Passwort für den Zugriff auf das Repository verwenden.

Hinweis: Der Anmeldename und das Passwort müssen im externen Verzeichnis Gültigkeit haben, andernfalls kann der Administrator nicht mit LDAP auf das Repository zugreifen.

Die Option -i enthält den XML-Dateinamen, der das Sicherheitsmodul angibt.

Wiederherstellen

Stellt eine Repository-Backup-Datei in einer Datenbank wieder her. Die Target-Datenbank muss leer sein.

Der *pmrep* Restore-Befehl verwendet die folgende Syntax:

```
restore

-u <domain_user_name>

[-s <domain_user_security_domain>]

[-p <domain_password> |

 -P <domain_password_environment_variable>]

-i <input_file_name>

[-g (create global repository)]

[-y (enable object versioning)]

[-b (skip workflow and session logs)]

[-j (skip deployment group history)]

[-q (skip MX data)]

[-f (skip task statistics)]

[-a (as new repository)]

[-e (exit if domain name in the binary file is different from current domain name)]
```

In der folgenden Tabelle werden die *pmrep* Restore-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-u	domain_user_name	Erforderlich. Benutzername.
-s	domain_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Standardwert ist "Native".
-p	domain_password	Optional. Passwort. Sie können die Option -p oder -P verwenden, aber nicht beide. Wenn Sie weder die Option -p noch -P verwenden, werden Sie von *pmrep* aufgefordert, das Passwort einzugeben.
-P	domain_password_ environment_variable	Optional. Passwort-Umgebungsvariable. Sie können die Option -p oder -P verwenden, aber nicht beide. Wenn Sie weder die Option -p noch -P verwenden, werden Sie von *pmrep* aufgefordert, das Passwort einzugeben.
-i	input_file_name	Erforderlich. Name der Repository-Backup-Datei. Verwenden Sie einen lokalen Dateinamen und Pfad des Repository Service.
-g	-	Optional. Stuft das Repository zu einem globalen Repository hoch.
-y	-	Optional. Ermöglicht Objektversionierung für das Repository.
-b	-	Optional. Überspringt beim Wiederherstellen Tabellen, die sich auf Arbeitsablauf und Sitzungsprotokolle beziehen.
-j	-	Optional. Überspringt beim Wiederherstellen die Bereitstellungsgruppen-Historie.
-q	-	Optional. Überspringt beim Wiederherstellen Tabellen, die sich auf MX-Daten beziehen.
-f	-	Optional. Überspringt beim Wiederherstellen Aufgabenstatistiken.
-a	-	Optional. Erstellt neue interne Ordner-IDs für Ordner im wiederhergestellten Repository. Dies ermöglicht Ihnen das Kopieren von Ordnern und Bereitstellungsgruppen zwischen dem ursprünglichen Repository und dem wiederhergestellten Repository. Wenn Sie nicht -a verwenden, können Sie keine Ordner und Bereitstellungsgruppen zwischen dem ursprünglichen und dem wiederhergestellten Repository kopieren.
-e	-	Optional. Abbruch, wenn der Domänenname in der Binärdatei vom aktuellen Domänennamen abweicht.

Beispiel

Das folgende Beispiel stellt ein Repository als versionsgesteuertes Repository wieder her und gibt den Benutzernamen und das Passwort des Administrators an, um die Registrierung des LDAP-Sicherheitsmoduls beizubehalten:

```
restore -u administrator -p password -i repository1_backup.rep -y
```

RollbackDeployment

Führt ein Rollback für eine Bereitstellung aus, um bereitgestellte Versionen von Objekten aus dem Target-Repository zu löschen. Verwenden Sie diesen Befehl zum Rollback für alle Objekte in einer Bereitstellungsgruppe, die Sie zu einem bestimmten Zeitpunkt (Datum und Uhrzeit) bereitgestellt haben.

Ein Rollback kann nicht nur für einen Teil der Bereitstellung durchgeführt werden. Um ein Rollback auszuführen, müssen Sie eine Verbindung zum Target-Repository herstellen. Sie können kein Rollback einer Bereitstellung von einem nicht versionsgesteuerten Repository ausführen.

Um ein Rollback zu initiieren, müssen Sie die aktuelle Version jedes Objekts für das Rollback verwenden.

Der RollbackDeployment-Befehl verwendet die folgende Syntax:

```
pmrep rollbackdeployment -p <deployment_group_name> -t <nth_latest_deploy_run> -r
<repository_name> -v <nth_latest_version_of_deployment_group>
```

In der folgenden Tabelle werden die *pmrep*-RollbackDeployment-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-p	deployment_group_name	Erforderlich. Name der Bereitstellungsgruppe, für die ein Rollback ausgeführt werden soll.
-t	nth_latest_deploy_run	Erforderlich. Version der Bereitstellung, für die ein Rollback ausgeführt werden soll.
-r	repository_name	Optional. Name des Quellen-Repositorys, aus dem Sie die Bereitstellungsgruppe bereitstellen.
-v	nth_latest_version_of_deployment_group	Optional. Version der Bereitstellungsgruppe, für die ein Rollback ausgeführt werden soll.

Beispiel

Sie haben eine Bereitstellung mit fünf Versionen und möchten ein Rollback für die letzten zwei Versionen durchführen. Dazu müssen Sie zuerst ein Rollback der neuesten Bereitstellung ausführen. Geben Sie den folgenden Text bei der Eingabeaufforderung ein, um ein einzelnes Rollback auszuführen und die letzte Bereitstellung zu bereinigen:

```
rollbackdeployment -p Deploy_sales -t 1
```

Geben Sie anschließend folgenden Text ein, um ein Rollback der vorletzten Bereitstellung durchzuführen:

```
rollbackdeployment -p Deploy_sales -t 2
```

Ausführen

Öffnet eine Skriptdatei mit mehreren *pmrep*-Befehlen, liest die einzelnen Befehle und führt diese aus. Wenn die Skript-Datei mit UTF-8 kodiert ist, müssen Sie die Option -u verwenden und die Repository-Codepage muss UTF-8-kodiert sein. Wenn Sie eine mit UTF-8 kodierte Skriptdatei ausführen, die den Connect-Befehl für ein Repository beinhaltet, das keine UTF-8-Codepage aufweist, schlägt der Run-Befehl fehl.

Wenn die Skriptdatei nicht mit UTF-8 kodiert ist, lassen Sie die Option -u aus. Wenn Sie die Option -o und die Option -u verwenden, generiert *pmrep* die Ausgabedatei in UTF-8. Wenn Sie die Option -o verwenden und die

Option -u auslassen, generiert *pmrep* die Ausgabedatei basierend auf dem Systemgebietsschema des Computers, auf dem Sie *pmrep* ausführen.

Der Befehl gibt "Run erfolgreich abgeschlossen" oder "Run fehlgeschlagen" aus. Die Ausführung schlägt möglicherweise fehl, wenn der Repository Service die Skriptdatei oder Ausgabedatei nicht öffnen kann.

Der Run-Befehl verwendet die folgende Syntax:

```
run

-f <script_file_name>

[-o <output_file_name>]

[-e (echo commands)]

[-s (stop at first error)]

[-u (UTF-8 encoded script file and output file)]
```

In der folgenden Tabelle werden die *pmrep* Run-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-f	script file name	Erforderlich. Name der Skriptdatei
-o	Ausgabedateiname	Optional. Name der Ausgabedatei. Diese Option schreibt alle Meldungen, die von den Befehlen in der Skriptdatei generiert wurden, in die Ausgabedatei. Wenn Sie die Option -u und die Option -o verwenden, generiert *pmrep* eine mit UTF-8 kodierte Ausgabedatei. Wenn Sie die Option -o ohne die Option -u verwenden, kodiert *pmrep* die Ausgabedatei basierend auf dem Systemgebietsschema des Computers, der *pmrep* ausführt.
-e	-	Optional. Befehle werden im Skript wiedergegeben.
-s	-	Optional. Stoppt die Skriptausführung nach dem ersten Fehler.
-u	-	Optional. Kodiert die Ausgabedatei im UTF-8-Format. Wenn Sie die Option -u und die Option -o verwenden, kodiert *pmrep* auch die Ausgabedatei im UTF-8-Format. Verwenden Sie diese Option nur, wenn die Repository-Codepage UTF-8-kodiert ist.

ShowConnectionInfo

Gibt den Repository-Namen und Benutzerinformationen für die aktuelle Verbindung zurück.

Verwenden Sie den ShowConnectionInfo-Befehl im interaktiven Modus. Wenn Sie eine Verbindung zu einem Repository im interaktiven Modus herstellen, speichert *pmrep* die Verbindungsinformationen bis Sie das Repository beenden oder eine Verbindung zu einem anderen Repository herstellen.

Wenn Sie den ShowConnectionInfo-Befehl im Befehlszeilenmodus verwenden, wird eine Meldung angezeigt, dass der Befehl nicht ausgeführt werden konnte. *pmrep* behält keine Verbindungsinformationen im Befehlszeilenmodus bei. Der ShowConnectionInfo-Befehl stellt keine Verbindung zum Repository her.

Der ShowConnectionInfo-Befehl verwendet die folgende Syntax:

```
showconnectioninfo
```

Er gibt Informationen zurück, die wie folgt aussehen können:

```
Connected to Repository MyRepository in MyDomain as user MyUserName
```

SwitchConnection

Ändert den Namen einer vorhandenen Verbindung. Wenn Sie SwitchConnection verwenden, ersetzt der Repository Service die relationalen Datenbankverbindungen für alle Sitzungen, die die Verbindung an einem der folgenden Speicherorte verwenden:

- Quellverbindung
- Target-Verbindung
- Verbindungsinformations-Eigenschaft in Lookup-Transformationen
- Verbindungsinformations-Eigenschaft in Transformationen einer gespeicherten Prozedur
- $Quellenverbindungswert-Sitzungseigenschaft
- $Target-Verbindungswert-Sitzungseigenschaft

Wenn das Repository sowohl relationale Verbindungen als auch Anwendungsverbindungen mit dem gleichen Namen enthält und Sie den Verbindungstyp als relational in *allen* Speicherorten im Repository angeben, ersetzt der Repository Service die relationale Verbindung.

Beispiel: Sie haben eine relationale und eine Anwendungsquelle, beide mit der Bezeichnung ITEMS. In einer Sitzung haben Sie einer relationalen Quellverbindung den Namen ITEMS statt Relational:ITEMS gegeben. Wenn Sie SwitchConnection zum Ersetzen der relationale Verbindung ITEMS durch eine andere relationale Verbindung verwenden, ersetzt *pmrep* keine relationale Verbindung im Repository, weil es keinen Verbindungstyp für die Quellverbindung mit der Bezeichnung ITEMS bestimmen kann.

Der SwitchConnection-Befehl verwendet die folgende Syntax:

```
switchconnection

-o <old_connection_name>

-n <new_connection_name>
```

In der folgenden Tabelle werden die *pmrep* SwitchConnection-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-o	old_connection_name	Erforderlich. Name der zu ändernden Verbindung.
-n	new_connection_name	Erforderlich. Name der neuen Verbindung.

TruncateLog

Löscht Details aus dem Repository. Sie können alle Protokolle oder Protokolle für einen Ordner oder einen Arbeitsablauf löschen. Sie können auch ein Datum eingeben und alle Protokolle löschen, die älter sind.

Der Befehl gibt eine Meldung mit dem Hinweis zurück, dass TruncateLog erfolgreich abgeschlossen wurde oder dass TruncateLog fehlgeschlagen ist. Der Kürzungsvorgang kann aus folgenden Gründen fehlschlagen:

- Der Ordnername ist ungültig.
- Der Arbeitsablauf ist im angegebenen Ordner nicht vorhanden.
- Sie haben zwar einen Arbeitsablauf angegeben, aber keinen Ordnernamen.

Der TruncateLog-Befehl verwendet die folgende Syntax:

```
truncatelog

-t <logs_truncated (all or up to end time in MM/DD/YYYY HH24:MI:SS format or as number
of days before current date)>

[-f <folder_name>]

[-w <workflow_name>]
```

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

Option	Argument	Beschreibung
-t	logs_truncated	Erforderlich. Verwenden Sie „all“ zum Löschen aller Protokolle oder geben Sie einen Endzeitpunkt ein. *pmrep* löscht alle Protokolle, die nach dem Endzeitpunkt liegen. Sie können den Endzeitpunkt im Format MM/DD/YYYY HH24:MI:SS eingeben. Es ist aber auch möglich, die Anzahl der Tage vor dem aktuellen Datum anzugeben. Wenn Sie die Anzahl der Tage angeben, muss der Endzeitpunkt eine Ganzzahl größer als 0 sein.
-f	folder_name	Optional. Löscht mit dem Ordner verbundene Protokolle. Wenn Sie weder den Ordnernamen noch den Arbeitsablaufnamen angeben, löscht *pmrep* alle Protokolle aus dem Repository.
-w	workflow_name	Optional. Löscht mit dem Arbeitsablauf verbundene Protokolle. Der Repository-Dienst löscht alle Protokolle aus dem Repository, wenn Sie nicht sowohl den Ordnernamen als auch den Arbeitsablaufnamen angeben. Wenn Sie sowohl den Ordnernamen als auch den Arbeitsablaufnamen angeben, löscht der Repository-Dienst mit dem Arbeitsablauf verbundene Protokolle. Wenn Sie den Arbeitsablaufnamen eingeben, müssen Sie auch den Ordnernamen bereitstellen.

UndoCheckout

Macht den Checkout eines Objekts rückgängig. Wenn Sie einen Checkout rückgängig machen, löst das Repository die Schreibprioritätssperre für das Objekt und kehrt zur zuletzt eingecheckten Version des Objekts zurück. Wenn Sie das Objekt wieder ändern möchten , müssen Sie es auschecken.

Der UndoCheckout-Befehl verwendet die folgende Syntax:

```
undocheckout

-o <object_type>

[-t <object_subtype>]

-n <object_name>

-f <folder_name>

[-s dbd_separator]
```

In der folgenden Tabelle werden die *pmrep* UndoCheckout-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-o	object_type	Erforderlich. Typ des Objekts. Sie können Quelle und Target, Transformation, Mapping, Sitzung, Worklet, Arbeitsablauf, Scheduler, Sitzungskonfiguration, Aufgabe, Cube und Größenordnung festlegen.
-t	object_subtype	Optional. Typ der Transformation oder Aufgabe. Ignoriert bei anderen Objekttypen. Weitere Informationen zu gültigen Subtypen finden Sie unter "Auflisten von Objekttypen" auf Seite 1192.
-n	object_name	Erforderlich. Name des ausgecheckten Objekts.
-f	folder_name	Erforderlich. Name des Ordners, der das Objekt enthält.
-s	dbd_separator	Optional. Wenn bei einer ODBC-Quelle ein Punkt (.) im Namen vorkommt, legen Sie beim Definieren des Quellobjekts ein anderes Trennzeichen fest. Beispiel: Definieren Sie statt database_name.source_name das Quellobjekt als database_name\source_name, und legen Sie als dbd_separator den umgekehrten Schrägstrich (\) fest.

Unregister

Hebt die Registrierung eines lokalen Repository in einem verbundenen globalen Repository auf.

Um diesen Befehl zu verwenden, müssen Sie den Repository Service für das lokale Repository im exklusiven Modus ausführen. Sie können die Ausführung des Repository Service im exklusiven Modus im Administrator-Tool konfigurieren oder den Befehl *infacmd* UpdateRepositoryService verwenden.

Der Befehl gibt die Meldung zurück, dass die Registrierung erfolgreich aufgehoben wurde oder dass die Registrierung nicht aufgehoben werden konnte. Die Registrierung schlägt möglicherweise aus folgenden Gründen fehl:

- Der Repository Service für das lokale Repository wird nicht im exklusiven Modus ausgeführt.
- Der Repository Service konnte Informationen zum globalen Repository nicht initialisieren.
- Die Verbindung zum Repository Service wurde nicht hergestellt.

Der Unregister-Befehl verwendet die folgende Syntax:

```
unregister

-r <local_repository_name>

-n <local_repository_user_name>

[-s <local_repository_user_security_domain>]

[-x <local_repository_password> |

 -X <repository_password_environment_variable>]

[-d <local_repository_domain_name> |

{-h <local_repository_portal_host_name>

-o <local_repository_portal_port_number>}] (if local repository is in a different domain)
```

In der folgenden Tabelle werden die *pmrep* Unregister-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-r	local_repository_name	Erforderlich. Name des lokalen Repository, dessen Registrierung aufgehoben werden soll.
-n	local_repository_user_name	Erforderlich. Lokaler Benutzernamen.
-s	local_repository_user_security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Die Standardeinstellung ist "Native".
-x	local_repository_password	Erforderlich, wenn Sie nicht die Option -X verwenden. Anmelde-Passwort für das lokale Target-Repository. Sie müssen die Option -x oder -X verwenden, aber nicht beide.
-X	local_repository_password_environment_variable	Erforderlich, wenn Sie nicht die Option -x verwenden. Anmelde-Passwort-Umgebungsvariable für das lokale Target-Repository. Sie müssen die Option -x oder -X verwenden, aber nicht beide.
-d	local_repository_domain_name	Erforderlich, wenn sich das lokale Repository in einer anderen Domäne befindet und Sie nicht die Optionen -h und -o verwenden. Name der Informatica-Domäne für das Repository.
-h	local_repository_portal_host_name	Erforderlich, wenn sich das lokale Repository in einer anderen Domäne befindet und Sie nicht die Option -d verwenden. Computername der Domäne, in der sich das lokale Repository befindet. Wenn Sie diese Option verwenden, müssen Sie auch die Option -o benutzen.
-o	local_repository_portal_port_number	Erforderlich, wenn sich das lokale Repository in einer anderen Domäne befindet und Sie nicht die Option -d verwenden. Portnummer für die Domäne, in der sich das lokale Repository befindet. Wenn Sie diese Option verwenden, müssen Sie auch die Option -h verwenden.

UnregisterPlugin

Entfernt ein Plug-In aus einem Repository. Sie können Plug-Ins hinzufügen und entfernen, um die Systemfunktionalität zu erweitern. Ein Plug-In ist ein Softwaremodul, das neue Repository-Metadaten einsetzt.

Wenn Sie diesen Befehl verwenden, muss der Repository Service im exklusiven Modus ausgeführt werden. Sie können die Ausführung des Repository Service im exklusiven Modus im Administrator-Tool konfigurieren oder den Befehl *infacmd* UpdateRepositoryService verwenden.

Der UnregisterPlugin-Befehl verwendet die folgende Syntax:

```
unregisterplugin

-v <vendor_id>

-l <plug-in_id>

[-s (is security module)
```

```
[-g (remove user-name-login mapping)]
{-w <new_password> |
 -W <new_password_environment_variable>}]
```

In der folgenden Tabelle werden die *pmrep* UnregisterPlugin-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-v	vendor_id	Erforderlich. Kennzeichnet das Sicherheits-Plug-In anhand der Identifikationsnummer des Lieferanten. Sie definieren diese Zahl beim Registrieren des Plug-Ins.
-l	plug-in_id	Erforderlich. Kennzeichnet das Plug-In anhand der Identifikationsnummer. Sie definieren diese Identifikationsnummer beim Registrieren des Plug-Ins.
-s	-	Optional. Gibt an, ob das Modul ein externes Sicherheitsmodul ist.
-g	-	Optional. Beim Registrieren eines externen Sicherheitsmoduls anwendbar. Entfernt die Zuordnung zwischen Benutzernamen und Anmeldenamen im Repository, wenn Sie die Registrierung eines externen Sicherheitsmoduls aufheben. Wenn Sie diese Option nicht angeben, bleibt die Zuordnung im Repository erhalten, aber der Repository Manager zeigt es nirgends an. Verwenden Sie diese Option, wenn Sie die Registrierung eines Sicherheitsmoduls aufheben.
-w	new_password	Erforderlich, wenn das Plug-In ein Sicherheitsmodul enthält. Erforderlich, wenn Sie nicht die Option -W verwenden. Sie müssen die Option -w oder -W verwenden, aber nicht beide. Gibt ein neues Passwort für den Benutzer an, der den UnregisterPlugin-Befehl ausführt. Wenn Sie die Registrierung eines externen Authentifizierungsmoduls aufheben, werden alle Benutzerpasswörter auf die Werte im Repository zurückgesetzt. Sie müssen ein neues Passwort für den Zugriff auf das Repository eingeben.
-W	new_password_environment_variable	Erforderlich, wenn das Plug-In ein Sicherheitsmodul enthält. Erforderlich, wenn Sie nicht die Option -w verwenden. Sie müssen die Option -w oder -W verwenden, aber nicht beide. Gibt eine neue Passwortumgebungsvariable für den Benutzer an, der den Befehl zum Aufheben der Registrierung ausführt. Wenn Sie die Registrierung eines externen Authentifizierungsmoduls aufheben, werden alle Benutzerpasswörter auf die Werte im Repository zurückgesetzt. Sie müssen ein neues Passwort für den Zugriff auf das Repository eingeben.

Aufheben der Registrierung eines externen Sicherheitsmoduls

Verwenden Sie den UnregisterPlugin-Befehl, um ein externes Sicherheitsmodul nicht mehr mit einem Repository zu verwenden. Wenn Sie die Registrierung des externen Sicherheitsmoduls aufheben, wechselt PowerCenter in den Repository-Authentifizierungmodus. Alle Benutzerpasswörter werden auf die Werte im Repository und nicht auf die Werte im externen Verzeichnis zurückgesetzt. Wenn Sie die Registrierung des Sicherheitsmoduls aufheben, gehen die Mappings zwischen den Benutzernamen und den externen

Sicherheitsanmeldenamen nicht verloren, sofern Sie nicht die Option -g eingeben. Verwenden Sie das Mapping erneut, wenn Sie ein neues Sicherheitsmodul registrieren.

Hinweis: Obwohl Sie die Zuordnungen zwischen externen Anmeldungen und Benutzernamen speichern können, zeigt der Repository Manager die externen Anmeldungen während der Ausführung unter der Benutzerauthentifizierung nicht an.

Sie müssen mithilfe der Option -w oder -W ein neues Passwort erstellen, wenn Sie die Registrierung des Sicherheitsmoduls aufheben.

Beispiel

Als Administrator entscheiden Sie, aus dem LDAP-Sicherheitsmodul zurück zur Repository-Authentifizierung zu wechseln. Sie entfernen das Mapping zwischen Benutzername und Anmeldung. Alle Benutzer, die Sie unter der Repository-Authentifizierung zum System hinzugefügt haben, können sich mit ihren alten Benutzernamen und Passwörtern anmelden. Alle Benutzer, die Sie unter der LDAP-Sicherheit zum Repository hinzugefügt haben, können sich erst anmelden, wenn Sie die zugehörigen Benutzernamen aktivieren.

Hinweis: Sie müssen die LDAP-NIS-Anmeldung und das Passwort bereitstellen, um den Befehl UnregisterPlugin zu verwenden. Sie müssen außerdem eine neues Passwort bereitstellen, das Sie nach dem Wechsel zur Benutzerauthentifizierung verwenden können.

UpdateConnection

Updates the user name, password, connect string, and attributes for a database connection.

The command returns an “operation successfully completed” or returns “operation failed” message. A failure might occur for the following reasons:

- The database type is not supported.
- The connection object does not exist.
- *pmrep* cannot acquire a lock on the object.
- One of the required parameters is missing.

The UpdateConnection command uses the following syntax:

```
updateconnection

-t <connection_subtype >

-d <connection_name>

[{-u <new_user_name>

[-p <new_password>|-P <new_password_environment_variable>]}|

-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>]
```

The following table describes *pmrep* UpdateConnection options and arguments:

Option	Argument	Description
-t	connection_subtype	Required. Displays the connection subtype. For example, for a Relational connection, connection subtypes include Oracle, Sybase, and Microsoft SQL Server. For FTP connections, the valid subtype is FTP. For a list of predefined connection subtypes, see "Verbindungsuntertypen" auf Seite 1151. **Hinweis:** The connection subtype in the -t option must be valid for the associated connection type specified with the -s option.
-d	connection_name	Required. Database connection name.
-u	new_user_name	Optional. User name used for authentication when you connect to the relational database.
-p	new_password	Optional. Password used for authentication when you connect to the relational database. Use the -p or -P option, but not both.
-P	new_password_ environment_variable	Optional. Password environment variable used for authentication when you connect to the relational database. Use the -p or -P option, but not both.
-K	-	Optional. Indicates that the database that you are connecting to runs on a network that uses Kerberos authentication.
-c	new_connection_string	Optional. Connect string the Integration Service uses to connect to the relational database.
-a	attribute_name	Optional. Name of the attribute.
-v	new_attribute_value	Required if you use the -a option. New attribute value of the connection. Enter "yes" to enable new attributes, and "no" to disable new attributes.
-s	connection type application, relational, ftp, loader or queue	Optional. Type of connection. A connection can be one of the following types: - Application - FTP - Loader - Queue - Relational Default is relational. **Hinweis:** The connection subtype in the -t option must be valid for the associated connection type specified with the -s option.
-l	code page	Optional. Code page associated with the connection.

For more information about connection subtypes, see "Verbindungsuntertypen" auf Seite 1151.

UpdateEmailAddr

Aktualisiert mit den der Sitzung zugewiesenen E-Mail-Aufgaben verbundene E-Mail-Adressen für die Sitzungsbenachrichtigung. Wenn Sie zuvor keine Erfolgs- bzw. Fehler-E-Mail-Aufgabe für die Sitzung eingegeben haben, aktualisiert der Befehl die E-Mail-Adressen nicht. Sie können die E-Mail-Benachrichtigungsadressen für eine nicht wiederverwendbare Sitzung mit einem einmaligen Namen im Ordner aktualisieren. Sie können unterschiedliche Adressen für den Empfang von Erfolgs- oder Fehlerbenachrichtigungen eingeben. Dieser Befehl erfordert eine Verbindung zu einem Repository.

Der UpdateEmailAddr-Befehl verwendet die folgende Syntax:

```
updateemailaddr

-d <folder_name>

-s <session_name>

-u <success_email_address>

-f <failure_email_address>
```

In der folgenden Tabelle werden die *pmrep* UpdateEmailAddr-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-d	folder_name	Erforderlich. Name des Sitzungsordners.
-s	session_name	Erforderlich. Name der Sitzung.
-u	success_email_address	Erforderlich. E-Mail-Adresse zum Senden von Benachrichtigungen für erfolgreiche Sitzungen.
-f	failure_email_address	Erforderlich. E-Mail-Adresse zum Senden von Benachrichtigungen für fehlgeschlagene Sitzungen.

UpdateSeqGenVals

Aktualisiert eine oder mehrere der folgenden Eigenschaften für die angegebene Sequenzgenerator-Transformation:

- Startwert
- Endwert
- Inkrementieren um
- Aktueller Wert

Möglicherweise möchten Sie Sequenzwerte beim Verschieben eines Mappings von einem Entwicklungsumfeld in eine Produktionsumgebung aktualisieren. Verwenden Sie den UpdateSeqGenVals-Befehl zum Aktualisieren wiederverwendbarer und nicht wiederverwendbarer Sequenzgenerator-Transformationen. Werte für Instanzen wiederverwendbarer Sequenzgenerator-Transformationen oder Shortcuts zu Sequenzgenerator-Transformationen können Sie jedoch nicht aktualisieren.

Der UpdateSeqGenVals-Befehl verwendet die folgende Syntax:

```
updateseqgenvals
```

```
-f <folder_name>

[-m <mapping_name>]

-t <sequence_generator_name>

[-s <start_value>]

[-e <end_value>]

[-i <increment_by>]

[-c <current_value>]
```

In der folgenden Tabelle werden die *pmrep* UpdateSeqGenVals-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-f	folder_name	Erforderlich. Ordnername.
-m	mapping_name	Mapping-Name. Beim Aktualisieren von Werten für eine nicht wiederverwendbare Sequenzgenerator-Transformation müssen Sie den Mapping-Namen einbeziehen.
-t	sequence_generator_name	Erforderlich. Sequenzgenerator-Transformationsname.
-s	start_value	Optional. Startwert der generierten Sequenz, die der Integration Service verwenden soll, wenn die Sequenzgenerator-Transformation die Zykluseigenschaft verwendet. Wenn Sie in den Transformationseigenschaften Zyklus auswählen, kehrt der Integration Service zu diesem Wert zurück, wenn er den Endwert erreicht. Wenn Sie einen ungültigen Wert bestimmen, gibt *pmrep* eine Fehlermeldung aus und aktualisiert die Sequenzgenerator-Transformation nicht.
-e	end_value	Optional. Maximaler von Integration Service generierter Wert. Wenn der Integration Service diesen Wert während der Sitzung erreicht und die Sequenz nicht für den Zyklus konfiguriert ist, schlägt die Sitzung fehl. Wenn Sie einen ungültigen Wert bestimmen, zeigt *pmrep* eine Fehlermeldung an und aktualisiert die Sequenzgenerator-Transformation nicht.
-i	increment_by	Optional. Unterschied zwischen zwei aufeinander folgenden Werten aus dem NEXTVAL-Port. Wenn Sie einen ungültigen Wert bestimmen, zeigt *pmrep* eine Fehlermeldung an und aktualisiert die Sequenzgenerator-Transformation nicht.
-c	current_value	Optional. Aktueller Wert der Sequenz. Geben Sie den Wert ein, den der Integration Service als ersten Wert in der Sequenz verwenden soll. Wenn Sie eine Reihe von Werten nacheinander verwenden möchten, muss der aktuelle Wert größer oder gleich dem Anfangswert und kleiner als der Endwert sein. Wenn Sie einen ungültigen Wert bestimmen, gibt *pmrep* eine Fehlermeldung aus und aktualisiert die Sequenzgenerator-Transformation nicht.

UpdateSrcPrefix

Aktualisiert den Eigentümernamen für Sitzungsquelltabellen. Sie können den Eigentümernamen für eine oder alle Quellen in einer Sitzung aktualisieren. Updatesrcprefix aktualisiert den Eigentümernamen für Quelltabellen auf Sitzungsebene.

pmrep aktualisiert Eigentümernamen für Quelltabellen, wenn Sie zuvor den Quelltabellennamen in den Sitzungseigenschaften bearbeitet haben.

Der UpdateSrcPrefix-Befehl verwendet die folgende Syntax:

```
updatesrcprefix

-f <folder_name>

-s [<qualifying_path>.]<session_name>

[-t <source_name>]

-p <prefix_name>

[-n (use source instance name; not using -n gives old, deprecated behavior)]
```

In der folgenden Tabelle werden die *pmrep* UpdateSrcPrefix-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-f	folder_name	Erforderlich. Name des Ordners, der die Sitzung enthält.
-s	session_name	Erforderlich. Name der Sitzung, in der die zu aktualisierenden Quellen enthalten sind. Geben Sie für wiederverwendbare Sitzungen den Sitzungsnamen ein. Für nicht wiederverwendbare Sitzungen müssen Sie außerdem den Sitzungspfad eingeben, z. B.*worklet_name.session_name* oder *workflow_name.session_name*.
-t	source_name	Optional. Name der zu aktualisierenden Quelle. Wenn Sie diese Option nicht angeben, aktualisiert *pmrep* alle Eigentümernamen für Quelltabellen in der Sitzung. Wenn Sie die Option -n einbeziehen, können Sie den Namen der Quellinstanz wie in den Sitzungseigenschaften angezeigt oder als Ausgabe des ListTablesBySess-Befehls eingeben. Obwohl der UpdateSrcPrefix-Befehl auch ohne die Option -n ausgeführt wird, beziehen Sie die Option -n ein, um den Quellinstanznamen zu verwenden. Wenn Sie die Option -n nicht angeben, müssen Sie den DBD-Namen und die Quelltabellennamen als *dbd_name.source_name* eingeben. Der Quell-DBD-Name befindet sich im Designer Navigator. Der Designer generiert den DBD-Namen aus dem Quelltyp oder Datenquellnamen beim Erstellen einer Quelldefinition im Repository.

Option	Argument	Beschreibung
-p	prefix_name	Erforderlich. Eigentümername, den Sie in der Quelltabelle aktualisieren möchten.
-n	-	Optional. Gleicht das source_name-Argument mit Quellinstanznamen ab. Obwohl der UpdateSrcPrefix-Befehl auch ohne die Option -n ausgeführt wird, beziehen Sie die Option -n ein, um den Quellinstanznamen zu verwenden. Wenn Sie diese Option nicht angeben, gleicht *pmrep* das source_name-Argument mit den Quelltabellenamen ab.

UpdateStatistics

Aktualisiert die Statistiken für Repository-Tabellen und -Indizes.

Der Befehl gibt „updatestatistics erfolgreich abgeschlossen“ oder „updatestatistics fehlgeschlagen“ zurück.

Der UpdateStatistics-Befehl verwendet die folgende Syntax:

```
updatestatistics
```

UpdateTargPrefix

Aktualisiert den Tabellennamenspräfix für Sitzungs-Target-Tabellen. Der Tabellennamenspräfix gibt den Eigentümer der Tabelle in der Datenbank an. Sie können den Eigentümernamen eines oder aller in einer Sitzung angegebenen Targets aktualisieren. UpdateTargPrefix aktualisiert den Namenspräfix der Target-Tabelle auf Sitzungsebene.

pmrep aktualisiert Tabellennamenspräfixe, wenn Sie zuvor den Tabellennamenspräfix auf Sitzungsebene bearbeitet haben.

Der UpdateTargPrefix-Befehl verwendet die folgende Syntax:

```
updatetargprefix

-f <folder_name>

-s [<qualifying_path>.]<session_name>

[-t <target_name>]

-p <prefix_name>

[-n (use target instance name; not using -n gives old, deprecated behavior)]
```

In der folgenden Tabelle werden die *pmrep* UpdateTargPrefix-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-f	folder_name	Erforderlich. Name des Ordners, der die Sitzung enthält.
-s	session_name	Erforderlich. Name der Sitzung, in der die zu aktualisierenden Ziele enthalten sind. Geben Sie für wiederverwendbare Sitzungen den Sitzungsnamen ein. Für nicht wiederverwendbare Sitzungen geben Sie den Sitzungsnamen und -pfad ein, z. B.*worklet_name.session_name* oder *workflow_name.session_name*.
-t	target_name	Optional. Name des zu aktualisierenden Ziels. Wenn Sie diese Option nicht angeben, aktualisiert *pmrep* alle Namenspräfixe von Zieltabellen in der Sitzung. Wenn Sie die Option -n einbeziehen, können Sie den Namen der Zielinstanz wie in den Sitzungseigenschaften angezeigt oder als Ausgabe des ListTablesBySess-Befehls eingeben. Obwohl der UpdateTargPrefix-Befehl auch ohne die Option -n ausgeführt wird, beziehen Sie die Option -n ein, um den Zielinstanznamen zu verwenden. Wenn Sie die Option -n nicht angeben, müssen Sie den Zieltabellennamen anstelle des Zielinstanznamens eingeben.
-p	prefix_name	Erforderlich. Tabellennamenspräfix, das Sie in der Zieltabelle aktualisieren möchten.
-n	-	Optional. Gleicht das Zielnamensargument mit den Zielinstanznamen ab. Obwohl der UpdateTargPrefix-Befehl auch ohne die Option -n ausgeführt wird, beziehen Sie die Option -n ein, um den Zielinstanznamen zu verwenden. Wenn Sie diese Option nicht angeben, gleicht *pmrep* das Zielnamensargument mit den Zieltabellennamen ab.

Upgrade

Aktualisiert ein Repository auf die neueste Version.

Der Upgrade-Befehl verwendet die folgende Syntax:

```
upgrade

[-x <repository_password_for_confirmation> |

 -X <repository_password_environment_variable_for_confirmation>]
```

In der folgenden Tabelle werden *pmrep* Upgrade-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-x	repository_ password_for_ confirmation	Optional. Passwort. Sie können die Option -x oder -X Option verwenden, aber nicht beide. Wenn Sie weder die Option -x noch -X verwenden, werden Sie von pmrep aufgefordert, zur Bestätigung das Passwort einzugeben.
-X	repository_password_ environment_variable_for_ confirmation	Erforderlich, wenn Sie nicht die Option -x verwenden. Passwort-Umgebungsvariable. Sie müssen die Option -x oder -X verwenden, aber nicht beide.

UninstallAbapProgram

Deinstalliert das ABAP-Programm. Deinstallieren Sie ein ABAP-Programm, wenn das Programm nicht länger einem Mapping zugeordnet werden soll. Der Befehl deinstalliert die Programme vom SAP-System und entfernt die entsprechenden Programminformationen aus dem PowerCenter Repository.

Der UninstallAbapProgram-Befehl verwendet die folgende Syntax:

```
uninstallabapprogram

-s <folder_name>

-m <mapping_name>

[-v <version_number>]

[-l <log_filename>]

-u <user_name>

-x <password>

-c <connect_string>

-t <client>

[-y <language>]

-p <program_mode (file, stream)>
```

In der folgenden Tabelle werden die pmrep UninstallAbapProgram-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-s	folder_name	Erforderlich. Der Name des Ordners, in dem das Mapping des ABAP-Programms enthalten ist, das Sie deinstallieren möchten.
-m	mapping_name	Erforderlich. Name des Mappings.
-v	version_number	Optional. Versionsnummer des Mappings. Standardmäßig ist die neueste Version.

Option	Argument	Beschreibung
-l	log_filename	Optional. Name der Protokolldatei, in die der Befehl die Informationen oder Fehlermeldungen schreibt. Standardmäßig wird die Protokolldatei in dem Verzeichnis gespeichert, in dem Sie den Befehl ausführen.
-u	user_name	Erforderlich. Benutzername für die SAP-Quellsystemverbindung. Muss ein Benutzer sein, für den Sie eine Quellsystemverbindung erstellt haben.
-x	passwort	Erforderlich. Passwort für den Benutzernamen. Verwenden Sie das Befehlszeilenprogramm pmpasswd zum Verschlüsseln des Benutzerpasswords.
-c	connect_string	Erforderlich. In der Datei `sapnwrfc.ini` definierter DEST-Eintrag für eine Verbindung mit einem bestimmten SAP-Anwendungsserver oder für eine Verbindung, die den SAP-Lastenausgleich verwendet.
-t	Client	Erforderlich. SAP-Clientnummer.
-y	Sprache	Optional. SAP-Anmeldesprache. Muss mit der Codepage des PowerCenter Client kompatibel sein. Standardwert ist die Sprache des SAP-Systems.
-p	program_mode (file, stream)	Erforderlich. Modus, in denen der PowerCenter-Integrationsdienst Daten aus dem SAP-System extrahiert. Wählen Sie die Datei oder den Stream aus.

Beispiel

Das folgende Beispiel deinstalliert das ABAP-Programm:

```
uninstallabapprogram -s folder_name -m mapping_name -l logfile_name -u user_name -x
password -c connect_string -t 800 -y EN -p stream
```

Validieren

Validiert Objekte. Sie können die Ergebnisse in eine persistente Ausgabedatei oder Standardausgabe ausgeben.

Es zeigt außerdem eine Zusammenfassung der Validierung in „stdout“ an. Die Zusammenfassung enthält die Anzahl der gültigen Objekte, ungültigen Objekte und übersprungenen Objekte. Die persistente Ausgabedatei enthält Standardinformationen, kodierte IDs und eine CRC-Überprüfung. Sie können die Objekte speichern und einchecken, die von ungültig zu gültig wechseln.

Sie können die folgenden Objekttypen validieren:

- Mappings
- Mapplets
- Sitzungen
- Arbeitsabläufe
- Worklet-Objekte

Wenn Sie im Eingabeparameter einen anderen Objekttyp verwenden, gibt *pmrep* einen Fehler zurück. Wenn Sie in einer persistenten Eingabedatei den falschen Objekttyp verwenden, berichtet *pmrep* einen Fehler und überspringt das Objekt.

Hinweis: Der *pmrep* Validate-Befehl validiert keine Shortcuts.

Wenn Sie Validate ausführen, können Sie Informationen zum Objektstatus ausgeben:

- **valid.** Objekte wurden erfolgreich validiert.
- **saved.** Objekte wurden nach der Validierung gespeichert.
- **skipped.** Shortcuts und Objekttypen, die keine Validierung erfordern.
- **save_failed.** Objekte, die aufgrund von Sperrkonflikten nicht gespeichert wurden oder von einem anderen Benutzer ausgecheckt wurden.
- **invalid_before.** Objekte, die vor der Validierungsprüfung ungültig sind.
- **invalid_after.** Objekte, die nach der Validierungsprüfung ungültig sind.

Ein nicht wiederverwendbares Objekt kann erst gespeichert werden, wenn das wiederverwendbare übergeordnete Objekt des Objekts gespeichert wird. Wenn Sie die Option -s verwenden, speichert der Befehl keine validierten nicht wiederverwendbaren Objekte, es sei denn, Sie listen als Teil desselben Befehls wiederverwendbare Objekte auf, die als übergeordnete Objekte der nicht wiederverwendbaren Objekte fungieren.

Der Validate-Befehl verwendet die folgende Syntax:

```
validate
{{-n <object_name>
-o <object_type (mapplet, mapping, session, worklet, workflow)>
[-v <version_number>]
[-f <folder_name>]} |
-i <persistent_input_file>}
[-s (save upon valid)
[-k (check in upon valid)
[-m <check_in_comments>]]]
[-p <output_option_types (valid, saved, skipped, save_failed, invalid_before,
invalid_after, or all)>]
[-u <persistent_output_file_name>
[-a (append)]]
[-c <column_separator>]
[-r <end-of-record_separator>]
[-l <end-of-listing_indicator>]
[-b (verbose)]
[-y (print database type)]
```

In der folgenden Tabelle werden die Optionen und Argumente für „*pmrep* Validate“ beschrieben:

Option	Argument	Beschreibung
-n	object_name	Erforderlich. Name des zu validierenden Objekts. Verwenden Sie diese Option nicht bei Verwendung des Arguments -i. Schließen Sie beim Validieren einer nicht wiederverwendbaren Sitzung den Namen des Arbeitsablaufs ein. Geben Sie den Namen des Arbeitsablaufs und den Namen der Sitzung in folgendem Format ein: <Name des Arbeitsablaufs>.<Name der Sitzungsinstanz>
-o	object_type	Erforderlich, wenn Sie keine persistente Eingabedatei verwenden. Zu validierender Objekttyp. Sie können Mapplets, Zuordnungen, Sitzungen, Worklets und Arbeitsabläufe angeben.
-v	version_number	Optional. Version des zu validierenden Objekts. Standardwert ist die neueste oder ausgecheckte Version des Objekts.
-f	folder_name	Erforderlich. Name des Ordners, der das Objekt enthält.

Option	Argument	Beschreibung
-i	persistent_input_file	Optional. Textdatei aus dem Befehl ExecuteQuery, Validate oder ListObjectDependencies. Enthält eine Liste mit Objektdatensätzen. Sie können diese Datei nicht verwenden, wenn Sie Objekte mithilfe der Argumente -n, -o oder -f angeben.
-s	-	Optional. Speichern Sie Objekte, die von ungültig zu gültig wechseln, im Repository.
-k	-	Erforderlich, wenn Sie -s verwenden. Checken Sie gespeicherte Objekte ein.
-m	check_in_comments	Erforderlich, wenn Sie die Option -k verwenden. Zudem erfordert das aktuelle Repository Eincheck-Kommentare. Fügen Sie beim Einchecken eines Objekts Kommentare hinzu.
-p	output_option_types	Erforderlich, wenn Sie das Argument -u verwenden. Objekttyp, den Sie nach der Validierung in die persistente Ausgabedatei oder in „stdout“ ausgeben möchten. Sie können valid, saved, skipped, save_failed, invalid_before oder invalid_after angeben. Geben Sie eine oder mehrere Optionen durch Kommas getrennt ein.
-u	persistent_output_file_name	Erforderlich, wenn Sie das Argument -p verwenden. Name einer Ausgabetextdatei. Wenn Sie einen Dateinamen eingeben, schreibt die Abfrage die Ergebnisse in eine Datei.
-a	append	Optional. Hängt die Ergebnisse an die persistente Ausgabedatei an, statt sie zu überschreiben.
-c	column_separator	Optional. Zeichen oder Zeichenfolgen zum Trennen von Spalten mit Objektmetadaten. Verwenden Sie ein Zeichen oder eine Zeichenfolge, die nicht in Repository-Objektnamen verwendet wird. Wenn ein Repository-Objektname Leerzeichen enthält, sollten Sie kein Leerzeichen als Spaltentrennzeichen verwenden. Wenn Sie diese Option auslassen, verwendet *pmrep* ein einzelnes Leerzeichen.
-r	end-of-record_separator	Optional. Zeichen oder Zeichenfolgen, die das Ende der Objektmetadaten kennzeichnen. Verwenden Sie ein Zeichen oder eine Zeichenfolge, die nicht in Repository-Objektnamen verwendet wird. Standardwert ist „newline“ /n.
-l	end-of-listing_indicator	Optional. Zeichen oder Zeichenfolgen, die das Ende der Objektliste kennzeichnen. Geben Sie ein Zeichen oder eine Zeichenfolge ein, die nicht in Repository-Objektnamen verwendet wird. Wenn Sie diese Option auslassen, verwendet *pmrep* einen Punkt.

Option	Argument	Beschreibung
-b	-	Optional. Verbose. Zeigt neben den Mindestinformationen weitere Informationen zu den Objekten an. Wenn Sie diese Option auslassen, zeigt *pmrep* ein reduziertes Format an, einschließlich des Objekttyps, wiederverwendbarer oder nicht wiederverwendbarer Wörter, des Objektnamens und -pfads. Verbose-Format enthält die Versionsnummer und den Ordnernamen. Das Kurzformat für globale Objekte, wie Beschriftung, Abfrage, Bereitstellungsgruppe und Verbindung, enthält den Objekttyp und den Objektnamen. Verbose-Format enthält den Erstellernamen und den Zeitpunkt der Erstellung.
-y	-	Optional. Zeigt den Datenbanktyp von Quellen und Zielen an.

Version

Zeigt die PowerCenter-Version und Informatica-Handelsmarke sowie Urheberrechtsinformationen an.

Der Version-Befehl verwendet die folgende Syntax:

```
version
```

KAPITEL 34

Arbeiten mit pmrep-Dateien

Dieses Kapitel umfasst die folgenden Themen:

- Arbeiten mit pmrep-Dateien - Übersicht, 1235
- Verwenden der persistenten Eingabedatei , 1235
- Verwenden der Objektimport-Steuerdatei, 1238
- Objektimport-Steuerdatei – Beispiele, 1242
- Verwenden der Bereitstellungssteuerdatei , 1249
- Bereitstellungs-Steuerdatei – Beispiele, 1254
- Tipps für die Arbeit mit pmrep-Dateien, 1256

Arbeiten mit pmrep-Dateien - Übersicht

pmrep enthält eine Reihe von Steuerdateien, mit denen Sie definieren können, wie Objekte ins Repository importiert werden. Die Steuerdateiparameter verwenden dieselben Parameter in der Steuerdatei, die Sie im PowerCenter Client verwenden. Sie können die folgenden Steuerdateien verwenden:

- **Persistente Eingabedatei**. Verwenden Sie eine persistente Eingabedatei, um Repository-Objekte anzugeben, die Sie verarbeiten möchten.
- **Objektimport-Steuerdatei**. Verwenden Sie die Objektimport-Steuerdatei und geben Sie eine Reihe von Fragen an, um zu definieren, wie Objekte importiert werden.
- **Bereitstellungssteuerdatei** Sie können die Objekte in einer dynamischen oder statischen Bereitstellungsgruppe in mehrere Target-Ordner im Target-Repository kopieren.

Verwenden der persistenten Eingabedatei

Wenn Sie *pmrep* mit einigen Aufgaben ausführen, verwenden Sie eine persistente Eingabedatei zum Angeben der Repository-Objekte, die Sie verarbeiten möchten. Die persistente Eingabedatei repräsentiert bereits im Repository vorhandene Objekte. Sie können eine persistente Eingabedatei manuell oder mithilfe von *pmrep* erstellen.

Verwenden Sie eine persistente Eingabedatei mit den folgenden *pmrep*-Befehlen:

- **AddToDeploymentGroup**. Fügt Objekte einer Bereitstellungsgruppe hinzu.
- **ApplyLabel**. Beschriftet Objekte.

- **ExecuteQuery.** Führt eine Abfrage aus, um eine persistente Eingabedatei zu erstellen. Verwenden Sie die Datei für andere *pmrep*-Befehle.
- **ListObjectDependencies**. Listet Abhängigkeitsobjekte auf. Dieser Befehl kann eine persistente Eingabedatei für die Verarbeitung verwenden und er kann eine erstellen.
- **MassUpdate.** Aktualisiert die Sitzungseigenschaften für eine Reihe von Sitzungen.
- **ObjectExport**. Exportiert Objekte in eine XML-Datei.
- **Validate**. Validiert Objekte. Dieser Befehl kann eine persistente Eingabedatei für die Verarbeitung verwenden und er kann eine erstellen.

Die persistente Eingabedatei verwendet das folgende Format:

```
encoded ID, foldername, object_name, object_type, object_subtype, version_number,
reusable|non-reusable
```

Erstellen einer persistenten Eingabedatei mit pmrep

Sie können eine persistente Eingabedatei unter Verwendung der *pmrep*-Befehle ExecuteQuery, Validate oder ListObjectDependencies erstellen. Mithilfe dieser Befehle werden Dateien erstellt, die eine Liste von Objekten mit verschlüsselten IDs und einem CRC-Wert (Cyclic Redundancy Check, zyklische Redundanzprüfung) enthalten. Weiterhin ist eine verschlüsselte Repository-GID enthalten. Mit dieser ID wird das Repository angegeben, aus dem der Datensatz stammt.

Die *pmrep*-Befehle, die eine persistente Eingabedatei verwenden, rufen die Objektinformationen aus den verschlüsselten IDs ab. Die verschlüsselten IDs ermöglichen *pmrep* die schnelle Verarbeitung der Eingabedatei.

Beim Erstellen einer persistenten Eingabedatei mit *pmrep* wird diese im *pmrep*-Installationsverzeichnis gespeichert. Sie können einen anderen Pfad angeben.

Der folgende Text zeigt ein Beispiel für eine persistente Eingabedatei:

```
2072670638:57bfc2ff-df64-40fc-9cd4-
a15cb489bab8:3538944199885:138608640183285:1376256153425:131072168215:65536142655:0288235
:088154:65536122855,EXPORT,M_ITEMS,mapping,none,2
1995857227:57bfc2ff-df64-40fc-9cd4-
a15cb489bab8:3538944135065:13867417666804:1376256233835:19660880104:65536271545:0319425:0
17154:6553644164,EXPORT,M_ITEMS_2,mapping,none,3
1828891977:57bfc2ff-df64-40fc-9cd4-
a15cb489bab8:3538944279765:138739712184505:137625613474:65536221345:65536133675:091734:09
053:65536156675,EXPORT,M_NIELSEN,mapping,none,1
3267622055:57bfc2ff-df64-40fc-9cd4-
a15cb489bab8:353894462954:138805248300075:1376256151365:6553675414:65536174015:0273455:02
41435:65536261685,EXPORT,M_OS1,mapping,none,1
```

Beispiel

Sie können den Befehl ExecuteQuery zum Erstellen einer persistenten Eingabedatei für Objekte verwenden, die in einem anderen *pmrep*-Befehl verarbeitet werden. Sie möchten beispielsweise alle logisch gelöschten Objekte aus dem Repository exportieren. Sie können eine Abfrage mit der Bezeichnung "find_deleted_objects" erstellen. Wenn Sie die Abfrage wie hier angezeigt mit *pmrep* ausführen, werden alle gelöschten Objekte im Repository gefunden und die Ergebnisse in eine persistente Eingabedatei geschrieben:

```
ExecuteQuery -q find_deleted_objects -t private -u deletes_workfile
```

Sie können "deletes_workfile" dann als persistente Eingabedatei für ObjectExport verwenden:

```
ObjectExport -i deletes_workfile -u exported_del_file
```

ObjectExport exportiert alle referenzierten Objekte in eine XML-Datei mit der Bezeichnung "exported_del_file".

Manuelles Erstellen einer persistenten Eingabedatei

Wenn Sie *pmrep*-Befehle für eine Gruppe von Objekten ausführen möchten, die über Befehle wie ExecuteQuery nicht ermittelt werden können, besteht die Möglichkeit zur manuellen Erstellung einer Eingabedatei.

Verwenden Sie die folgenden Regeln und Richtlinien, wenn Sie ein persistente Eingabedatei erstellen:

- Geben Sie "none" für die verschlüsselte ID ein. Die *pmrep*-Befehle erhalten die Objektinformationen aus den anderen Argumenten in den Datensätzen.
- Geben Sie für Quellobjekte den Objektnamen wie folgt ein: <DBD_name>.<source_name>.
- Geben Sie für Objekte, wie z. B. Mappings, die nicht über sub_type verfügen, "none" als object_subtype ein oder nehmen Sie keine Eingabe vor. Weitere Informationen zu gültigen Umwandlungen und Aufgabentypen finden Sie unter "Auflisten von Objekttypen" auf Seite 1192.
- Geben Sie bei versionierten Repositories die Versionsnummer des gewünschten Objekts ein. Alternativ können Sie auch "AKTUELL" eingeben, um die aktuelle Version des Objekts zu verwenden.
- Lassen Sie bei unversionierten Repositories das Argument version_number leer.
- Ignorieren Sie das Argument bei Objekttypen, wie z. B. Targets, die weder wiederverwendbar noch nicht wiederverwendbar sein können.
- Nicht wiederverwendbare Objekte können nicht aufgenommen werden. Sie können das wiederverwendbare übergeordnete Objekt des nicht wiederverwendbaren Objekts angeben.

  Sie möchten beispielsweise die Objektabhängigkeiten für eine nicht wiederverwendbare Filtertransformation auflisten. Sie können das Mapping, das als übergeordnetes Objekt der Transformation fungiert, angeben:

  ```
  none,CAPO,m_seqgen_map,mapping,none,1,reusable
  ```

  Das Mapping m_seqgen_map ist das wiederverwendbare übergeordnete Objekt der Filtertransformation. Der Befehl wird erfolgreich ausgeführt, wenn Sie das wiederverwendbare übergeordnete Objekt angeben.

Hinweis: Wenn Sie eine manuell erstellte persistente Eingabedatei verwenden, gibt der Repository Service eine Meldung mit dem Hinweis zurück, dass die ID ungültig ist. Hierbei handelt es sich um eine Informationsmeldung. Der Repository Service erkennt, dass es sich um eine manuell erstellte Eingabedatei handelt, und kann den Befehl mit "none" als ID verarbeiten.

Beispiel

Das folgende Beispiel zeigt eine manuell erstellte persistente Eingabedatei:

```
none,EXPORT,CustTgt,target,none,2
none,EXPORT,S_Orders,session,,2,reusable
none,EXPORT,EXP_CalcTot,transformation,expression,LATEST,reusable
```

Im ersten Datensatz handelt es sich bei CustTgt um eine Target-Definition. Targets haben keinen Untertyp, d. h., Sie geben "none" für das Argument object_subtype ein. Ein Target kann weder wiederverwendbar noch nicht wiederverwendbar sein, daher kann das Wiederverwendbarkeitsargument wegfallen. Beachten Sie, dass der Datensatz sechs statt sieben Argumente aufweist.

Im zweiten Datensatz handelt es sich bei S_Orders um eine Sitzung. Sitzungen haben keinen Untertyp, d. h. Sie lassen das Argument leer.

Der dritte Datensatz soll die aktuelle Version der Transformation aufweisen, d. h., Sie geben "LATEST" für das Argument version_number ein.

Verwenden der Objektimport-Steuerdatei

Wenn Sie den *pmrep* ObjectImport-Befehl verwenden, können Sie mit einer Steuerdatei Fragen beantworten, die Sie in der Regel beim Importieren von Objekten mit dem Importassistenten bearbeiten. Zum Erstellen einer Steuerdatei müssen Sie eine durch impcntl.dtd definierte XML-Datei erstellen. Die Importsteuerdatei wird mit dem PowerCenter Client installiert. Sie müssen deren Speicherort in der Eingabe-XML-Datei aufnehmen.

Im Folgenden sehen Sie ein Beispiel für eine impcntl.dtd-Datei:

```
<!-- Informatica Object Import Control DTD Grammar - >

<!--IMPORTPARAMS This inputs the options and inputs required for import operation -->
<!--CHECKIN_AFTER_IMPORT Check in objects on successful import operation -->
<!--CHECKIN_COMMENTS Check in comments -->
<!--APPLY_LABEL_NAME Apply the given label name on imported objects -->
<!--RETAIN_GENERATED_VALUE Retain existing sequence generator, normalizer and XML DSQ
current values in the destination -->
<!--COPY_SAP_PROGRAM Copy SAP program information into the target repository -->
<!--APPLY_DEFAULT_CONNECTION Apply the default connection when a connection used by a
session does not exist in the target repository -->
<!ELEMENT IMPORTPARAMS (FOLDERMAP*, TYPEFILTER*, RESOLVECONFLICT?)>
<!ATTLIST IMPORTPARAMS
        CHECKIN_AFTER_IMPORT                                    (YES | NO) "NO"
        CHECKIN_COMMENTS          CDATA      #IMPLIED
        APPLY_LABEL_NAME          CDATA      #IMPLIED
        RETAIN_GENERATED_VALUE    (YES | NO) "NO"
        COPY_SAP_PROGRAM          (YES | NO) "YES"
        APPLY_DEFAULT_CONNECTION  (YES | NO) "NO"
>

<!--FOLDERMAP matches the folders in the imported file with the folders in the target
repository -->
<!ELEMENT FOLDERMAP EMPTY>
<!ATTLIST FOLDERMAP
        SOURCEFOLDERNAME     CDATA    #REQUIRED
            SOURCEREPOSITORYNAME CDATA    #REQUIRED
        TARGETFOLDERNAME     CDATA    #REQUIRED
        TARGETREPOSITORYNAME CDATA    #REQUIRED
>

<!--Import will only import the objects in the selected types in TYPEFILTER node -->
<!--TYPENAME type name to import. This should comforming to the element name in
powermart.dtd, e.g. SOURCE, TARGET and etc.-->
<!ELEMENT TYPEFILTER EMPTY>
<!ATTLIST TYPEFILTER
        TYPENAME    CDATA    #REQUIRED
>

<!--RESOLVECONFLICT allows to specify resolution for conflicting objects during import.
The combination of specified child nodes can be supplied -->
<!ELEMENT RESOLVECONFLICT (LABELOBJECT | QUERYOBJECT | TYPEOBJECT | SPECIFICOBJECT)*>

<!--LABELOBJECT allows objects in the target with label name to apply replace/reuse upon
conflict -->
<!ELEMENT LABELOBJECT EMPTY>
<!ATTLIST LABELOBJECT
        LABELNAME            CDATA                        #REQUIRED
        RESOLUTION          (REPLACE | REUSE | RENAME)    #REQUIRED
>

<!--QUERYOBJECT allows objects result from a query to apply replace/reuse upon conflict
-->
<!ELEMENT QUERYOBJECT EMPTY>
<!ATTLIST QUERYOBJECT
        QUERYNAME             CDATA                        #REQUIRED
        RESOLUTION            (REPLACE | REUSE | RENAME)    #REQUIRED
>
```

```
<!--TYPEOBJECT allows objects of certain type to apply replace/reuse upon conflict-->
<!ELEMENT TYPEOBJECT EMPTY>
<!ATTLIST TYPEOBJECT
OBJECTTYPENAME            CDATA                        #REQUIRED
RESOLUTION                REPLACE | REUSE | RENAME)    #REQUIRED
>

<!--SPECIFICOBJECT allows a particular object(name, typename etc.) to apply replace/
reuse upon conflict -->
<!--NAME Object name-->
<!--EXTRANAME Source DBD name - required for source object to identify uniquely-->
<!--OBJECTTYPENAME Object type name-->
<!--FOLDERNAME Folder which the object belongs to-->
<!--REPOSITORYNAME Repository name that this object belongs to-->
<!--RESOLUTION Resolution to apply for the object in case of conflict-->
<!ELEMENT SPECIFICOBJECT EMPTY>
<!ATTLIST SPECIFICOBJECT
        NAME           CDATA    #REQUIRED
        DBDNAME        CDATA    #IMPLIED
        OBJECTTYPENAME CDATA    #REQUIRED
        FOLDERNAME     CDATA    #REQUIRED
        REPOSITORYNAME CDATA    #REQUIRED
        RESOLUTION
(REPLACE | REUSE | RENAME)    #REQUIRED>
```

Objektimport-Steuerdatei-Parameter

In der folgenden Tabelle finden Sie ein Auflistung der *pmrep*-Objektimport-Steuerdatei-Parameter:

Element	Attributname	Attributbeschreibung
IMPORTPARAMS	CHECKIN_AFTER_IMPORT	Bei Aktivierung der Versionsverwaltung erforderlich. Checkt Objekte nach erfolgreichem Import ein.
IMPORTPARAMS	CHECKIN_COMMENTS	Optional. Wendet die Kommentare auf die eingecheckten Objekte an.
IMPORTPARAMS	APPLY_LABEL_NAME	Optional. Wendet die Beschriftung auf die importierten Objekte an.
IMPORTPARAMS	RETAIN_GENERATED_VALUE	Bei Verwendung von Sequenzgenerator-, Normalisierungsprogramm- oder XML-Quellqualifikator-Transformationen erforderlich. Behält vorhandene Werte der Sequenzgenerator-, Normalisierungsprogramm- oder XML-Quellqualifikator-Transformationen im Ziel bei.
IMPORTPARAMS	COPY_SAP_PROGRAM	Optional. Kopiert SAP-Programminformationen in das Target-Repository.

Element	Attributname	Attributbeschreibung
IMPORTPARAMS	APPLY_DEFAULT_CONNECTION	Optional. Wendet die Standardverbindung an, wenn eine von einer Sitzung verwendete Verbindung im Target-Repository nicht vorhanden ist. Die Standardverbindung ist die erste Verbindung aus der sortierten Liste der verfügbaren Verbindungen. Sucht die Liste der Verbindungen im Workflow Manager.
FOLDERMAP	SOURCEFOLDERNAME	Erforderlich. Importiert den Ordnernamen in Übereinstimmung mit einem Ordner im Target-Repository.
FOLDERMAP	SOURCEREPOSITORYNAME	Erforderlich. Repository mit dem Quellordner.
FOLDERMAP	TARGETFOLDERNAME	Erforderlich. Target-Ordnername für Matching.
FOLDERMAP	TARGETREPOSITORYNAME	Erforderlich. Repository mit dem Target-Ordner.
TYPEFILTER	TYPENAME	Optional. Importiert die Objekte aus einem bestimmten Knoten, z. B. Quellen, Targets oder Mappings.
RESOLVECONFLICT	LABELOBJECT-, QUERYOBJECT-, TYPEOBJECT- UND SPECIFICOBJECT-Elemente.	Sie können Konfliktlösungen für Objekte angeben.
LABELOBJECT	LABELNAME	Erforderlich. Kennzeichnet Objekte nach Beschriftungsname für die Konfliktlösungsspezifikation.
LABELOBJECT	RESOLUTION	Erforderlich. Ersetzen, wiederverwenden, umbenennen.
QUERYOBJECT	QUERYNAME	Erforderlich. Kennzeichnet Objekte aus dieser Abfrage für die Konfliktlösungsspezifikation.
QUERYOBJECT	RESOLUTION	Erforderlich. Ersetzen, wiederverwenden oder umbenennen.
TYPEOBJECT	OBJECTTYPENAME	Erforderlich. Objekttyp für diese Konfliktlösung. Eine Liste mit Objekttypen finden Sie unter "Objektimport-Steuerdatei-Parameter" auf Seite 1239.
TYPEOBJECT	RESOLUTION	Erforderlich. Ersetzen, wiederverwenden oder umbenennen.

Element	Attributname	Attributbeschreibung
SPECIFICOBJECT	NAME	Erforderlich. Spezifischer Objektname für diese Konfliktlösung.
SPECIFICOBJECT	DBDNAME	Optional. Quell-DBD zum Identifizieren des Quellobjekts.
SPECIFICOBJECT	OBJECTTYPENAME	Erforderlich. Objekttyp für diese Konfliktlösung. Eine Liste mit Objekttypen finden Sie unter "Objektimport-Steuerdatei-Parameter" auf Seite 1239.
SPECIFICOBJECT	FOLDERNAME	Erforderlich. Quellordner, der das Objekt enthält.
SPECIFICOBJECT	REPOSITORYNAME	Erforderlich. Quell-Repository, in dem das Objekt enthalten ist.
SPECIFICOBJECT	RESOLUTION	Erforderlich. Ersetzen, wiederverwenden oder umbenennen.

Sie können folgende Objekttypen mit dem OBJECTTYPENAME-Attribut verwenden:

- Alle
- Aggregator
- Anwendungs-Mehrfachgruppen-Quellqualifikator
- Anwendungsquellqualifikator
- Zuweisung
- Befehl
- Kontrolle
- Benutzerdefinierte Umwandlung
- Entscheidung
- E-Mail
- Event-Raise
- Event-Wait
- Ausdruck
- Externe Prozedur
- Filter
- Eingabeumwandlung
- Joiner
- Lookup-Verfahren
- Mapping
- Mapplet
- MQ-Quellqualifikator

- Normalizer
- Ausgabeumwandlung
- Rang
- Router
- Scheduler
- Sitzung
- Sequenz
- SessionConfig
- Sortierer
- Quelldefinition
- Quellqualifikator
- Start
- Zieldefinition
- Timer
- Transaktionssteuerung
- Update-Strategie
- Benutzerdefinierte Funktion
- Arbeitsablauf
- Worklet
- XML-Quellqualifikator

Hinweis: Verwenden Sie den Objekttyp "Alle", um alle Objekte wiederzuverwenden oder zu ersetzen.

Objektimport-Steuerdatei – Beispiele

Die im Code der Steuerdatei von Ihnen angegebenen Parameter bestimmen die Aktionen, die beim Ausführen des Befehls ObjectImport in *pmrep* durchgeführt werden. In den folgenden Beispielen werden Instanzen beschrieben, in denen der Befehl ObjectImport zusammen mit einer Steuerdatei zum Importieren von Repository-Objekten verwendet wird. Die Elemente und Attributnamen, die für die Durchführung der beschriebenen Aufgaben benötigt werden, sind im Code mit Kommentaren gekennzeichnet.

In der folgenden Tabelle werden Beispiele für Objektimport-Steuerdateien beschrieben:

Funktion	Beschreibung
Importieren von Quellobjekten.	Verwenden des Elements TYPEFILTER, um ausschließlich Quellobjekte zu importieren.
Importieren mehrerer Objekte in einen Ordner.	Verwenden der Elemente IMPORTPARAMS und FOLDERMAP, um mehrere Objekte zu importieren.
Einchecken und Beschriften importierter Objekte.	Verwenden der Attribute CHECKIN_AFTER_IMPORT und APPLY_LABEL_NAME des Elements IMPORTPARAMS, um importierte Objekte zu beschriften.

Funktion	Beschreibung
Beibehalten von Werten für Sequenzgenerator- und Normalisierungsprogramm-Transformationen.	Verwenden des Attributs RETAIN_GENERATED_VALUE des Elements IMPORTPARAMS, um Sequenzgenerator- und Normalisierungsprogramm-Werte beim Import von Objekten beizubehalten.
Importieren von Objekten und lokalen Shortcut-Objekten in dasselbe Repository.	Verwenden aller Attribute des Elements FOLDERMAP zum Importieren von Objekten und lokalen Shortcut-Objekten, die auf die Objekte verweisen.
Importieren von Shortcut-Objekten aus einem anderen Repository.	Verwenden aller Attribute des Elements FOLDERMAP, um Shortcut-Objekte aus einem anderen Repository zu importieren.
Importieren von Objekten in mehrere Ordner.	Verwenden aller Attribute des Elements FOLDERMAP zum Importieren von Objekten in mehrere Ordner.
Importieren bestimmter Objekte.	Verwenden des Elements TYPEFILTER zum Importieren bestimmter Objekte.
Erneutes Verwenden und Ersetzen abhängiger Objekte.	Verwenden der Attribute OBJECTTYPENAME und RESOLUTION des Elements TYPEOBJECT, um abhängige Objekte erneut zu verwenden und zu ersetzen.
Ersetzen ungültiger Mappings.	Verwenden des Elements QUERYOBJECT, um ungültige Mappings zu ersetzen.
Umbenennen von Objekten.	Verwenden des Attributs RESOLUTION des Elements SPECIFICOBJECT, um Objekte umzubenennen.
Kopieren von SAP-Mappings und SAP-Programminformationen.	Verwenden des Attributs COPY_SAP_PROGRAM des Elements IMPORTPARAMS, um SAP-Mappings und SAP-Programminformationen zu kopieren.
Anwenden von Standard-Verbindungsattributen.	Verwenden des Attributs APPLY_DEFAULT_CONNECTION des Elements IMPORTPARAMS, um standardmäßige Verbindungsattribute anzuwenden.
Lösen von Objektkonflikten.	Verwenden des Elements RESOLVECONFLICT, um Objektkonflikte zu lösen.

Importieren von Quellobjekten

Quellobjekte können importiert werden. Sie möchten beispielsweise alle doppelten Objekte mit der Bezeichnung "Monatsende" im Zielordner ersetzen. Sie möchten jedoch kollidierende Quellobjekte, die "Jahr_Ende" im Objektnamen enthalten, umbenennen. Sie verfügen über eine Abfrage mit der Bezeichnung "Jahr_ENDE_Abfrage", die diese Objekte findet.

Sie möchten unter Umständen eine Steuerdatei mit den folgenden Attributen erstellen:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">
<IMPORTPARAMS CHECKIN_AFTER_IMPORT ="NO">
<FOLDERMAP SOURCEFOLDERNAME ="OLD_ACCOUNTING"
   SOURCEREPOSITORYNAME ="OLD_REPOS"
   TARGETFOLDERNAME ="NEW_ACCOUNTING"
   TARGETREPOSITORYNAME ="NEW_REPOS"/>

<!-- use the TYPEFILTER element to import only source objects -->
<TYPEFILTER TYPENAME ="SOURCE"/>
<RESOLVECONFLICT>
     <LABELOBJECT LABELNAME ="Monthend"
```

```
    RESOLUTION = "REPLACE"/>
<QUERYOBJECT QUERYNAME ="yr_end_qry"
    RESOLUTION ="RENAME"/>
</RESOLVECONFLICT>
</IMPORTPARAMS>
```

Importieren von mehreren Objekten in einen Ordner

Sie können mehrere Objekte in einen Ordner importieren, diese einchecken und beschriften. Sie möchten beispielsweise die Objekte in Ordner SRC_F1 importieren und die Objekte mit LABEL_IMPORT_NEW beschriften.

Sie möchten unter Umständen eine Steuerdatei mit den folgenden Attributen erstellen:

```
<xml version="1.0" encoding="UTF-16LE"?>
<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">
<!--apply label name LABEL_IMPORT_NEW to imported objects-->
<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES" CHECKIN_COMMENTS="NEWOBJECTS"
APPLY_LABEL_NAME="LABEL_IMPORT_NEW">
<FOLDERMAP SOURCEFOLDERNAME="SRC_F1" SOURCEREPOSITORYNAME="SRC_REPO1"
TARGETFOLDERNAME="TGT_F1" TARGETREPOSITORYNAME="TGT_REPO1"/>
</IMPORTPARAMS>
```

Einchecken der und Beschriften von importierten Objekten

Sie können Objekte in einen Ordner importieren, diese einchecken und beschriften sowie Konflikte zwischen Sitzungskonfigurationsobjekten lösen. Sie möchten beispielsweise die Objekte aus Ordner SRC_F1 exportieren und in Ordner TGT_F1 importieren. Der Repository Service erstellt standardmäßig eine Sitzungskonfiguration im Target-Ordner. Sie schließen das Attribut APPLY_LABEL_NAME in das Element IMPORTPARAMS ein, um die importierten Objekte zu beschriften, und das Element RESOLVECONFLICT in die Steuerdatei, um den Konflikt zu lösen.

Sie möchten unter Umständen eine Steuerdatei mit den folgenden Attributen erstellen:

```
<?xml version="1.0" encoding="UTF-16LE"?>

<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">
<!--enter VERSION1 as the comment for the object you check in-->
<!--apply label name LABEL_IMPORT_NEW to imported objects-->

<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES" CHECKIN_COMMENTS="VERSION1"
APPLY_LABEL_NAME="LABEL_IMPORT_NEW">
<FOLDERMAP SOURCEFOLDERNAME="SRC_F1" SOURCEREPOSITORYNAME="SRC_REPO1"
TARGETFOLDERNAME="TGT_F1" TARGETREPOSITORYNAME="TGT_REPO1"/>
<RESOLVECONFLICT>
<TYPEOBJECT OBJECTTYPENAME="SessionConfig" RESOLUTION="REUSE"/>
</RESOLVECONFLICT>
</IMPORTPARAMS>
```

Beibehalten von Sequenzgenerator- und Normalisierungsprogramm-Werten

Beim Importieren von Objekten und Ersetzen aller Objekte im Zielordner können Sie die Werte von Sequenzgenerator- und Normalisierungsprogramm-Transformationen beibehalten.

Sie möchten unter Umständen eine Steuerdatei mit den folgenden Attributen erstellen:

```
<?xml version="1.0" encoding="UTF-16LE"?>

<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">
<!--enter YES as the value for the RETAIN_GENERATED_VALUE attribute -->
<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES" CHECKIN_COMMENTS="VERSION1"
APPLY_LABEL_NAME="LABEL_IMPORT_NEW" RETAIN_GENERATED_VALUE="YES">w
```

```
<FOLDERMAP SOURCEFOLDERNAME="SRC_F1" SOURCEREPOSITORYNAME="SRC_REPO1"
TARGETFOLDERNAME="TGT_F1" TARGETREPOSITORYNAME="TGT_REPO1"/>
<RESOLVECONFLICT>
<TYPEOBJECT OBJECTTYPENAME="ALL" RESOLUTION="REPLACE"/>
</RESOLVECONFLICT>
</IMPORTPARAMS>
```

Importieren von Objekten und lokalen Shortcut-Objekten zum selben Repository

Sie können Objekte und die zugehörigen lokalen Shortcut-Objekte in dasselbe Repository importieren. Sie verfügen beispielsweise über Ordner mit den Bezeichnungen SRC_SHARED_F1 und SRC_NONSHARED_F1. Der Ordner SRC_NONSHARED_F1 ist nicht freigegeben und enthält lokale Shortcut-Objekte, die auf Objekte im Ordner SRC_SHARED_F1 verweisen. Sie möchten die Objekte in verschiedene Ordner im Target-Repository importieren. Darüber hinaus sollen die Shortcut-Objekte im Ordner TGT_NONSHARED_F1 auf die Objekte im Ordner TGT_SHARED_F1 zeigen.

Sie möchten unter Umständen eine Steuerdatei mit den folgenden Attributen erstellen:

```
<?xml version="1.0" encoding="UTF-16LE"?>

<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">
<IMPORTPARAMS CHECKIN_AFTER_IMPORT="NO">

<!-- import objects from SRC_SHARED_F1 to TGT_SHARED_F1, and shortcut objects from
SRC_NONSHARED_F1 to TGT_NONSHARED_F1-->
<FOLDERMAP SOURCEFOLDERNAME="SRC_SHARED_F1" SOURCEREPOSITORYNAME="SRC__REPO1"
TARGETFOLDERNAME="TGT_SHARED_F1" TARGETREPOSITORYNAME="TGT_REPO1"/>
<FOLDERMAP SOURCEFOLDERNAME="SRC_NONSHARED_F1" SOURCEREPOSITORYNAME="SRC_REPO1"
TARGETFOLDERNAME="TGT_NONSHARED_F1" TARGETREPOSITORYNAME="TGT_REPO1"/>
</IMPORTPARAMS>
```

Importieren von Shortcut-Objekten aus einem anderen Repository

Sie können Objekte aus anderen Repositories importieren. Sie verfügen beispielsweise über Ordner in einem lokalen Repository, das Shortcuts zu Objekten in einem globalen Repository enthält. Sie möchten die globalen Shortcut-Objekte in ein Repository importieren, das im globalen Repository registriert ist, und Shortcuts zu den ursprünglichen Objekten im globalen Repository beibehalten.

Sie möchten unter Umständen eine Steuerdatei mit den folgenden Attributen erstellen:

```
<?xml version="1.0" encoding="UTF-16LE"?>
<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">
<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES" CHECKIN_COMMENTS="global objects"
APPLY_LABEL_NAME="LABEL_IMPORT_GLOBAL_SHORTCUT">

<!--import the shortcut objects from source folder SRC_SHARED_F1 in source repository
SRC_GDR_REPO1 to source folder SRC_SHARED_F1 in target repository SRC_GDR_REPO2 -->

<FOLDERMAP SOURCEFOLDERNAME="SRC_SHARED_F1" SOURCEREPOSITORYNAME="SRC_GDR_REPO1"
TARGETFOLDERNAME="SRC_SHARED_F1" TARGETREPOSITORYNAME="SRC_GDR_REPO2"/>
<FOLDERMAP SOURCEFOLDERNAME="SRC_NONSHARED_F1" SOURCEREPOSITORYNAME="SRC_LDR_REPO1"
TARGETFOLDERNAME="TGT_NONSHARED_F1" TARGETREPOSITORYNAME="SRC_LDR_REPO2"/>
</IMPORTPARAMS>
```

Importieren von Objekten in mehrere Ordner

Sie können Objekte in mehrere Ordner importieren, die aus mehreren Ordnern exportiert wurden. Sie haben beispielsweise Objekte aus den Ordnern SRC_F1, SRC_F2 und SRC_F3 exportiert und möchten sie in die Target-Ordner TGT_F1, TGT_F2, TGT_F3 in Repository TGT_REPO1 importieren.

Sie möchten unter Umständen eine Steuerdatei mit den folgenden Attributen erstellen:

```
<?xml version="1.0" encoding="UTF-16LE"?>

<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">
<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES" CHECKIN_COMMENTS="mulfolders"
APPLY_LABEL_NAME="L1">

<!-- import objects from source folders SRC_F1, SRC_F2, and SRC_F3 to target folders
TGT_F1, TGT_F2, and TGT_F3 in repository TGT_REPO1 -->
<FOLDERMAP SOURCEFOLDERNAME="SRC_F1" SOURCEREPOSITORYNAME="SRC_REPO1"
TARGETFOLDERNAME="TGT_F1 TARGETREPOSITORYNAME="TGT_REPO1"/>
<FOLDERMAP SOURCEFOLDERNAME="SRC_F2" SOURCEREPOSITORYNAME="SRC_REPO2"
TARGETFOLDERNAME="TGT_F2" TARGETREPOSITORYNAME="TGT_REPO1"/>
<FOLDERMAP SOURCEFOLDERNAME="SRC_F3" SOURCEREPOSITORYNAME="SRC_REPO3"
TARGETFOLDERNAME="TGT_F3" TARGETREPOSITORYNAME="TGT_REPO1"/>
   <RESOLVECONFLICT>
<TYPEOBJECT OBJECTTYPENAME = "SESSIONCONFIG" RESOLUTION="REUSE"/>
</RESOLVECONFLICT>

</IMPORTPARAMS>
```

Importieren von spezifischen Objekten

Sie können die Objekte auswählen, die Sie importieren möchten. Sie können beispielsweise mehrere Objekttypen in eine XML-Datei exportieren. Sie möchten nur Mappings und die jeweiligen Quellen und Targets in einen Ordner importieren.

Sie möchten unter Umständen eine Steuerdatei mit den folgenden Attributen erstellen:

```
<?xml version="1.0" encoding="UTF-16LE"?>

<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">
<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES" CHECKIN_COMMENTS="PMREP_IMPORT_TYPEFILTER"
APPLY_LABEL_NAME="LABEL_MAPPING_TYPEFILTER">
<FOLDERMAP SOURCEFOLDERNAME="SRC_F1" SOURCEREPOSITORYNAME="REPO_EX_1"
TARGETFOLDERNAME="TGT_F1" TARGETREPOSITORYNAME="REPO_EX1_"/>

<!-- use the TYPENAME attribute to import only mappings -->
   <TYPEFILTER TYPENAME="MAPPING"/>
</IMPORTPARAMS>
```

Wiederverwenden und Ersetzen von abhängigen Objekten

Sie können Sitzungen importieren, Mappings ersetzen und vorhandene Quellen und Targets im Target-Ordner wiederverwenden. Sie möchten beispielsweise die Mappings ersetzen und die Quelldefinitionen, Target-Definitionen und Sitzungskonfigurationsobjekte wiederverwenden.

Sie möchten unter Umständen eine Steuerdatei mit den folgenden Attributen erstellen:

```
<?xml version="1.0" encoding="UTF-16LE"?>
<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">

<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES" CHECKIN_COMMENTS="PMREP_IMPORT_TYPEFILTER"
APPLY_LABEL_NAME="LABEL_SESSION_TYPEFILTER">
<FOLDERMAP SOURCEFOLDERNAME="PMREP_CHECKED_OUT" SOURCEREPOSITORYNAME="REPO_EX_1"
TARGETFOLDERNAME="PMREP_CHECKED_OUT_IMPORT_TYPEFILTER_SESSION"
TARGETREPOSITORYNAME="REPO_EX_1"/>
   <TYPEFILTER TYPENAME="SESSION"/>
   <RESOLVECONFLICT>

<!-- replace all mappings -->
      <TYPEOBJECT OBJECTTYPENAME = "MAPPING" RESOLUTION="REPLACE"/>

<!-- reuse source definitions, target definitions, and sessionconfigs -->
<TYPEOBJECT OBJECTTYPENAME = "SOURCE DEFINITION" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME = "TARGET DEFINITION" RESOLUTION="REUSE"/>
```

```
<TYPEOBJECT OBJECTTYPENAME = "SESSIONCONFIG" RESOLUTION="REUSE"/>

<!-- replace some object types and reuse remaining objects-->
<TYPEOBJECT OBJECTTYPENAME = "ALL" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME = "SOURCE DEFINITION" RESOLUTION="REPLACE"/>
<TYPEOBJECT OBJECTTYPENAME = "MAPPING" RESOLUTION="REPLACE"/>

</RESOLVECONFLICT>
</IMPORTPARAMS>
```

Hinweis: Wenn Sie einen Objekttyp wiederverwenden oder ersetzen, überschreibt die Auflösung für diesen Objekttyp die Auflösung für alle Objekttypen. Im vorangehenden Beispiel werden Quelldefinitionen und Mappings ersetzt und die übrigen Objekte wiederverwendet. Verwenden Sie den Objekttyp "Alle", um alle Objekte wiederzuverwenden oder zu ersetzen. Weitere Informationen zu Objekttypen finden Sie unter “Objektimport-Steuerdatei-Parameter” auf Seite 1239.

Ersetzen ungültiger Mappings

Sie können ungültige Mappings sowie die zugehörigen untergeordneten Objekte ersetzen, die von einer Abfrage zurückgegeben wurden. Sie möchten beispielsweise Objekte ersetzen, die von der Abfrage QUERY_PARENT_RENAME zurückgegeben wurden.

Sie möchten unter Umständen eine Steuerdatei mit den folgenden Attributen erstellen:

```
<?xml version="1.0" encoding="UTF-16LE"?>
<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">

<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES"

CHECKIN_COMMENTS="PMREP_IMPORT_QUERY_PARENT_REPLACE_CHILD_REUSE"
APPLY_LABEL_NAME="LABEL_QUERY_PARENT_RENAME_CHILD_REUSE">
   <FOLDERMAP SOURCEFOLDERNAME="PMREP_CHECKED_OUT" 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>
```

Umbenennen von Objekten

Sie können bestimmte Objekte umbenennen, wenn bei Objekten Konflikte auftreten. Sie möchten beispielsweise die Objekte ADDRESS, ADDRESS1, R_LKP, MAP_MLET, R_S3, WF_RS1 umbenennen. Der Repository Service hängt eine Zahl an den Objektnamen an.

Sie möchten unter Umständen eine Steuerdatei mit den folgenden Attributen erstellen:

```
<?xml version="1.0" encoding="UTF-16LE"?>

<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">

<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES"
CHECKIN_COMMENTS="PMREP_IMPORT_SPECIFICOBJECT_RENAME"
APPLY_LABEL_NAME="LABEL_IMPORT_SPECIFIC_OBJECT_RENAME">
<FOLDERMAP SOURCEFOLDERNAME="SRC_FOLDER1" 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" OBJECTTYPENAME="Source Definition"
FOLDERNAME="PMREP_CHECKED_OUT" REPOSITORYNAME="REPO_EX_1" RESOLUTION="RENAME"/>
<SPECIFICOBJECT NAME="ADDRESS1" OBJECTTYPENAME="Target Definition"
```

```
FOLDERNAME="PMREP_CHECKED_OUT" REPOSITORYNAME="REPO_EX_1" RESOLUTION="RENAME"/>
<SPECIFICOBJECT NAME="R_LKP" OBJECTTYPENAME="Lookup Procedure"
FOLDERNAME="PMREP_CHECKED_OUT" REPOSITORYNAME="REPO_EX_1" RESOLUTION="RENAME"/>
<SPECIFICOBJECT NAME="MAP_MLET" OBJECTTYPENAME="Mapping" FOLDERNAME="PMREP_CHECKED_OUT"
REPOSITORYNAME="REPO_EX_1" RESOLUTION="RENAME"/>
<SPECIFICOBJECT NAME="R_S3" OBJECTTYPENAME="Session" FOLDERNAME="PMREP_CHECKED_OUT"
REPOSITORYNAME="REPO_EX_1" RESOLUTION="RENAME"/>
<SPECIFICOBJECT NAME="WF_RS1" OBJECTTYPENAME="Workflow" FOLDERNAME="PMREP_CHECKED_OUT"
REPOSITORYNAME="REPO_EX_1" RESOLUTION="RENAME"/>
</RESOLVECONFLICT></IMPORTPARAMS>
```

Kopieren von SAP-Mappings und SAP-Programminformationen

Sie können SAP-Programminformationen beim Importieren von SAP-Mappings kopieren. Sie möchten beispielsweise SAP-Mappings importieren und die Programminformationen kopieren, die dem in den Ordner TGT_F1 zu importierenden Objekt zugeordnet sind.

Sie möchten unter Umständen eine Steuerdatei mit den folgenden Attributen erstellen:

```
<?xml version="1.0" encoding="UTF-16LE"?>

<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">

<!-- enter YES as the value for the COPY_SAP_PROGRAM attribute to copy SAP mappings and
SAP program information -->

<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES" CHECKIN_COMMENTS="Version2 of objects"
APPLY_LABEL_NAME="LABEL71_REPLACE_FOLDER" COPY_SAP_PROGRAM="YES">
   <FOLDERMAP SOURCEFOLDERNAME="SRC_F1" SOURCEREPOSITORYNAME="REPO_EX_1"
TARGETFOLDERNAME="TGT_F1" TARGETREPOSITORYNAME="REPO_EX_1"/>
</IMPORTPARAMS>
```

Anwenden von Standard-Verbindungsattributen

Sie können ein standardmäßiges Verbindungsattribut auf eine Sitzung anwenden, wenn im Target-Repository keine Verbindung existiert. Im Target-Repository REPO_EX_1 existiert beispielsweise keine Verbindung.

Sie möchten unter Umständen eine Steuerdatei mit den folgenden Attributen erstellen:

```
<?xml version="1.0" encoding="UTF-16LE"?>
<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">

<!-- enter YES as the value of the APPLY_DEFAULT_CONNECTION element to apply a default
connection attribute -->
<IMPORTPARAMS CHECKIN_AFTER_IMPORT="NO" APPLY_DEFAULT_CONNECTION="YES">
   <FOLDERMAP SOURCEFOLDERNAME="SRC_F1" SOURCEREPOSITORYNAME="REPO_EX_1"
TARGETFOLDERNAME="TGT_F1" TARGETREPOSITORYNAME="REPO_EX_1"/>
<RESOLVECONFLICT>
<SPECIFICOBJECT NAME="R_S3" OBJECTTYPENAME="Session" FOLDERNAME="PMREP_CHECKED_OUT"
REPOSITORYNAME="REPO_EX_1" RESOLUTION="REPLACE"/>
<RESOLVECONFLICT>
</IMPORTPARAMS>
```

Auflösen von Objektkonflikten

Sie können Objektkonflikte für beschriftete Objekte im Target-Repository auflösen. Sie verfügen beispielsweise über Mappings, Mapplets, Quellen und Targets mit der Beschriftung LBL_MPNG_MPLTS_SRCS_TGTS. Sie möchten diese Objekte ersetzen, mit der Beschriftung REPLACE_LBL_MPNG_MPLTS_SRCS_TGTS versehen und alle Transformationen wiederverwenden.

Sie möchten unter Umständen eine Steuerdatei mit den folgenden Attributen erstellen:

```
<?xml version="1.0" encoding="UTF-16LE"?>

<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">
```

```
<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES" CHECKIN_COMMENTS="PMREP_IMPORT_LABEL_REPLACE"
APPLY_LABEL_NAME="REPLACE_LBL_MPNG_MPLTS_SRCS_TGTS" >
<FOLDERMAP SOURCEFOLDERNAME="SRC_F1" SOURCEREPOSITORYNAME="REPO_EX_1"
TARGETFOLDERNAME="TGT_F1" TARGETREPOSITORYNAME="REPO_EX_1"/>

<!-- use the RESOLVECONFLICT element in conjunction with the RESOLUTION attribute of the
OBJECTTYPENAME element to resolve conflicts when you import objects -->
   <RESOLVECONFLICT>
<LABELOBJECT LABELNAME="LBL_MPNG_MPLTS_SRCS_TGTS" RESOLUTION="REPLACE"/>
<TYPEOBJECT OBJECTTYPENAME="Lookup Procedure" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME="Stored Procedure" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME="Expression" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME="Filter" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME="Aggregator" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME="Rank" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME="Normalizer" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME="Router" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME="Sequence" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME="Sorter" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME="update strategy" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME="Custom Transformation" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME="Transaction control" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME="External Procedure" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME="Joiner" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME="SessionConfig" RESOLUTION="REUSE"/>
</RESOLVECONFLICT>

</IMPORTPARAMS>
```

Verwenden der Bereitstellungssteuerdatei

Eine Bereitstellungssteuerdatei ist eine XML-Datei, die Sie mit den *pmrep*-Befehlen "DeployFolder" und "DeployDeploymentGroup" verwenden, um einen Ordner oder eine Bereitstellungsgruppe bereitzustellen. Sie können eine Bereitstellungssteuerdatei manuell erstellen, um Parameter für die Bereitstellung anzugeben. Sie können sie aber auch mit dem Kopierassistenten erstellen.

Wenn Sie die Bereitstellungssteuerdatei manuell erstellen, muss sie der depcntl.dtd-Datei entsprechen, die mit dem PowerCenter Client installiert wird. Sie nehmen den Speicherort der depcntl.dtd-Datei in der Bereitstellungssteuerdatei auf.

Sie können in der Bereitstellungssteuerdatei einen Bereitstellungs-Timeout angeben. Der Bereitstellungs-Timeout ist der Zeitraum, den *pmrep* wartet, um Objektsperren im Target-Repository abzurufen. Standardmäßig wartet *pmrep* unbegrenzt, bis Sperren abgerufen werden oder Sie brechen die Bereitstellung ab. Wenn Sie eine Bereitstellung abbrechen möchten, während *pmrep* auf das Abrufen von Sperren wartet, drücken Sie Strg+C.

Hinweis: Sie müssen die Bereitstellungssteuerdatei manuell erstellen, um einige Bereitstellungsparameter wie DEPLOYTIMEOUT zu verwenden.

Im Folgenden sehen Sie ein Beispiel für eine depcntl.dtd-Datei:

```
<!ELEMENT DEPLOYPARAMS (DEPLOYFOLDER?, DEPLOYGROUP?)>
<!ATTLIST DEPLOYPARAMS
        DEFAULTSERVERNAME    CDATA      #IMPLIED
        COPYPROGRAMINFO      (YES | NO) "YES"
        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">

<!--criteria specific to deploying folder-->
<!ELEMENT DEPLOYFOLDER (REPLACEFOLDER?, DEPLOYEDFOLDEROWNER?, OVERRIDEFOLDER*)>
<!ATTLIST DEPLOYFOLDER
        NEWFOLDERNAME         CDATA      #IMPLIED>

<!--folder to replace-->
<!ELEMENT REPLACEFOLDER EMPTY>
<!ATTLIST REPLACEFOLDER
        FOLDERNAME            CDATA      #REQUIRED
        RETAINMAPVARPERVALS   (YES | NO) "NO"
        RETAINWFLOWVARPERVALS (YES | NO) "YES"
        RETAINWFLOWSESSLOGS   (YES | NO) "NO"
        MODIFIEDMANUALLY      (YES | NO) "NO"
        RETAINORIGFOLDEROWNER (YES | NO) "NO">

<!--shared folder to override-->
<!ELEMENT OVERRIDEFOLDER EMPTY>
<!ATTLIST OVERRIDEFOLDER
        SOURCEFOLDERNAME    CDATA            #REQUIRED
        SOURCEFOLDERTYPE    (LOCAL | GLOBAL) "LOCAL"
        TARGETFOLDERNAME    CDATA            #REQUIRED
        TARGETFOLDERTYPE    (LOCAL | GLOBAL) "LOCAL"
        MODIFIEDMANUALLY    (YES | NO)     "NO"

<!--criteria specific to deploy deployment group-->
<!ELEMENT DEPLOYGROUP (REPLACEDG?, TARGETDGOWNER?, OVERRIDEFOLDER*, APPLYLABEL?)>
<!ATTLIST DEPLOYGROUP
        CLEARSRCDEPLOYGROUP (YES | NO) "NO">
        NEWDEPLOYGROUPNAME   CDATA  #IMPLIED

<!--labels used to apply on the src objects and deployed objects-->
<!ELEMENT APPLYLABEL EMPTY>
<!ATTLIST APPLYLABEL
        SOURCELABELNAME     CDATA            #IMPLIED
        SOURCEMOVELABEL         (YES | NO)          "NO"
        TARGETLABELNAME     CDATA            #IMPLIED
        TARGETMOVELABEL             (YES | NO)          "NO">

<!-- new owners of deployed folders -->
<!ELEMENT DEPLOYEDFOLDEROWNER EMPTY>
<!ATTLIST DEPLOYEDFOLDEROWNER
        USERNAME         CDATA        #IMPLIED
                    SECURITYDOMAIN   CDATA        #IMPLIED
        GROUPNAME        CDATA #IMPLIED>

<!-- to indicate that a deployment group should be replaced-->
<!ELEMENT REPLACEDG EMPTY>
<!ATTLIST REPLACEDG
        DGNAME          CDATA        #REQUIRED
                    SECURITYDOMAIN   CDATA        #IMPLIED

<!-- new owner of copied deployment group-->
<!ELEMENT TARGETDGOWNER EMPTY>
<!ATTLIST TARGETDGOWNER
        USERNAME         CDATA        #IMPLIED
                    SECURITYDOMAIN   CDATA        #IMPLIED
```

Bereitstellungs-Steuerdatei-Parameter

In der folgenden Tabelle finden Sie eine Auflistung mit *pmrep*-Bereitstellungs-Steuerdatei-Parametern:

Element	Attributname	Attributbeschreibung
DEPLOYPARAMS (Mit DeployFolder und DeployDeploymentGroup verwenden)	DEFAULTSERVERNAME	Optional. Der Integrationsdienst ist im Ziel-Repository zur Ausführung von Arbeitsabläufen registriert. Für Bereitstellungen können Sie einen Standardservernamen angeben.
-	COPYPROGRAMINFO	Optional. Kopiert das mit SAP installierte ABAP-Programm.
-	COPYMAPVARPERVALS	Optional. Kopiert persistente Werte für die Zuordnungsvariable.
-	RETAINMAPVARPERVALS	Optional. Behält persistente Werte für die Zuordnungsvariable im Ziel bei.
-	COPYWFLOWVARPERVALS	Optional. Kopiert persistente Werte für die Arbeitsablaufvariable.
-	COPYWFLOWSESSLOGS	Optional. Kopiert Arbeitsablaufprotokolle.
-	COPYDEPENDENCY	Optional. Kopiert Abhängigkeitsinformationen für Objekte in Zuordnungen.
-	COPYDEPLOYMENTGROUP	Optional. Kopiert die Bereitstellungsgruppe zusammen mit den Objekten in der Bereitstellungsgruppe in das Ziel-Repository.
-	VALIDATETARGETREPOSITORY	Optional. Validiert Objekte im Ziel-Repository.
-	LATESTVERSIONONLY	Optional. Kopiert die neueste Version.
-	CHECKIN_COMMENTS	Optional. Überschreibt den Standardkommentar und fügt einen Kommentar im Ziel-Repository beim Kopieren oder Bereitstellen eines Objekts hinzu. Sie müssen LATESTVERSIONONLY auf TRUE festlegen, um dieses Attribut zu verwenden.
-	DEPLOYTIMEOUT	Optional. Zeitraum (in Sekunden), in dem *pmrep* versucht, Sperren für Objekte im Ziel-Repository abzurufen. Bei einem Wert von 0 schlägt der Kopiervorgang sofort fehl, wenn *pmrep* keine Sperre erhält. Der Wert -1 weist *pmrep* an, so lange zu warten, bis die Sperren übermittelt werden oder der Benutzer den Vorgang abbricht. Standardwert ist -1.

Element	Attributname	Attributbeschreibung
-	RETAINGENERATEDVAL	Optional. Speichert den aktuellen Wert für Sequenzgenerator- oder Normalisierungsumwandlungen.
-	RETAINSERVERNETVALS	Optional. Behält Werte, die sich auf das Netzwerk oder den Server beziehen, in Aufgaben bei.
DEPLOYFOLDER (Mit DeployFolder verwenden)	NEWFOLDERNAME	Optional. Erstellt einen Ordner mit diesem Namen.
REPLACEFOLDER (Mit DeployFolder verwenden)	FOLDERNAME	Erforderlich. Benennt den Ordner, nachdem dieser ersetzt wurde.
-	RETAINMAPVARPERVALS	Optional. Behält persistente Werte für die Zuordnungsvariable im Ziel bei.
-	RETAINWFLOWVARPERVALS	Optional. Behält persistente Werte für Arbeitsablaufvariablen bei.
-	RETAINWFLOWSESSLOGS	Optional. Behält Sitzungsprotokolle des Arbeitsablaufs im Ziel bei.
-	MODIFIEDMANUALLY	Optional. Vergleicht Ordner, wenn Objekte im Zielordner seit der letzten Bereitstellung erstellt oder geändert wurden.
-	RETAINORIGFOLDEROWNER	Optional. Behält den vorhandenen Ordnereigentümer bei. *pmrep* ignoriert alle im DEPLOYEDFOLDEROWNER-Element bereitgestellten Informationen.
OVERRIDEFOLDER (Mit DeployFolder und DeployDeploymentGroup verwenden)	SOURCEFOLDERNAME	Erforderlich. Bei der Bereitstellung eines Ordners wird der aktuelle Ordner angegeben, auf den die Shortcuts zeigen. Bei der Bereitstellung einer Bereitstellungsgruppe werden die folgenden Ordner angegeben: - Ein oder mehrere Ordner, auf den bzw. die die Shortcuts zeigen - Ein oder mehrere Ordner mit den Bereitstellungsgruppenobjekten
-	SOURCEFOLDERTYPE	Optional. Bei der Bereitstellung eines Ordners wird der Ordnertyp angegeben, auf den die Shortcuts zeigen. Verwenden Sie lokale oder globale Shortcuts.

Element	Attributname	Attributbeschreibung
-	TARGETFOLDERNAME	Erforderlich. Bei der Bereitstellung eines Ordners wird der Ordner angegeben, auf den die Shortcuts zeigen. Bei der Bereitstellung einer Bereitstellungsgruppe werden die folgenden Ordner angegeben: - Ein oder mehrere Ordner, auf den bzw. die die Shortcuts zeigen - Ein oder mehrere Ordner mit den Bereitstellungsgruppenobjekten
-	TARGETFOLDERTYPE	Optional. Bei der Bereitstellung eines Ordners wird der Ordnertyp angegeben, auf den die Shortcuts zeigen. Verwenden Sie lokale oder globale Shortcuts.
-	MODIFIEDMANUALLY	Optional. Vergleicht Ordner, wenn Objekte im Zielordner seit der letzten Bereitstellung erstellt oder geändert wurden. Verwenden Sie dieses Attribut nur mit dem DeployDeploymentGroup-Befehl.
DEPLOYGROUP (Mit DeployDeploymentGroup verwenden)	CLEARSRCDEPLOYGROUP	Optional. Entfernt nach der Bereitstellung Objekte aus der Quellgruppe.
-	NEWDEPLOYGROUPNAME	Optional. Erstellt eine Bereitstellungsgruppe mit diesem Namen. Wird bei Angabe von REPLACEDG ignoriert. Standardwert ist der Name der Quellbereitstellungsgruppe.
REPLACEDG	DGNAME	Optional. Name der zu ersetzenden Bereitstellungsgruppe.
-	RETAINORIGINALOWNER	Optional. Gibt an, ob der Eigentümer der Bereitstellungsgruppe, die im Ziel-Repository ersetzt wurde, beibehalten werden soll.
TARGETDGOWNER	USERNAME	Optional. Eigentümer der kopierten Bereitstellungsgruppe. Standardwert ist der Eigentümer der Quellbereitstellungsgruppe.
-	SECURITYDOMAIN	Optional. Sicherheitsdomäne der Zielbereitstellungsgruppe.
APPLYLABEL (Mit DeployDeploymentGroup verwenden)	SOURCELABELNAME	Optional. Wendet eine Beschriftung auf alle Objekte in der Quellgruppe an.

Element	Attributname	Attributbeschreibung
-	SOURCEMOVELABEL	Optional. Verschiebt die Beschriftung aus einer anderen Version des Objekts in der Quellgruppe in die Bereitstellungsgruppenversion des Objekts. Wenn der Repository Agent feststellt, dass die Beschriftung auf eine andere Version desselben Objekts angewendet wird, können Sie die Beschriftung in die ausgewählte Version des Objekts verschieben.
-	TARGETLABELNAME	Optional. Wendet eine Beschriftung auf alle im Ziel-Repository bereitgestellten Objekte an.
-	TARGETMOVELABEL	Optional. Verschiebt die Beschriftung aus einer anderen Version des Objekts in der Zielgruppe in die Bereitstellungsgruppenversion des Objekts. Wenn der Repository Agent feststellt, dass die Beschriftung auf eine andere Version desselben Objekts angewendet wird, können Sie die Beschriftung in die aktuelle Version des Objekts verschieben.
DEPLOYEDFOLDEROWNER (Mit DeployFolder und DeployDeploymentGroup verwenden)	USERNAME	Optional. Eigentümer des bereitgestellten Ordners oder der Bereitstellungsgruppe im Ziel-Repository.
-	SECURITYDOMAIN	Optional. Name der Sicherheitsdomäne, der der Eigentümer des bereitgestellten Ordners oder der Bereitstellungsgruppe angehört.
-	GROUPNAME	Optional. Gruppeneigentümer des bereitgestellten Ordners oder der Bereitstellungsgruppe im Ziel-Repository.

Bereitstellungs-Steuerdatei – Beispiele

Die im Code der Bereitstellungs-Steuerdatei angegebenen Parameter bestimmen die Aktionen, die stattfinden, wenn Sie die Befehle DeployFolder oder DeployDeploymentGroup in *pmrep* ausführen. Die folgenden Beispiele behandeln Instanzen, in denen die Befehle DeployFolder und DeployDeploymentGroup mit einer Bereitstellungs-Steuerdatei verwendet werden.

Bereitstellen der aktuellen Version eines Ordners

Sie können die aktuelle Version eines Ordners bereitstellen und alle Abhängigkeiten einschließen. Sie müssen beispielsweise die aktuellen Werte in einer Sequenzgenerator-Transformation beibehalten und die Shortcuts

für den Ordner "sc_folder" auf den Ordner "new_sc_folder" anpassen. Nach dem Kopieren des Ordners möchten Sie ihn in "new_year" umbenennen.

Sie möchten unter Umständen eine Steuerdatei mit folgenden Attributen erstellen:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE DEPLOYPARAMS SYSTEM "depcntl.dtd">
<DEPLOYPARAMS DEFAULTSERVERNAME ="info7261"
  COPYPROGRAMINFO ="NO"
  COPYWFLOWVARPERVALS ="NO"
  COPYWFLOWSESSLOGS ="NO"
  COPYDEPENDENCY ="YES"
  LATESTVERSIONONLY = "NO">

<REPLACEFOLDER FOLDERNAME ="NEW_YEAR"
   RETAINMAPVARPERVALS ="YES"/>

<OVERRIDEFOLDER SOURCEFOLDERNAME ="SC_FOLDER"
   OVERRIDEFOLDERNAME ="NEW_SC_FOLDER"/>

</DEPLOYPARAMS>
```

Bereitstellen der aktuellen Version einer Bereitstellungsgruppe

Sie können die aktuelle Version einer Bereitstellungsgruppe bereitstellen und die Objekte in der Bereitstellungsgruppe mit einer Beschriftung versehen. Sie möchten beispielsweise die Beschriftung NEW_SRC_LABEL_NAME auf alle Objekte in der Quellgruppe und die Beschriftung NEW_TGT_LABEL_NAME auf alle Objekte in der Target-Gruppe anwenden. Sie möchten unter Umständen eine Steuerdatei mit folgenden Attributen erstellen:

```
<?xml version="1.0" encoding="UTF-16LE"?>
<!DOCTYPE DEPLOYPARAMS SYSTEM "depcntl.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>
```

Auflisten mehrerer Quell- und Target-Ordner

Verwenden Sie das Element OVERRIDEFOLDER in der Steuerdatei, um mehrere Quell- und Target-Ordner aufzulisten. Verwenden Sie die Attribute SOURCEFOLDERNAME und TARGETFOLDERNAME, um die folgenden Ordner in den Quell- und Target-Repositories anzugeben:

- Der oder die Ordner, auf den bzw. die die Shortcuts zeigen
- Der oder die Ordner, in dem bzw. denen die Bereitstellungsgruppenobjekte enthalten sind

Beim Ausführen des Befehls *pmrep* DeployDeploymentGroup, verwendet der Bereitstellungsvorgang den rechten Target-Ordner, nachdem die Objekte in der Bereitstellungsgruppe überprüft wurden.

Wenn eine Bereitstellungsgruppe beispielsweise Objekte in zwei Ordnern mit Shortcuts zu einem dritten Ordner enthält, können Sie eine Steuerdatei mit drei Vorkommen von OVERRIDEFOLDER erstellen. Die folgende Beispielsteuerdatei stellt eine Bereitstellungsgruppe bereit, die Objekte in den Ordnern OBJECTFOLDER1 und OBJECTFOLDER2 enthält, in denen Shortcuts enthalten sind, die auf den Ordner SHAREDSHORTCUT zeigen.

```
<!DOCTYPE DEPLOYPARAMS SYSTEM "depcntl.dtd">
<DEPLOYPARAMS DEFAULTSERVERNAME="dg_sun_71099"
   COPYPROGRAMINFO="YES"
   COPYMAPVARPERVALS="YES"
   COPYWFLOWVARPERVALS="YES"
   COPYWFLOWSESSLOGS="NO"
   COPYDEPENDENCY="YES"
   LATESTVERSIONONLY="YES"
   RETAINGENERATEDVAL="YES"
   RETAINSERVERNETVALS="YES">
<DEPLOYGROUP CLEARSRCDEPLOYGROUP="NO">
<OVERRIDEFOLDER SOURCEFOLDERNAME="OBJECTFOLDER1"
   SOURCEFOLDERTYPE="LOCAL"
   TARGETFOLDERNAME="OBJECTFOLDER1"
   TARGETFOLDERTYPE="LOCAL"/>
<OVERRIDEFOLDER SOURCEFOLDERNAME="OBJECTFOLDER2"
   SOURCEFOLDERTYPE="LOCAL"
   TARGETFOLDERNAME="OBJECTFOLDER2"
   TARGETFOLDERTYPE="LOCAL"/>
<OVERRIDEFOLDER SOURCEFOLDERNAME="SHAREDSHORTCUTS"
   SOURCEFOLDERTYPE="GLOBAL"
   TARGETFOLDERNAME="SHAREDSHORTCUTS"
   TARGETFOLDERTYPE="GLOBAL"/>
</DEPLOYGROUP>
</DEPLOYPARAMS>
```

Tipps für die Arbeit mit pmrep-Dateien

Verwenden Sie die Option -n, wenn Sie die *pmrep*-Befehle "Updatesrcprefix" oder "Updatetargprefix" verwenden.

Wenn Sie die Option -n angeben, müssen Sie den Namen der Quell- oder Target-Instanz für die Option -t eingeben. Der Quell- oder Target-Instanzname muss mit dem in den Sitzungseigenschaften angezeigten Namen oder dem vom Listtablesbysess-Befehl ausgegebenen Namen übereinstimmen.

Geben Sie die Option -n an, um den Listtablesbysess-Befehl mit dem Updatesrcprefix- oder dem Updatetargprefix-Befehl in einem Shell-Skript zu verwenden, wenn Quell- und Target-Instanznamen nicht übereinstimmen. Geben Sie außerdem die Option -n zum Aktualisieren einer Quelle an, selbst wenn die Sitzung einen Shortcut zum Mapping verwendet.

Geben Sie beim Verwenden des *pmrep* ListObjects-Befehls ein Zeichen oder eine Zeichenfolge ein, das bzw. die in Repository-Objektnamen nicht als Spaltentrennzeichen, Satzendekennzeichen oder Endekennzeichen der Auflistung verwendet wird.

Wenn Sie Zeichen eingeben, um Datensätze und Spalten zu trennen und das Ende einer Auflistung zu kennzeichnen, verwenden Sie Zeichen, die nicht in Repository-Objektnamen enthalten sind. Dies hilft bei der Verwendung eines Shell-Skripts zum Parsen der Objektmetadaten.

Verwenden Sie in *pmrep* die Option -v, wenn Sie ein Repository wiederherstellen, das einen externen Verzeichnisdienst für die Benutzerverwaltung einsetzt.

Wenn Sie die Option -v mit Restore verwenden, können Sie die externe Verzeichnisdienstregistrierung für das Repository beibehalten. Wenn Sie diese Option nicht mit dem gültigen Administratorbenutzernamen und -passwort eingeben, wird standardmäßig der Repository-Authentifizierungmodus für das wiederhergestellte Repository verwendet und die Zuordnungen zwischen Anmeldenamen und Benutzernamen gehen verloren.

ANHANG A

Veraltete Befehle

Dieser Anhang umfasst die folgenden Themen:

- Veraltete Befehle - Übersicht, 1258
- BackupDARepositoryContents (veraltet), 1259
- CreateDARepositoryContents (veraltet), 1260
- CreateReportingService (veraltet), 1262
- DeleteDARepositoryContents (veraltet), 1267
- RestoreDARepositoryContents (veraltet), 1269
- UpdateReportingService (veraltet), 1271
- UpgradeDARepositoryContents (veraltet), 1272
- UpgradeDARepositoryUsers (veraltet), 1274

Veraltete Befehle - Übersicht

Ab Version 10.1 hat Informatica den Berichterstellungs- und Dashboard-Dienst sowie die Data Analyzer-Befehle als veraltet klassifiziert. Informatica wird die Unterstützung für den Berichterstellungs- und Dashboard-Dienst sowie die Data Analyzer-Befehle in einer zukünftigen Version einstellen.

Wenn Sie auf Version 10.1 aktualisieren, können Sie den Berichterstellungs- und Dashboard-Dienst oder den Berichterstellungsdienst weiterhin verwenden. Informatica empfiehlt Benutzern, Berichterstellungstools von Drittanbietern zu verwenden, bevor die Unterstützung eingestellt wird. Wenn Sie JasperReports zur Erstellung von Berichten verwendet haben, können Sie eine Lizenz von JasperSoft erwerben, um die Berichte weiterhin ausführen zu können, wenn Informatica die Unterstützung einstellt.

Wenn Sie Version 10.1 installieren, können Sie keinen Berichterstellungs- und Dashboard-Dienst oder Berichterstellungsdienst erstellen. Sie müssen das Berichterstellungstool eines Drittanbieters verwenden, um PowerCenter- und Metadata Manager-Berichte auszuführen.

Weitere Informationen zu PowerCenter-Berichten finden Sie im *Informatica PowerCenter-Handbuch unter „Verwenden von PowerCenter-Berichten“*. Weitere Informationen zu den Ansichten des PowerCenter-Repositorys finden Sie im *Informatica PowerCenter-Repository-Handbuch*. Informationen zu den Metadata Manager-Repository-Ansichten finden Sie in der *Informatica Metadata Manager-Ansichtsreferenz*.

BackupDARepositoryContents (veraltet)

Sichert den Inhalt für ein Data Analyzer-Repository in einer binären Datei. Wenn Sie den Inhalt sichern, speichert der Berichterstellungsdienst das Data Analyzer-Repository. Dazu zählen die Repository-Objekte, Verbindungsinformationen und Codepage-Informationen. Führen Sie infacmd isp RestoreDARepositoryContents aus, um den Repository-Inhalt wiederherzustellen.

Der Befehl „infacmd isp BackupDARepositoryContents“ verwendet die folgende Syntax:

```
BackupDARepositoryContents

<-DomainName|-dn> domain_name

<-UserName|-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

<-fileName|-f> file_name

[<-overwrite|-o> overwrite_file]
```

In der folgenden Tabelle werden Optionen und Argumente für „infacmd isp BackupDARepositoryContent“ beschrieben:

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

Option	Argument	Beschreibung
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des Berichterstellungsdiensts, für den Sie Inhalte sichern möchten.
-fileName -f	file_name	Erforderlich. Name und Dateipfad für die Erstellung der Backup-Datei.
-overwrite -o	overwrite_file	Überschreibt die Backup-Datei, wenn eine Datei mit demselben Namen bereits vorhanden ist. Erforderlich, wenn eine Datei mit demselben Namen vorhanden ist.

CreateDARepositoryContents (veraltet)

Erstellt Inhalt für ein Data Analyzer-Repository. Sie fügen Repository-Inhalt hinzu, wenn Sie den Berichterstellungsdienst erstellen oder den Repository-Inhalt löschen. Sie können keinen Inhalt für ein Repository erstellen, das bereits Inhalt aufweist.

Der Befehl „infacmd isp CreateDARepositoryContents“ verwendet die folgende Syntax:

```
CreateDARepositoryContents

<-DomainName|-dn> domain_name

<-UserName|-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

<-initialAdmin|-ia> initial_administrator
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp CreateDARepositoryContents“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des Diensts, für den Sie Inhalt erstellen möchten.
-initialAdmin -ia	initial_administrator	Erforderlich. Name des Administrators für den Berichterstellungsdienst.

CreateReportingService (veraltet)

Erstellt einen Berichterstellungsdienst in der Domäne. führen Sie infacmd EnableService aus, um den Berichterstellungsdienst zu aktivieren.

Der Befehl „infacmd isp CreateReportingService“ verwendet die folgende Syntax:

```
CreateReportingService

<-DomainName|-dn> domain_name

<-UserName|-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

[<-FolderPath|-fp> full_folder_path]

<-ServiceOptions|-so> option_name=value ...

<-ReportingSource|-rs> option_name=value ...

[<-LineageService|-ls> option_name=value ...]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp CreateReportingService“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des Berichterstellungsdiensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf maximal 79 Zeichen und weder voran- bzw. nachgestellte Leerzeichen, Wagenrückläufe oder Tabulatoren noch die folgenden Zeichen enthalten: `/ * ? < > " |`
-NodeName -nn	node_name	Erforderlich. Name des Knotens, auf dem der Berichterstellungsdienst-Prozess ausgeführt werden soll.
-LicenseName -ln	license_name	Erforderlich. Name der Lizenz, die Sie dem ReportingService zuweisen möchten.
-FolderPath -fp	full_folder_path	Optional. Vollständiger Pfad (ohne Domänenname) des Ordners, in dem Sie den Berichterstellungsdienst erstellen möchten. Folgendes Format ist erforderlich: */parent_folder/child_folder* Standardwert ist „/“ (die Domäne).
-ServiceOptions -so	option_name=value	Erforderlich. Diensteigenschaften, mit denen definiert wird, wie der Berichterstellungsdienst ausgeführt wird.
-ReportingSource -rs	option_name=value	Erforderlich. Geben Sie den Namen und Typ der Datenquelle an.
-LineageService -ls	option_name=value	Optional. Für die Ausführung von Lineage-Analysen für Daten in Data Analyzer erforderliche Lineage-Eigenschaften.

Reporting Service-Optionen

Geben Sie Reporting Service-Optionen im folgenden Format ein:

```
infacmd CreateReportingService ... -so option_name=value option_name=value ...
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Reporting Service-Optionen beschrieben:

Option	Beschreibung
AdditionalJdbcParams	Optional. Geben Sie weitere JDBC-Optionen ein. Verwenden Sie diese Option, um die Zeichenkodierung oder den Speicherort eines Servers anzugeben, wenn Sie einen hochverfügbaren Datenbankserver wie z. B. Oracle RAC verwenden.
DatabaseDriver	Erforderlich. JDBC-Treiber, den der Reporting Service verwendet, um eine Verbindung mit der Data Analyzer Repository-Datenbank herzustellen.
DatabaseHost	Erforderlich. Name des Computers, der als Host für den Datenbankserver eingesetzt ist.
DatabaseName	Erforderlich. Vollständiger Dienstname oder SID für Oracle-Datenbanken. Dienstname für IBM DB2-Datenbanken. Datenbankname für Microsoft SQL Server- oder Sybase ASE-Datenbanken. Verwenden Sie die DatabaseNameInterpretation-Option, um festzulegen, ob die DatabaseName-Option einen Dienstnamen, eine SID oder einen Datenbanknamen enthält.
DatabaseNameInterpretation	Erforderlich, wenn die DatabaseName-Option einen vollständigen Oracle-Dienstnamen enthält. Typ der DatabaseName-Option. Sie können folgende Werte verwenden: - DatabaseName. Die DatabaseName-Option enthält einen Datenbanknamen für Microsoft SQL Server- oder Sybase ASE-Datenbanken oder einen Dienstnamen für IBM DB2-Datenbanken. - OracleSID. Die DatabaseName-Option enthält eine Oracle-SID. - OracleServiceName. Die DatabaseName-Option enthält einen vollständigen Oracle-Dienstnamen. Standardmäßig verwendet *infacmd* DatabaseName für alle Nicht-Oracle-Datenbanken.
DatabasePassword	Erforderlich. Das dem Datenbankbenutzer entsprechende Datenbankpasswort für das Data Analyzer Repository. Sie können ein Passwort mit der Option -so oder der Umgebungsvariable INFA_DEFAULT_DATABASE_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -so festgelegte Passwort Vorrang.
DatabasePort	Erforderlich. Portnummer für die Repository-Datenbank.
DatabaseTablespaceName	Erforderlich, wenn Sie eine IBM DB2-Datenbank wählen. Tablespace-Name für IBM DB2-Repositories. Wenn Sie den Tablespace-Namen angeben, erstellt der Reporting Service alle Repository-Tabellen in demselben Tablespace.
DatabaseUser	Erforderlich. Benutzerkonto für die Repository-Datenbank.
DatasourceDriver	Optional. Der Treiber, den der Reporting Service verwendet, um eine Verbindung zur Datenquelle herzustellen.
DatasourcePassword	Erforderlich. Passwort für den Datenquellenbenutzer. Sie können ein Passwort mit der Option -so oder der Umgebungsvariable INFA_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option -so festgelegte Passwort Vorrang.
DatasourceTestTable	Erforderlich. Testtabelle, die der Reporting Service verwendet, um die Verbindung zur Datenquelle zu überprüfen.

Option	Beschreibung
DatasourceURL	Erforderlich. JDBC-Verbindungsstring, den der Reporting Service verwendet, um eine Verbindung zur Datenquelle herzustellen.
DatasourceUser	Erforderlich. Benutzerkonto für die Datenquellen-Datenbank.
HttpPort	Erforderlich, wenn Sie nicht die Option SslPort verwenden. Der vom Reporting Service verwendete TCP-Port.
SslPort	Erforderlich, wenn Sie nicht die Option HttpPort verwenden. Der vom Reporting Service verwendete SSL-Port für sichere Verbindungen.
DataSourceAdvancedMode	Bearbeitungsmodus, mit dem der Bearbeitungsort für Datenquelleigenschaften bestimmt wird. Bei Aktivierung erfolgt die Bearbeitung im erweiterten Modus und der Wert ist TRUE. Im erweiterten Bearbeitungsmodus können Sie *Datasource*- und *Dataconnector*-Eigenschaften in der Data Analyzer-Instanz bearbeiten. Bei Deaktivierung erfolgt die Bearbeitung im Basismodus und der Wert ist FALSE. Im Basisbearbeitungsmodus können Sie *Datasource*-Eigenschaften im Administrator Tool bearbeiten. **Hinweis:** Nachdem Sie den Reporting Service im erweiterten Bearbeitungsmodus aktiviert haben, kann dies nicht mehr in den Basisbearbeitungsmodus zurück geändert werden.

Reporting-Quelloptionen

Geben Sie Reporting-Quelloptionen im folgenden Format ein:

```
infacmd CreateReportingService ... -rs option_name=value option_name=value
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Reporting-Quelloptionen beschrieben:

Option	Beschreibung
DatasourceName	Erforderlich. Name des Dienstes für das Reporting.
DatasourceType	Erforderlich. Typ des Dienstes. Diensttypen umfassen: - Dataprofiling - MM - PCRR - Other

Lineage Service-Optionen

Geben Sie Lineage Service-Optionen im folgenden Format ein:

```
infacmd CreateReportingService ... -ls option_name=value option_name=value
```

Wenn Sie mehrere Optionen eingeben, trennen Sie diese durch ein Leerzeichen. Zur Eingabe eines Werts, der ein Leerzeichen oder andere nicht-alphanumerische Zeichen enthält, schließen Sie den Wert in Anführungszeichen ein.

In der folgenden Tabelle werden die Lineage Service-Optionen beschrieben:

Option	Beschreibung
MetadataManagerService	Optional. Name des Metadata Manager Service, mit dem Sie eine Verbindung herstellen möchten, um eine Datenverlaufskontrolle auszuführen.
ResourceName	Optional. Name der Ressource im Metadata Manager, für die Sie die Data Analyzer-Metadaten geladen haben.

DeleteDARepositoryContents (veraltet)

Löscht Repository-Inhalt aus einem Data Analyzer-Repository. Wenn Sie Repository-Inhalt löschen, werden ebenfalls alle Berechtigungen und Rollen gelöscht, die Benutzern für den Berichterstellungsdienst zugewiesen sind.

Der Befehl „infacmd isp DeleteDARepositoryUsers“ verwendet die folgende Syntax:

```
DeleteDARepositoryContents

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp DeleteDARepositoryUsers“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des Berichterstellungsdiensts, für den Sie Inhalte löschen möchten.

RestoreDARepositoryContents (veraltet)

Stellt den Inhalt für ein Data Analyzer-Repository in aus binären Datei wieder her. Sie können Metadaten aus einer Repository-Backup-Datei in einer Datenbank wiederherstellen. Wenn Sie die Backup-Datei in einer vorhandenen Datenbank wiederherstellen, überschreiben Sie den vorhandenen Inhalt.

Der Befehl „infacmd isp RestoreDARepositoryContents“ verwendet die folgende Syntax:

```
RestoreDARepositoryContents

<-DomainName|-dn> domain_name

<-UserName|-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

<-fileName|-f> file_name
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp RestoreDARepositoryContents“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.

Option	Argument	Beschreibung
-ServiceName -sn	service_name	Erforderlich. Name des Berichterstellungsdiensts, für den Sie Inhalte wiederherstellen möchten.
-fileName -f	file_name	Erforderlich. Name und Dateipfad der Datei, in der Sie den Inhalt gespeichert haben.

UpdateReportingService (veraltet)

Aktualisiert oder erstellt den Dienst und die Herkunftsoptionen für den Berichterstellungsdienst.

Der Befehl „infacmd isp UpdateReportingService“ verwendet die folgende Syntax:

```
UpdateReportingService

<-DomainName|-dn> domain_name

<-UserName|-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

[<-ServiceOptions|-so> option_name=value]

[<-LineageService|-ls> option_name=value ]
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpdateReportingService“ beschrieben:

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

Option	Argument	Beschreibung
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des Berichterstellungsdiensts, den Sie aktualisieren möchten. Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen.
-ServiceOptions -so	option_name=value	Optional. Diensteigenschaften, mit denen definiert wird, wie der Berichterstellungsdienst ausgeführt wird.
-LineageService -ls	option_name=value	Optional. Für die Ausführung von Lineage-Analysen für Daten in Data Analyzer erforderliche Lineage-Eigenschaften.

UpgradeDARepositoryContents (veraltet)

Aktualisiert den Inhalt für ein Data Analyzer Repository.

Stellen Sie mit einem Upgrade von Inhalten des Repository sicher, dass die Metadaten in einer früheren Version des Data Analyzer Repository mit dem Reporting Service kompatibel sind.

Der infacmd isp UpgradeDARepositoryContents-Befehl verwendet die folgende Syntax:

```
UpgradeDARepositoryContents

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name
```

In der folgenden Tabelle werden infacmd isp UpgradeDARepositoryContents-Optionen und -Argumente beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang.
-Password -pd	password	Erforderlich. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn Sie LDAP-Authentifizierung verwenden. Name der Sicherheitsdomäne, zu der der Benutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Bei der Sicherheitsdomäne wird die Groß-/Kleinschreibung beachtet. Standardwert ist „Nativ“.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des Reporting Service, für den Sie Inhalte upgraden möchten.

UpgradeDARepositoryUsers (veraltet)

Aktualisiert Benutzer und Gruppen in einem Data Analyzer-Repository. Wenn Sie die Benutzer und Gruppen in einem Data Analyzer-Repository aktualisieren, werden diese vom Dienstmanager in die Informatica-Domäne verschoben.

Der Befehl „infacmd isp UpgradeDARepositoryUsers“ verwendet die folgende Syntax:

```
UpgradeDARepositoryUsers

<-DomainName|-dn> domain_name

<-UserName|-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

<-MigrateSecurityDomain|-msd> migrate_securitydomain
```

In der folgenden Tabelle werden die Optionen und Argumente für „infacmd isp UpgradeDARepositoryUsers“ beschrieben:

Option	Argument	Beschreibung
-DomainName -dn	domain_name	Erforderlich. Name der Informatica-Domäne. Sie können den Domänennamen mit der Option -dn oder der Umgebungsvariable INFA_DEFAULT_DOMAIN festlegen. Wenn Sie einen Domänennamen mit beiden Methoden festlegen, hat die Option -dn Vorrang.
-UserName -un	user_name	Erforderlich, wenn die Domäne die native oder die LDAP-Authentifizierung verwendet. Benutzername zum Herstellen einer Verbindung zur Domäne. Sie können den Benutzernamen mit der Option -un oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_USER festlegen. Wenn Sie einen Benutzernamen mit beiden Methoden festlegen, hat die Option -un Vorrang. Optional, wenn die Domäne Kerberos-Authentifizierung verwendet. Zum Ausführen des Befehls mit Single Sign-On legen Sie den Benutzernamen nicht fest. Wenn Sie den Benutzernamen festlegen, wird der Befehl ohne Single Sign-On ausgeführt.
-Password -pd	password	Erforderlich, wenn Sie den Benutzernamen angeben. Passwort für den Benutzernamen. Beim Passwort wird die Groß-/Kleinschreibung beachtet. Sie können ein Passwort mit der Option -pd oder der Umgebungsvariable INFA_DEFAULT_DOMAIN_PASSWORD festlegen. Wenn Sie ein Passwort mit beiden Methoden festlegen, hat das mit der Option „-pd“ festgelegte Passwort Vorrang.
-SecurityDomain -sdn	security_domain	Erforderlich, wenn die Domäne LDAP-Authentifizierung verwendet. Optional, wenn die Domäne native Authentifizierung oder Kerberos-Authentifizierung verwendet. Name der Sicherheitsdomäne, zu der der Domänenbenutzer gehört. Sie können eine Sicherheitsdomäne mit der Option -sdn oder der Umgebungsvariable INFA_DEFAULT_SECURITY_DOMAIN festlegen. Wenn Sie einen Sicherheitsdomänennamen mit beiden Methoden festlegen, hat die Option -sdn Vorrang. Der Name der Sicherheitsdomäne unterliegt der Groß-/Kleinschreibung. Wenn die Domäne eine native oder eine LDAP-Authentifizierung verwendet, ist der Standardwert „Nativ“. Wenn die Domäne Kerberos-Authentifizierung verwendet, ist die während der Installation erstellte LDAP-Sicherheitsdomäne der Standardwert. Der Name der Sicherheitsdomäne ist mit dem während der Installation angegebenen Benutzerbereich identisch.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Erforderlich, wenn die Informationen zur Gateway-Konnektivität in der Datei „domains.infa“ veraltet sind. Die Hostnamen und Portnummern für die Gateway-Knoten in der Domäne.

Option	Argument	Beschreibung
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Zeit in Sekunden, in der infacmd versucht, eine Verbindung zur Domäne herzustellen bzw. erneut herzustellen. Wenn Sie diese Option auslassen, verwendet infacmd den in der Umgebungsvariable INFA_CLIENT_RESILIENCE_TIMEOUT angegebenen Timeout-Wert. Wenn in der Umgebungsvariable kein Wert angegeben wurde, wird der Standardwert von 180 Sekunden verwendet.
-ServiceName -sn	service_name	Erforderlich. Name des Berichterstellungsdiensts für das Repository, für das Sie die Benutzer und Gruppen aktualisieren möchten.
-MigrateSecurityDomain -msd	migrate_securitydomain	Erforderlich. Name der Sicherheitsdomäne, in die Sie die Benutzer und Gruppen verschieben.

INDEX

A

Abfragen
  Ausführen 1178
AbortTask (pmcmd)
  Beschreibung 1103
abortWorkflow
  infacmd wfs 966
AbortWorkflow (pmcmd)
  Beschreibung 1105
AddAlertUser (infacmd isp) 242
AddConnectionPermissions (infacmd isp) 244
AddDomainLink (infacmd isp) 246
AddDomainNode (infacmd isp) 248
AddGroupPrivilege (infacmd isp) 250, 265
AddLicense (infacmd isp) 252
AddNamespace (infacmd isp) 254
AddNodeResource (infacmd isp) 256
AddParameterSetEntries (infacmd dis) 126
AddRolePrivilege (infacmd isp) 259
AddServiceLevel (infacmd isp) 261
AddToDeploymentGroup (pmrep)
  Beschreibung 1153
AddUserPrivilege (infacmd isp) 263
Alarme
  Abonnieren für Benutzer 242
  Aufheben des Abonnements mit infacmd isp 534
  Auflisten von eingetragenen Benutzern mit infacmd isp 459
  Auflisten von SMTP-Einstellungen mit infacmd 515
  Konfigurieren von SMTP-Einstellungen mit infacmd isp 652
Analyst-Dienst
  Aktualisieren von Business Glossary-Daten 88
  Aktualisieren von Eigenschaften für 71
  Auflisten der Konfiguration 67
  Auflisten von Eigenschaften für 69
  Auflisten von Unternehmensglossaren 90
  Erstellen in einer Domäne 64
  Exportieren von Unternehmensglossaren 91
  Importieren von Unternehmensglossaren aus XLSX-Dateien 95
Analyst-Dienst-Prozess
  Konfigurieren von Eigenschaften für 73
Anwendungen
  Auflisten von Objekten für 141
  Wiederherstellen 170
Anwendungsarchiv-Dateien (iar)
  Bereitstellen im Datenintegrationsdienst 137
Anwendungsdienste
  Abrufen des Status 439
  Abrufen von Eigenschaften 433
  aktivieren 962
  Aktivieren 413
  Deaktivieren 402
  Entfernen mit infacmd isp 562
Anwendungsdienstprozesse
  Abrufen des Status 437
Anwendungsobjekt
  Auflisten von Berechtigungen für Benutzer oder Gruppen 139
  Einrichten von Berechtigungen 174
application
  Auflisten von Eigenschaften für 143
  Einrichten von Berechtigungen 172
Application
  Aktualisieren 186
  Anhalten 181
  Bereinigen des Ergebnissatz-Caches 165
  Entfernen aus dem Datenintegrationsdienst 185
  Konfigurieren von Eigenschaften für 188
  Starten 179
  Umbenennen 168
ApplyLabel (pmrep)
  Beschreibung 1155
Arbeitsablauf
  Einrichten von Berechtigungen 174
Arbeitsablaufdienst
  Entfernen von Datenbanktabellen 974
Arbeitsabläufe
  Abrufen von Protokollereignissen 449
  Anhalten über Befehlszeile 1137
  Auflisten 982
  Starten über Befehlszeile 1131
  Wiederherstellen mithilfe der pmcmd-Syntax 1122
ArbeitsflussWiederherstellen (pmcmd)
  Beschreibung 1122
AssignDefaultOSProfile (infacmd isp) 267
AssignedToLicense (infacmd isp) 270
AssignGroupPermission (infacmd isp) 271
AssignIntegrationService (pmrep)
  Beschreibung 1157
AssignISToMMService (infacmd isp) 274
AssignLicense (infacmd isp) 276
AssignPermission (pmrep)
  Beschreibung 1158
AssignRoleToGroup (infacmd isp) 277
AssignRoletoUser (infacmd isp) 279
AssignRSToWSHubService (infacmd isp) 281
AssignUserPermission (infacmd isp) 283
Audit-Trail-Tabellen
  Erstellen, Content-Managementdienst 101
  Löschen, Content-Managementdienst 106
Ausführen einer Zuordnung
  mit einem Laufzeitparametersatz 741

B

BackUp (pmrep)
  Beschreibung 1160
BackupApplication (infacmd dis) 128
BackupContents (infacmd mrs) 677
BackupDARepositoryContents (infacmd isp) 1259

BackupDomain (infasetup)
Beschreibung 1046
Befehle
Eingeben von Optionen und Argumenten für 33
Befehlszeilendienstprogramme
Datei „domains.infa“ 30
konfigurieren 29
Befehlszeilendienstprogramme (Metadata Manager-Dienstprogramme konfigurieren) 30
Befehlszeilendienstprogramme (PowerCenter-Dienstprogramme konfigurieren) 29
Befehlszeilenmodus für pmcmd
Verbinden 1098
Befehlszeilenprogramme
Syntax für 34
Übersicht 32
Benutzer
Auflisten mit infacmd isp 463
Auflisten von Berechtigungstypen für 469
Auflisten von Gruppen für einen Benutzer 487
Entfernen aus einer Gruppe mit infacmd isp 568
Entfernen mit infacmd isp 566
Erstellen in einer Domäne 391
Exportieren 421
Exportieren mit infacmd isp 418
Hinzufügen zu Gruppen in einer Domäne 265
Importieren mit infacmd isp 453, 457
Migrieren mit infacmd 521
Benutzer und Gruppen
Entfernen von Berechtigungen 580
Benutzer und Gruppen in der Sicherheitsdomäne
Synchronisieren mit LDAP-Benutzern und -Gruppen 595
Benutzerberechtigungen
Auflisten für Domänenobjekte 517
Benutzerkonten
Aktivieren 416
Bearbeiten von Eigenschaften 408
Deaktivieren in einer Domäne 406
Berechnungsknoten
Auflisten von Attributen für 849
Einrichten von Attributen 852
Berechtigungen
Auflisten für Dienste mit infacmd isp 511
Auflisten für eine Gruppe mit infacmd isp 485
Auflisten für eine Rolle mit infacmd isp 504
Auflisten für einen Benutzer 519
Entfernen 1216
Entfernen aus Benutzer- oder Gruppenverbindungen mit infacmd isp 538
Entfernen aus einer Gruppe mit infacmd isp 549
Entfernen aus einer Rolle mit infacmd isp 560
Entfernen von einem Benutzer mit infacmd isp 572
Zuweisen mit pmrep 1158
Zuweisen zu Gruppen in einer Domäne 250
Zuweisen zu Rollen 259
Bereitgestellte Anwendungen
Auflisten 145
Sichern 128
Bereitstellen von Objekten
depcntl.dtd 1249
BereitstellungsGruppeBereitstellen (pmrep)
Beschreibung 1175
Bereitstellungsgruppen
Auflisten mehrerer Ordner 1255
Bereitstellungssteuerdatei
Beschreibung 1249
Berichterstellungsdienst
Aktualisieren mit infacmd isp 1271
Berichterstellungsdienst *(Fortsetzung)*
Erstellen in einer Domäne 1262
Beschreibung 528
Beschriftungen
Erstellen mit pmrep 1171
Löschen 1173
Betriebssystemprofil
Aktualisieren mit infacmd isp 638
Auflisten mit infacmd isp 501
Auflisten von Standardprofilen 475
Entfernen mit infacmd isp 557
Entfernen von Standardprofil von einem Benutzer oder einer Gruppe 597
Zuweisen von Standardprofil zu einem Benutzer oder einer Gruppe 267
Betriebssystemprofile
Erstellen in einer Domäne 374
Binäre Protokolldateien
Umwandeln in Text, XML oder lesbaren Text 286
Blaze-Dienst
Stoppen 183

C

Cache für virtuelle Tabellen
Aktualisieren 927
Bereinigen 925
CancelDataObjectCacheRefresh (infacmd dis) 130
cancelProfileExecution (infacmd ps) 762
cancelWorkflow
infacmd wfs 970
ChangeOwner (pmrep)
Beschreibung 1161
CheckIn (pmrep)
Beschreibung 1161
CheckInObject (infacmd mrs) 679
CleanUp (pmrep)
Beschreibung 1162
ClearDeploymentGroup (pmrep)
Beschreibung 1162
CloseForceListener (infacmd pwx) 785
CloseListener (infacmd pwx) 788
CondenseLogger (infacmd pwx) 791
Connect (pmcmd)
Beschreibung 1107
Connect (pmrep)
Beschreibung 1163
Content Management Service
Auflisten von Eigenschaften für 108
Upgrade erfolgt 122
Content-Managementdienst
Aktualisieren der Optionen für 118
Auflisten der Optionen für 110
Bereinigen verwaister Referenzdaten 112
Entfernen mithilfe von infacmd cms 115
Erstellen in einer Domäne 103
Synchronisieren von Daten mit Master-CMS-Rechner 116
Content-Managementdienst-Prozess
Konfigurieren von Optionen für 120
ConvertLogFile (infacmd isp) 286
CPU-Profil
Berechnen mit infacmd isp 578
Create (pmrep)
Beschreibung 1164
CreateAuditTables (infacmd cms) 101
CreateConnection (infacmd isp) 287

CreateConnection (pmrep)
Beschreibung 1165
CreateContent (infacmd tdm) 960
CreateContents (infacmd mrs) 680
CreateDARepositoryContents (infacmd isp) 1260
createdatamaps (infacmd pwx) 794
CreateDeploymentGroup (pmrep)
Beschreibung 1168
CreateFolder (infacmd isp) 355
CreateFolder (pmrep)
Beschreibung 1169
CreateGrid (infacmd isp) 357
CreateGroup (infacmd isp) 358
CreateGroup (pmrep)
Beschreibung 1171
CreateIntegrationService (infacmd isp) 360
CreateLabel (pmrep)
Beschreibung 1171
CreateListenerService (infacmd pwx) 797
CreateLoggerService (infacmd pwx) 799
CreateMMService (infacmd isp) 370
CreateOSProfile (infacmd isp) 374
CreateProject (infacmd mrs) 682, 684
CreateReportingService (infacmd isp) 1262
CreateRepositoryService (infacmd isp) 380
CreateRole (infacmd isp) 385
CreateSAPBWService (infacmd isp) 387
CreateSchedule (infacmd sch) 865
CreateService (infacmd as) 64
CreateService (infacmd cms) 103
CreateService (infacmd dis) 132
CreateService (infacmd mrs) 686
CreateService (infacmd search) 899
CreateService (infacmd tdm) 954
CreateUser (infacmd isp) 391
CreateWH (infacmd ps) 764
CreateWSHubService (infacmd isp) 394

D

Data Analyzer-Repository
Erstellen von Inhalt 1260
Löschen von Inhalt 1267
Sichern des Inhalts 1259
Upgraden von Benutzern und Gruppen mit infacmd isp 1274
Upgraden von Inhalten mit infacmd isp 1272
Wiederherstellen von Inhalt mit infacmd isp 1269
Datenintegrationsdienst
Auflisten von Berechnungseigenschaften 146
Auflisten von Eigenschaften für 159
Erstellen 132
Konfigurieren von Berechnungseigenschaften 190
Konfigurieren von Eigenschaften für 197
Datenintegrationsdienst-Prozess
Auflisten von Eigenschaften für 155, 161
Konfigurieren von Eigenschaften für 210
Datenobjekt-Cache
Aktualisieren 166
Datenobjekte
Auflisten von Eigenschaften für 148
Konfigurieren von Eigenschaften für 192
DB2
infacmd-Verbindungsoptionen 318
DefineDomain (infasetup)
Beschreibung 1049
DefineGatewayNode (infasetup)
Beschreibung 1062
DefineWorkerNode (infasetup)
Beschreibung 1068
Delete (pmrep)
Beschreibung 1171
DeleteAuditTables (infacmd cms) 106
DeleteConnection (pmrep)
Beschreibung 1172
DeleteContents (infacmd mrs) 689
DeleteDARepositoryContents (infacmd isp) 1267
DeleteDeploymentGroup (pmrep)
Beschreibung 1173
DeleteDomain (infasetup)
Beschreibung 1072
DeleteFolder (infacmd mrs) 691
DeleteFolder (pmrep)
Beschreibung 1173
DeleteLabel (pmrep)
Beschreibung 1173
DeleteNamespace (infacmd isp) 398
DeleteObject (pmrep)
Beschreibung 1174
DeleteParameterSetEntries (infacmd dis) 135, 150
DeleteProject (infacmd mrs) 693
DeleteSchedule (infacmd sch) 873
depcntl.dtd
Auflisten 1249
DeployApplication (infacmd dis) 137
DeployFolder (pmrep)
Beschreibung 1176
DeployImport (infacmd rtm) 857
DeployObjects
infacmd oie 748
Dienste
Auflisten mit infacmd isp 513
Pingen 527
Dienstebenen
Aktualisieren mit infacmd isp 648
Auflisten mit infacmd isp 508
Entfernen mit infacmd isp 564
Hinzufügen 261
Dienstprozesse
Aktivieren auf Knoten 414
Deaktivieren auf einem Knoten 404
DisableNodeResource (infacmd isp) 400
DisableService (infacmd isp) 402
DisableService (infacmd tdm) 963
DisableServiceProcess (infacmd isp) 404
DisableUser (infacmd isp) 406
Disconnect (pmcmd)
Beschreibung 1108
DisplayAllLogger (infacmd pwx) 804
DisplayCPULogger (infacmd pwx) 807
DisplayEventsLogger (infacmd pwx) 810
DisplayMemoryLogger (infacmd pwx) 813
DisplayRecordsLogger (infacmd pwx) 816
displayStatsListener (infacmd pwx) 819
DisplayStatusLogger (infacmd pwx) 822
Domäne für verschiedene Versionen
Ausführen von pmcmd 1098
Ausführen von pmrep 1148
Domänen
Aktualisieren von Eigenschaften mit infacmd isp 614
Auflisten verlinkter Domänen mit infacmd isp 477
Auflisten von Eigenschaften mit infacmd isp 479
Entfernen von Links mit infacmd isp 540
Erstellen mit infasetup 1049
Löschen mit infasetup 1072
Pingen 527

Domänen *(Fortsetzung)*
Sichern mit infasetup 1046
Wiederherstellen mit infasetup 1079
Domänengateway-Hosts
Pingen 527
Domänenüberwachung
Aktualisierungsoptionen 627
Auflisten von Optionen 493
Bereinigungsoptionen 532
Domänenüberwachungsoptionen aktualisieren (infacmd isp) 627
Domänenüberwachungsoptionen auflisten (infacmd isp) 493
dropTables (infacmd wfs) 974
DropWH (infacmd ps) 766
DTD-Datei
Plug-In-Vorlage 1213

E

EditUser (infacmd isp) 408
EditUser (pmrep)
Beschreibung 1178
EnableNodeResource (infacmd isp) 411
EnableService (infacmd isp) 413
EnableService (infacmd tdm) 962
EnableServiceProcess (infacmd isp) 414
EnableUser (infacmd isp) 416
Entsperren
Gesperrtes Objekt 721
Execute (infacmd ps) 767
executeProfile (infacmd ps) 770
ExecuteQuery (pmrep)
Beschreibung 1178
ExecuteSQL (infacmd sql) 910
Exit (pmrep)
Beschreibung 1180
Export (infacmd rtm) 859
Export-Steuerdateien
Beispiele für Domänenobjekte 1041
Beispiele für Model Repository-Objekte 1042
Parameter für Domänenobjekte 1028
Regeln und Richtlinien 1040
Schemadateien 1027
exportControl.xsd
infacmd-Steuerdateien 1027
ExportDomainObjects (infacmd isp)
Beschreibung 418
exportGlossary (infacmd bg) 91
ExportObjects
infacmd oie 749
exportResources
infacmd oie 753
Exportsteuerdateien
Benennungskonventionen 1027
infacmd 1026
Parameter für Modellrepository-Objekte 1030
ExportToPC (infacmd ipc) 233
ExportUsersAndGroups (infacmd isp) 421
Externe Sicherheitsmodule
Aufheben der Registrierung 1222
Registrieren 1213

F

FileSwitchLogger (infacmd pwx) 825
FindCheckout (pmrep)
Beschreibung 1180
Funktionen
validieren 655
Für einen Datenintegrationsdienst bereitgestellte Mappings
Ausführen 741

G

gateway
Aktualisieren von Informationen mit infacmd isp 618
GenerateAbapProgramToFile (pmrep)
Beschreibung 1182
GenerateEncryptionKey (infasetup)
beschreibung 1075
generateReadableViewXML
infacmd xrf 1024
genreusereportfrompc (infacmd ipc) 239
Gespeicherte Prozeduren
Auflisten von Berechtigungen 920
Einrichten von Berechtigungen 936
GetConnectionDetails (pmrep)
Beschreibung 1182
getDomainObjectPermissions (infacmd aud) 76
getExecutionStatus (infacmd ps) 772
GetFolderInfo (infacmd isp) 425
GetLastError (infacmd isp) 427
GetLog (infacmd isp) 429
GetNodeName (infacmd isp) 432
getPrivilegeAssociation (infacmd aud) 78
getProfileExecutionStatus (infacmd ps) 773
GetRequestLog
infacmd ms 734
GetRunningSessionsDetails (pmcmd)
Beschreibung 1109
GetServiceDetails (pmcmd)
Beschreibung 1110
GetServiceOption (infacmd isp) 433
GetServiceProcessOption (infacmd isp) 435
GetServiceProcessStatus (infacmd isp) 437
GetServiceProperties (pmcmd)
Beschreibung 1112
GetServiceStatus (infacmd isp) 439
GetSessionLog (infacmd isp) 441
Getsessionstatistics (pmcmd)
Beschreibung 1113
GetSystemLogDirectory (infacmd isp) 444
GetTaskDetails (pmcmd)
Beschreibung 1115
getUserGroupAssociation (infacmd aud) 80, 83
getUsersPersonalInfo (infacmd aud) 85
GetWorkflowDetails (pmcmd)
Beschreibung 1117
GetWorkflowLog (infacmd isp) 449
Gitter
Aktualisieren zugewiesener Knoten mit infacmd isp 619
Auflisten von Knoten mit infacmd isp 482
Entfernen mit infacmd isp 544
Erstellen 357
Gleichzeitige Arbeitsabläufe
Anhalten über Befehlszeile 1137
Starten über Befehlszeile 1131
Gruppen
Auflisten für einen Benutzer 487
Auflisten mit infacmd isp 460
Entfernen mit infacmd isp 545
Erstellen in Domänen 358
Exportieren 421
Exportieren mit infacmd isp 418

Gruppen *(Fortsetzung)*
Importieren mit infacmd isp 453, 457
Gruppenberechtigungen
Auflisten für Domänenobjekte 483
Entfernen für Objekte 547
Zuweisen zu Objekten 271

H

Help (infacmd) 453
Help (pmcmd)
Beschreibung 1121
Hilfe (pmrep)
Beschreibung 1184

I

IBM DB2
Verbindungsstring, Beispiel 1149
ICMD_JAVA_OPTS
Konfigurieren 41
Im Datenintegrationsdienst bereitgestellte Arbeitsabläufe
abbrechen 966
Starten 989
wiederherstellen 984
Wird abgebrochen 970
impcntl.dtd
Beschreibung 1238
Import (infacmd rtm) 862
Import-Steuerdateien
Beispiele für Domänenobjekte 1041
Beispiele für Model Repository-Objekte 1042
Parameter für Domänenobjekte 1033
Regeln und Richtlinien 1040
Schemadateien 1027
importControl.xsd
infacmd-Steuerdateien 1027
ImportDomainObjects (infacmd isp)
Beschreibung 453
importGlossary (infacmd bg) 95
Importieren aus PowerCenter
Optionen 237
Importieren von Objekten
impcntl.dtd 1238
ObjectImport XML-Beispiel 1242
ImportObjects
infacmd oie 755
Importsteuerdateien
Benennungskonventionen 1027
infacmd 1026
Parameter für Modellrepository-Objekte 1035
ImportUsersAndGroups (infacmd isp)
Beschreibung 457
INFA_CLIENT_RESILIENCE_TIMEOUT
Konfigurieren 42
INFA_CODEPAGENAME
Konfigurieren 43
INFA_DEFAULT_DATABASE_PASSWORD
Konfigurieren 43
INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD
konfigurieren 45
INFA_DEFAULT_DOMAIN
Konfigurieren 46
INFA_DEFAULT_DOMAIN_PASSWORD
Konfigurieren 46
INFA_DEFAULT_DOMAIN_USER
Konfigurieren 47
INFA_DEFAULT_PWX_OSEPASSWORD
Konfigurieren 48
INFA_DEFAULT_PWX_OSPASSWORD
Konfigurieren 49
INFA_JAVA_CMD_OPTS
Konfigurieren 50
INFA_NODE_KEYSTORE_PASSWORD
konfigurieren 52
INFA_NODE_TRUSTSTORE_PASSWORD
konfigurieren 53
INFA_PASSWORD
Konfigurieren 51
INFA_REPCNX_INFO
Konfigurieren 54
INFA_REPOSITORY_PASSWORD
Konfigurieren 55
infacmd
Aktualisieren von Domäneninformationen 62
Anzeigen der Hilfe für Befehle 453
Auflisten von Plugin-IDs 60
Ausführen von Befehlen 61
Dienstprozessoptionen 369
Integrationsdienst-Optionen 364, 725
Knoten, Wechseln von Arbeitsknoten zu Gateway-Knoten 591
Lizenzen, Aufheben der Zuweisung 601
Reporting Service-Optionen 1264
Rückgabewerte 62
SAP BW Service-Optionen 390
SAP BW Service-Prozessoptionen 391
Sicherheitsdomänen, Auflisten 506
Steuerdateien 1026
Trennen des Metadata Manager-Diensts 599
Versionsinformationen, Anzeigen 657
Web Services Hub-Dienstoptionen 397
infacmd advanced
Validieren von Funktionen 655
infacmd as
Aktualisieren von Eigenschaften für den Analyst-Dienst 71
Auflisten der Konfiguration für den Analyst-Dienst 67
Auflisten von Eigenschaften für den Analyst-Dienst-Prozess 69
Erstellen eines Analyst-Dienst in einer Domäne 64
Konfigurieren von Eigenschaften für Analyst-Dienst-Prozess 73
infacmd bg
Aktualisieren von Business Glossary-Daten im Modellrepository 88
Auflisten von Unternehmensglossaren in Analyst 90
Exportieren von Unternehmensglossaren aus dem Analyst Tool 91
Importieren von Unternehmensglossaren aus XLSX- oder ZIP-Dateien in das Analyst Tool 95
infacmd cms
Aktualisieren der Optionen für Content-Managementdienst 118
Auflisten der Optionen für den Content-Managementdienst-Prozess 110
Auflisten von Optionen für Content Management Service 108
Bereinigen verwaister Referenzdaten 112
Entfernen des Content-Managementdienst aus einer Domäne 115
Erstellen von Audit-Trail-Tabellen 101
Erstellen von Content-Managementdienst in einer Domäne 103
Konfigurieren von Optionen für den Content-Managementdienst-Prozess 120
Löschen von Audit-Trail-Tabellen 106
Synchronisieren von Daten 116
Upgrade des Dienstes 122
infacmd dis
Aktualisieren der Parametersatzeinträge 195
Aktualisieren des aktuellen Werts für das Sequenzdatenobjekt 177
Aktualisieren des Datenobjekt-Caches 166

infacmd dis *(Fortsetzung)*
Aktualisieren von Anwendungen 186
Aktualisierung des logischen Datenobjekt-Cache stoppen 130
Anhalten von Anwendungen 181
Auflisten bereitgestellter Anwendungen 145
Auflisten der Objekte in einem Parametersatz 152
Auflisten von Berechnungseigenschaften 146
Auflisten von Berechtigungen für Anwendungsobjekte für Benutzer oder Gruppen 139
Auflisten von Eigenschaften der Datenobjekte 148
Auflisten von Eigenschaften des Datenintegrationsdienst-Prozesses 161
Auflisten von Eigenschaften für Anwendungen 143
Auflisten von Eigenschaften für den Datenintegrationsdienst 159
Auflisten von Eigenschaften für Sequenzobjekte 155
Auflisten von Objekten für Anwendungen 141
Auflisten von Parametersätzen in einer Anwendung 154
Bereinigen des Caches für logische Datenobjekte 162
Bereinigen des Ergebnissatz-Caches 165
Bereitstellen von Anwendungsarchiv-Dateien (iar) 137
Datenobjektoptionen 194
Einrichten von Anwendungsberechtigungen 172
Einrichten von Arbeitsablaufberechtigungen 174
Einrichten von Berechtigungen für Anwendungsobjekte 174
Einrichten von Mapping-Berechtigungen 174
Entfernen von Anwendungen 185
Erstellen eines Datenintegrationsdiensts 132
Hinzufügen von Parametersatzeinträgen 126
Konfigurieren von Anwendungseigenschaften 188
Konfigurieren von Berechnungseigenschaften 190
Konfigurieren von Datenobjekteigenschaften 192
Konfigurieren von Eigenschaften für den Datenintegrationsdienst 197
Konfigurieren von Eigenschaften für den Datenintegrationsdienst-Prozess. 210
Listet Sequenzobjekte auf. 157
Löschen von Parametersatzeinträgen 135, 150
Sichern einer bereitgestellten Anwendung 128
Starten von Anwendungen 179
Stoppen des Blaze-Diensts 183
Umbenennen bereitgestellter Anwendungen 168
Wiederherstellen von Anwendungen aus Backup-Dateien 170
infacmd ipc
Exportieren von Objekten aus dem Modellrepository 233
Wiederverwendung eines Berichtsobjekts 239
infacmd isp
Abonnieren von Benachrichtigungen für Benutzer 242
Abrufen angegebener Protokollereignisse 429
Abrufen der neuesten Fehlermeldungen 427
Abrufen des Status eines Anwendungsdienstprozesses auf einem Knoten 437
Abrufen des Status eines Anwendungsdiensts 439
Abrufen des Verzeichnispfads des Systemprotokolls 444
Abrufen von Diensteigenschaften 433
Abrufen von Integrationsdienst-Prozesseigenschaften 435
Abrufen von Knotennamen 432
Abrufen von Protokollereignissen für Arbeitsabläufe 449
Abrufen von Protokollereignissen für Sitzungen 441
Aktivieren von Anwendungsdiensten 413
Aktivieren von Benutzerkonten 416
Aktivieren von Dienstprozessen auf einem Knoten 414
Aktivieren von Ressourcen 411
Aktualisieren der Knotenrolle 635
Alarme, Aufheben des Abonnements 534
Alarme, Auflisten von eingetragenen Benutzern 459
Alarme, Konfigurieren von SMTP-Einstellungen 652
Auflisten der Benutzer mit Verbindungsberechtigungen 469
infacmd isp *(Fortsetzung)*
Auflisten von Berechtigungen für Benutzer oder Gruppen für eine Verbindung 465
Auflisten von Diensten, die einer Lizenz zugewiesen sind 270
Auflisten von Domänenobjekten für Benutzer 517
Auflisten von Domänenobjekten für Gruppen 483
Auflisten von Gruppen für einen Benutzer 487
Auflisten von Knotenrollen 497
Auflisten von Ordnereigenschaften 425
Auflisten von SMTP-Einstellungen für den ausgehenden Mailserver 515
Auflisten von Standardbetriebssystemprofilen 475
Bearbeiten von Benutzerkontoeigenschaften 408
Benutzer und Gruppen, Exportieren 418
Benutzer und Gruppen, Importieren 453, 457
Benutzer, Auflisten 463
Benutzer, Auflisten von Berechtigungen für 519
Benutzer, Entfernen 566
Benutzer, Entfernen aus einer Gruppe 568
Benutzer, Entfernen von Berechtigungen 572
Berechtigungen, Entfernen aus Benutzer- oder Gruppenverbindungen 538
Berichterstellungsdienst, Aktualisieren 1271
Betriebssystemprofil, Aktualisieren 638
Betriebssystemprofil, Auflisten 501
Betriebssystemprofil, Entfernen 557
CPU-Profil, Berechnen 578
Data Analyzer Repository, Upgraden von Benutzern und Gruppen 1274
Data Analyzer Repository, Upgraden von Inhalten 1272
Data Analyzer Repository, Wiederherstellen von Inhalt 1269
Deaktivieren von Anwendungsdiensten 402
Deaktivieren von Benutzerkonten 406
Deaktivieren von Dienstprozessen auf einem Knoten 404
Deaktivieren von PowerCenter-Ressourcen 400
Dienste, Auflisten 513
Dienste, Auflisten von Berechtigungen für 511
Dienste, Entfernen 562
Dienstebene, Aktualisieren 648
Dienstebenen, Auflisten 508
Dienstebenen, Entfernen 564
Dienstprozesse, Aktualisieren 649
Domänen, Aktualisieren von Eigenschaften 614
Domänen, Auflisten verlinkter Domänen 477
Domänen, Auflisten von Eigenschaften 479
Domänen, Entfernen von Links 540
Entfernen von Benutzerberechtigungen für Objekte 569
Entfernen von Berechtigungen für Benutzer und Gruppen 580
Entfernen von Gruppenberechtigungen für Objekte 547
Entfernen von Standardbetriebssystemprofil 597
Erstellen des Berichterstellungsdiensts in einer Domäne 1262
Erstellen des Integrationsdiensts in einer Domäne 360
Erstellen des Repository-Diensts in einer Domäne 380
Erstellen des SAP BW-Dienst in einer Domäne 387
Erstellen einer Verbindung 287
Erstellen eines Metadata Manager-Diensts in einer Domäne 370
Erstellen eines Webdienst-Hub in einer Domäne 394
Erstellen von Benutzern in einer Domäne 391
Erstellen von Betriebssystemprofilen in einer Domäne 374
Erstellen von Gittern 357
Erstellen von Gruppen in Domänen 358
Erstellen von Inhalt für ein Data Analyzer Repository 1260
Erstellen von Ordnern 355
Erstellen von Rollen in einer Domäne 385
Exportieren von Benutzern und Gruppen in eine Datei 421
Exportsteuerdateien 1028
Gateway-Informationen, Aktualisieren 618
Gitter, Aktualisieren zugewiesener Knoten 619

infacmd isp *(Fortsetzung)*
Gitter, Auflisten von Knoten 482
Gitter, Entfernen 544
Gruppen, Auflisten 460
Gruppen, Auflisten von Berechtigungen für 485
Gruppen, Entfernen 545
Gruppen, Entfernen von Berechtigungen 549
Hinzufügen eines Domänenlinks 246
Hinzufügen von Benutzern zu Gruppen in einer Domäne 265
Hinzufügen von Dienstebenen 261
Hinzufügen von Knoten zu einer Domäne 248
Hinzufügen von Lizenzen zu Domänen 252
Hinzufügen von Ressourcen zu Knoten 256
Importsteuerdateien 1032
Integrationsdienste, Aktualisieren 621
Knoten, Aktualisieren 633
Knoten, Auflisten 499, 509
Knoten, Auflisten von Optionen 494
Knoten, Entfernen 553
Knoten, Herunterfahren 590
Knoten, Trennen von Domänen 608
Knoten, Wechseln von Gateway-Knoten zu Arbeitsknoten 593
LDAP-Authentifizierung, Einrichten 582
LDAP-Serverkonfiguration, Aktualisieren 585
LDAP-Serverkonfiguration, Auflisten 503
LDAP-Verbindung, Auflisten 489
Lizenzen, Aktualisieren 623
Lizenzen, Anzeigen von Informationen 588
Lizenzen, Auflisten 491
Lizenzen, Entfernen 551
Löschen von Inhalt aus dem Data Analyzer Repository 1267
Metadata Manager-Dienst-Eigenschaften, Aktualisieren 625
Migrieren von Benutzern 521
Ordner, Aktualisieren der Beschreibung 616
Ordner, Auflisten 480
Ordner, Entfernen 542
Ordner, Verschieben 523
Ordner, Verschieben von Objekten zwischen 525
Passwörter, Zurücksetzen von Benutzerpasswörtern 576
Pingen von Objekten 527
Protokollereignisse, Bereinigen 530
Repository-Dienste, Aktualisieren 641
Ressourcen, Auflisten für Knoten 496
Ressourcen, Entfernen aus Knoten 555
Rollen, Auflisten 462
Rollen, Auflisten von Berechtigungen für 504
Rollen, Entfernen 558
Rollen, Entfernen aus einer Gruppe 602
Rollen, Entfernen von Benutzern 605
Rollen, Entfernen von Berechtigungen 560
Rollen, Exportieren 418
Rollen, Importieren 453
SAP BW Services, Aktualisieren 646
Sichern des Inhalts für das Data Analyzer Repository 1259
Synchronisieren von Benutzern und Gruppen in der Sicherheitsdomäne mit LDAP-Benutzern und -Gruppen 595
Umbenennen von Verbindungen 574
Umwandeln von binären Protokolldateien 286
Verbinden eines Repository mit Webdienst-Hub 281
Verbindungen, Aktualisieren von Eigenschaften 610
Verbindungen, Auflisten 471
Verbindungen, Auflisten von Optionen 473
Verbindungen, Entfernen aus Domänen 536
Verbindungen, Exportieren 418
Verbindungen, Importieren 453
Verbindungsberechtigungen, Auflisten nach Gruppe 467
Web Services Hub, Aktualisieren 653
Web Services Hub, Trennen eines Repository 607

infacmd isp *(Fortsetzung)*
Zuordnen von Rollen zu Gruppen für Domänen oder Anwendungsdienste 277
Zuweisen des Integrationsdiensts 274
Zuweisen von Benutzerberechtigungen zu Objekten 283
Zuweisen von Berechtigungen zu Benutzern 263
Zuweisen von Berechtigungen zu Gruppen 250
Zuweisen von Gruppenberechtigungen zu Objekten 271
Zuweisen von Lizenzen zu Anwendungsdiensten 276
Zuweisen von Privilegien zu Rollen in Gruppen 259
Zuweisen von Rollen zu Benutzern 279
Zuweisen von Standardbetriebssystemprofil 267
Zuweisen von Verbindungsberechtigungen zu Benutzern oder Gruppen 244
infacmd mrs
Aktualisieren von Dienstprozessoptionen für den Modellrepository-Dienst 729
Aktualisieren von Optionen für den Modellrepository-Dienst 723
Auflisten von ausgecheckten Objekten 697
Auflisten von Dateien im Backup-Ordner 695
Auflisten von Dienstprozess-Optionen für den Modellrepository-Dienst 707
Auflisten von gesperrten Objekten 701
Auflisten von Optionen für den Modellrepository-Dienst 705
Auflisten von Ordnern im Repository des Modellrepository-Diensts 699
Auflisten von Projekten im Repository des Modellrepository-Dienst 703
Einchecken von Objekten 679
Entsperren eines Objekts 721
Erstellen des Modellrepository-Dienst 686
Erstellen eines Projekts 682, 684
Erstellen von Repository-Inhalt für einen Modellrepository-Dienst 680
Erstellt die Objektabhängigkeitsgrafik neu. 713
Füllen des Versionsverwaltungssystems 709
Löschen des Inhalts des Modellrepository 689
Löschen eines Ordners 691
Löschen eines Projekts 693
Neuzuweisung eines ausgecheckten Objekts 711
Neuzuweisung eines gesperrten Objekts 711
Sichern des Inhalts des Modellrepository in einer Datei 677
Umbenennen eines Ordners 715
Upgraden von Inhalten des Modellrepository-Dienst 731
Wiederherstellen der Inhalte des Modellrepository 717
Wiederherstellen von ausgecheckten Objekten 719
infacmd ms
Aktualisieren der Zuordnungsparameterdatei 745
Auflisten der Mappings in einer Anwendung 739
Ausführen eines für einen Datenintegrationsdienst bereitgestellten Mappings 741
Schreiben des Zuordnungsprotokolls 734
infacmd oie
Exportieren von Objekten 749
Exportieren von Ressourcen nach Metadata Manager 753
Exportsteuerdateien 1028
Importieren von Objekten 755
Importsteuerdateien 1032
Objekte werden bereitgestellt 748
infacmd ps
Abrufen des Profilaufgabenstatus 772
Abrufen des Profilmodellstatus 773
Auflisten von Profil- und Scorecard-Ergebnissen 775
Ausführen eines Profilmodells 770
Ausführen von Profil- und Scorecard-Ergebnissen 767
Bereinigen von Profil- und Scorecard-Ergebnissen 780
Entfernen von Profiling Warehouse-Inhalten 766
Erstellen eines Data Profiling Warehouse 764

infacmd ps *(Fortsetzung)*
gcenceling Profilmodell 762
Migrieren von Profilergebnissen 777
Migrieren von Schlüsseln 783
Migrieren von Scorecard-Ergebnissen 779
infacmd pwx
Aktualisieren von Listenerdienst-Eigenschaften 840
Aktualisieren von Protokollierungsdienst-Eigenschaften 844
Anhalten des Listenerdiensts 788
Anhalten des Protokollierungsdiensts 831
Anhalten von Listenerdienst-Aufgaben 834
Anzeigen aller Protokollierungsdienst-Nachrichten 804
Anzeigen der Anzahl der vom Protokollierungsdienst verarbeiteten Änderungsdatensätze 816
Anzeigen der Speichernutzung für den Protokollierungsdienst 813
Anzeigen des Status der Writer-Unteraufgabe für Protokollierungsdienst 822
Anzeigen von CPU-Informationen für den Protokollierungsdienst. 807
Anzeigen von Ereignissen für den Protokollierungsdienst 810
Anzeigen von Informationen für aktive Listenerdienst-Aufgaben 828
Anzeigen von Überwachungsstatistiken für den Listenerdienst und dessen Aufgaben 819
Erstellen des Listenerdiensts 797
Erstellen des Protokollierungsdiensts 799
Erstellen von Datenzuordnungen 794
Erzwingen des Abbruchs des Listenerdiensts 785
Starten des Protokollierungszyklus für den Protokollierungsdienst 791
Upgraden nichtrelationaler Datenobjekte 837
Wechseln zum neuen Satz an Protokolldateien des Protokollierungsdiensts 825
infacmd rms
Auflisten von Attributen des Berechnungsknotens 849
Auflisten von Eigenschaften für den Ressourcenmanager-Dienst 851
Einrichten von Attributen des Berechnungsknotens 852
Konfigurieren von Eigenschaften für Ressourcenmanager-Dienst 854
infacmd rtm
Exportieren von Referenztabellen 859
Importieren von Inhalt aus Anwendungsdateien 857
Importieren von Referenztabellen in Modellrepositorys 862
infacmd sch
Aktualisieren eines Zeitplans 887
Erstellen eines Zeitplans 865
Löschen eines Zeitplans 873
infacmd search
Auflisten von Eigenschaften für den Suchdienst 902
Auflistung der Eigenschaften für den Suchdienstprozess 904
Konfigurieren von Eigenschaften für den Suchdienstprozess 908
Konfigurieren von Eigenschaftgen für den Suchdienst 906
Suchdienst wird erstellt 899
infacmd sql
Aktualisieren des Caches für virtuelle Tabellen 927
Aktualisieren von SQL-Datendienst-Optionen 948
Anhalten des SQL-Datendiensts 943
Auflisten der SQL-Datendienste für einen Datenintegrationsdienst 918
Auflisten von Berechtigungen für einen SQL-Datendienst 917
Auflisten von Berechtigungen für gespeicherte Prozeduren 920
Auflisten von Berechtigungen für virtuelle Spalten 913
Auflisten von Berechtigungen für virtuelle Tabellen 924
Auflisten von Eigenschaften für einen SQL-Datendienst 915
Auflisten von Eigenschaften für Spalten in virtuellen Tabellen 911
Auflisten von Eigenschaften für virtuelle Tabellen 922
Bereinigen des Caches für virtuelle Tabellen 925
Einrichten von Benutzer- und Gruppenberechtigungen für gespeicherte Prozeduren 936
infacmd sql *(Fortsetzung)*
Einrichten von Berechtigungen für einen SQL-Datendienst 933
Einrichten von Berechtigungen in Spalten für virtuelle Tabellen 931
Einrichten von Gruppen- und Benutzerberechtigungen für virtuelle Tabellen 939
Konfigurieren von Eigenschaften für virtuelle Tabellen 951
Spaltenoptionen 947
SQL-Datendienst-Optionen 949
Starten des SQL-Datendiensts 941
Umbenennen des SQL-Datendiensts 929
Virtuelle Tabellenoptionen 953
infacmd sqlupdate, Optionen für virtuelle Spalten 945
infacmd tdm
Aktivieren des Test Data Manager-Diensts 962
Deaktivieren des Test Data Manager-Diensts 963
Test Data Manager-Dienste in einer Domäne erstellen 954
Test Data Manager-Dienstinhalte in einer Domäne erstellen 960
infacmd wfs
Aktualisieren dauerhafter Zuordnungsausgaben 986
Auflisten aktiver Arbeitsablaufinstanzen 976
Auflisten dauerhafter Zuordnungsausgaben 978
Auflisten der Arbeitsabläufe in einer Anwendung 982
Auflisten von Arbeitsablaufparametern 980
eine Arbeitsablaufinstanz abbrechen 970
eine Arbeitsablaufinstanz stornieren 966
eine Arbeitsablaufinstanz wiederherstellen 984
Entfernen von Datenbanktabellen 974
Starten einer Ablaufinstanz 989
infacmd ws
Aktualisieren von Eigenschaften für einen Webdienst 1020
Aktualisieren von Eigenschaften für einen Webdienstvorgang 1017
Auflisten der Berechtigungen für einen Webdienst 1002
Auflisten der Berechtigungen für einen Webdienstvorgang 998
Auflisten von Eigenschaften für einen Webdienstvorgang. 996
ListOperationOptions 996
ListOperationPermissions 998
ListWebServiceOptions 1000
ListWebServicePermissions 1002
ListWebServices 1004
RenameWebService 1006
SetOperationPermissions 1008
SetWebServicePermissions 1011
StartWebService 1014
StopWebService 1016
UpdateOperationOptions 1017
UpdateWebServiceOptions 1020
infacmd xrf
Aktualisieren von Export-XML 1024
Generieren einer lesbaren XML-Datei 1024
Infacmd-Befehle
Abrufen der Hilfe 453
infasetup
Arbeitsknoten, Aktualisieren 1092
Arbeitsknoten, Definieren 1068
ausführen 1045
Chiffre-Suites aktualisieren 1089
Domäne, Definieren 1049
Domäne, Löschen 1072
Domäne, Sichern 1046
Domäne, Wiederherstellen 1079
Gateway-Knoten, Aktualisieren 1083
Gateway-Knoten, Definieren 1062
Listen mit Chiffre-Suites anzeigen 1077
Rückgabewerte 1045
INFATOOL_DATEFORMAT
Konfigurieren 55
Informatica-Dienstprogramme (Installieren 28
Informatica-Dienstprogramme (Sicherheitskonfiguration 31

Inhalt
Importieren aus Anwendungsdateien 857
InstallAbapProgram (pmrep)
Beschreibung 1184
Integrationsdienst
Aktualisieren mit infacmd isp 621
Entfernen mit infacmd isp 562
Erstellen 360
Zuweisen zum Metadata Manager-Dienst 274
Integrationsdienst-Prozess
Abrufen von Eigenschaften 435
Aktualisieren der Optionen für 649
Interaktiver Modus für pmcmd
Festlegen von Standardwerten 1100
Verbinden 1100

K

KillUserConnection (pmrep)
Beschreibung 1187
Knoten
Abrufen des Namens von 432
Aktualisieren 633
Aktualisieren der Gateway mit infasetup 1083
Aktualisieren der Rolle 635
Aktualisieren des Arbeitsknotens mit infasetup 1092
Auflisten mit infacmd isp 509
Auflisten von allen in einer Domäne 499
Auflisten von Optionen mit infacmd isp 494
Auflisten von Rollen 497
Definieren des Gateways mit infasetup 1062
Definieren von Arbeitsknoten mit infasetup 1068
Entfernen aus Domänen 553
Hinzufügen von Ressourcen 256
Hinzufügen zu Domänen 248
Pingen 527
Trennen von Domänen mit infacmd isp 608
Wechseln von Arbeits- zu Gateway-Knoten mit infacmd 591
Wechseln von Gateway- zu Arbeitsknoten mit infacmd isp 593
konfigurieren
Befehlszeilendienstprogramme 29
Konnektivität
Verbindungsstring, Beispiele 1149

L

LDAP-Authentifizierung
Einrichten mit infacmd isp 582
LDAP-Severkonfiguration
Aktualisieren mit infacmd isp 585
Auflisten mit infacmd isp 503
LDAP-Verbindung
Auflisten mit infacmd isp 489
Links
Hinzufügen zu Domänen 246
List (infacmd ps) 775
listActiveWorkflowInstances
infacmd wfs 976
ListAlertUsers (infacmd isp)
Beschreibung 459
ListAllGroups (infacmd isp)
Beschreibung 460
ListAllRoles (infacmd isp)
Beschreibung 462
ListAllUsers (infacmd isp)
Beschreibung 463
ListAllUsers (pmrep)
Beschreibung 1188
ListApplicationObjectPermissions (infacmd dis) 139
ListApplicationObjects (infacmd dis) 141
ListApplicationOptions (infacmd dis) 143
ListApplications (infacmd dis) 145
ListBackupFiles (infacmd mrs) 695
ListCheckedOutObjects (infacmd mrs) 697
ListColumnOptions (infacmd sql) 911
ListComputeNodeAttributes (infacmd rms) 849
ListComputeOptions (infacmd dis) 146, 190
ListConnectionOptions (infacmd isp)
Beschreibung 473
ListConnectionPermissionByUser (infacmd isp) 469
ListConnectionPermissions (infacmd isp) 465
ListConnectionPermissionsByGroup (infacmd isp)
Beschreibung 467
ListConnections (infacmd isp)
Beschreibung 471
ListConnections (pmrep)
Beschreibung 1187
ListDataObjectOptions (infacmd dis) 148
ListDefaultOSProfiles (infacmd isp) 475
ListDomainLinks (infacmd isp)
Beschreibung 477
ListDomainOptions (infacmd isp)
Beschreibung 479
ListFolders (infacmd isp)
Beschreibung 480
ListFOlders (infacmd mrs) 699
listGlossary (infacmd bg) 90
ListGridNodes (infacmd isp)
Beschreibung 482
ListGroupPermissions (infacmd isp) 483
ListGroupPrivileges (infacmd isp)
Beschreibung 485
ListGroupsForUser (infacmd isp) 487
ListLDAPConnectivity (infacmd isp)
Beschreibung 489
ListLicenses (infacmd isp)
Beschreibung 491
ListLockedObjects (infacmd mrs) 701
listMappingPersistedOutputs
infacmd wfs 978
ListMappings (infacmd ms) 739
listMonitoringOptions (infacmd isp) 493
ListNodeOptions (infacmd isp)
Beschreibung 494
ListNodeResources (infacmd isp)
Beschreibung 496
ListNodeRoles (infacmd isp) 497
ListNodes (infacmd isp)
Beschreibung 499
ListObjectDependencies (pmrep)
Beschreibung 1188
ListObjects (pmrep)
Auflisten von Ordnern 1195
Beschreibung 1190
Transformationstypen 1192
ListOperationOptions
infacmd ws 996
ListOSProfiles (infacmd isp)
Beschreibung 501
ListParameterSetObjects (infacmd dis) 152
ListParameterSets (infacmd dis) 154
ListPlugins (infacmd) 60
ListProjects (infacmd mrs) 703

ListRepositoryLDAPConfiguration (infacmd isp)
Beschreibung 503
ListRolePrivileges (infacmd isp)
Beschreibung 504
ListSchedule (infacmd sch) 875
ListSecurityDomains (infacmd)
Beschreibung 506
ListSequenceObjectProperties (infacmd dis) 155
ListSequenceObjects (infacmd dis) 157
ListServiceLevels (infacmd isp)
Beschreibung 508
ListServiceNodes (infacmd isp)
Beschreibung 509
ListServiceOptions (infacmd as) 67
ListServiceOptions (infacmd cms) 108
ListServiceOptions (infacmd dis) 159
ListServiceOptions (infacmd mrs) 705
ListServiceOptions (infacmd rms) 851
ListServiceOptions (infacmd sch) 877
ListServiceOptions (infacmd search) 902
ListServicePrivileges (infacmd isp)
Beschreibung 511
ListServiceProcessOptions (infacmd as) 69
ListServiceProcessOptions (infacmd cms) 110
ListServiceProcessOptions (infacmd dis) 161
ListServiceProcessOptions (infacmd mrs) 707
ListServiceProcessOptions (infacmd sch) 879
ListServiceProcessOptions (infacmd search) 904
ListServices (infacmd isp)
Beschreibung 513
ListSMTPOptions (infacmd isp) 515
ListSQLDataServiceOptions (infacmd sql) 915
ListSQLDataServicePermissions (infacmd sql) 917
ListSQLDataServices (infacmd sql) 918
ListStoredProcedurePermissions (infacmd sql) 920
ListTableOptions (infacmd sql) 922
ListTablePermissions (infacmd sql) 913, 924
ListTablesBySess (pmrep)
Beschreibung 1196
ListTaskListener (infacmd pwx) 828
ListUserConnections (pmrep)
Beschreibung 1197
ListUserPermissions (infacmd isp) 517
ListUserPrivileges (infacmd isp)
Beschreibung 519
ListWebServiceOptions
infacmd ws 1000
ListWebServicePermissions
infacmd ws 1002
ListWebServices
infacmd ws 1004
listWorkflowParameters
infacmd wfs 980
listWorkflows
infacmd wfs 982
Lizenzen
Aktualisieren mit infacmd isp 623
Anzeigen mit infacmd isp 588
Aufheben der Zuweisung mit infacmd 601
Auflisten mit infacmd isp 491
Auflisten von zugewiesenen Diensten 270
Entfernen mit infacmd isp 551
Hinzufügen zu Domänen 252
Logische Datenobjekte
Bereinigen des Caches 162
Optionen für infacmd 194
logischer Datenobjekt-Cache
Aktualisierung stoppen für 130
Lokale Parameterdateien
Verwenden mit pmcmd StartWorkflow 1134

M

Mapping
Einrichten von Berechtigungen 174
Mappings
Auflisten 739
MassUpdate (pmrep)
Beschreibung 1197
Metadata Manager-Dienst
Aktualisieren von Eigenschaften für 625
Erstellen in einer Domäne 370
Metadata Manager-Dienstprogramme
Installation 28
konfigurieren 30
Sicherheitskonfiguration 31
Microsoft SQL Server
Verbindungsstring-Syntax 1149
MigrateEncryptionKey (infasetup)
Beschreibung 1078
migrateProfileResults (infacmd ps) 777
migrateScorecards (infacmd ps) 779
migrateUsers
infacmd isp 521
Modellrepository
Aktualisiert Dienstprozessoptionen für den Modellrepository-Dienst 729
Aktualisiert Optionen für den Modellrepository-Dienst 723
Auflisten von ausgecheckten Objekten in 697
Auflisten von Dateien im Backup-Ordner 695
Auflisten von gesperrten Objekten in 701
Auflisten von Ordnern im Repository des Modellrepository-Diensts 699
Auflisten von Projekten im Repository des Modellrepository-Dienst 703
Einchecken von Objekten 679
Entsperren eines Objekts in 721
Erstellt die Objektabhängigkeitsgrafik neu. 713
Listet Optionen für den Modellrepository-Dienst auf 705
Löschen des Inhalts 689
Neuzuweisung eines ausgecheckten Objekts in 711
Neuzuweisung eines gesperrten Objekts in 711
Sichern von Inhalten in einer Datei 677
Upgraden von Inhalten des Modellrepository-Dienst 731
Wiederherstellen der Inhalte 717
Wiederherstellen von ausgecheckten Objekten in 719
Modellrepository-Dienst
Auflisten 707
Erstellen 686
Erstellen von Repository-Inhalt 680
Modellrepository-Objekte
Exportieren 233
Wiederverwendung eines Berichtsobjekts 239
ModifyFolder (pmrep)
Beschreibung 1204
MoveFolder (infacmd isp)
Beschreibung 523
MoveObject (infacmd isp)
Beschreibung 525

N

Nachträgliche E-Mail für die Sitzung
Aktualisieren von Adressen mit pmrep 1225

Notify (pmrep)
Beschreibung 1205

O

ObjectExport (pmrep)
Beschreibung 1205
ObjectImport (pmrep)
Beschreibung 1207
Objekte
Bereitstellen in einer Archivdatei 748
Einchecken 1161
Entfernen von Benutzerberechtigungen 569
Exportieren 1205
Exportieren in Objektexportdatei 749
Importieren 1207
Importieren aus Objektexportdatei 755
Löschen 1174
Zuweisen von Benutzerberechtigungen 283
Objektimport-Steuerdatei
Beschreibung 1238
Olson-Zeitzone
gültige Werte 869
Optionen des Datenintegrationsdiensts
infacmd-Syntax 199
Optionen des Ressourcenmanager-Diensts
infacmd-Syntax 856
Optionen des Scheduler-Diensts
infacmd-Syntax 892, 895
Oracle
Verbindungsoptionen für 338
Verbindungsstring-Syntax 1149
Ordner
Aktualisieren der Beschreibung mit infacmd isp 616
Ändern 1204
Auflisten mit infacmd isp 480
Bereitstellen 1176
Entfernen mit infacmd isp 542
Erstellen in einer Domäne 355
Löschen 1173
Verschieben mit infacmd isp 523
Verschieben von Objekten zwischen Ordnern mit infacmd isp 525
OVERRIDEFOLDER
Beispielsteuerdatei 1255

P

Parameterdateien
Verwenden mit pmcmd StartTask 1130
Verwenden mit pmcmd StartWorkflow 1134
Passwörter
Verschlüsseln 56
Zurücksetzen von Benutzerpasswörtern mit infacmd isp 576
PauseAll (infacmd sch) 881
PauseSchedule (infacmd sch) 882
Persistente Eingabedatei
Erstellen mit pmrep 1236
Ping (infacmd isp)
Beschreibung 527
PingService (pmcmd)
Beschreibung 1121
Plug-Ins
XML-Vorlagen 1213
pmcmd
Arbeitsabläufe, Abbrechen 1105
Arbeitsabläufe, Abrufen von Informationen über 1110, 1117
pmcmd *(Fortsetzung)*
Arbeitsabläufe, Beenden 1137
Arbeitsabläufe, Entfernen aus einem Zeitplan 1139
Arbeitsabläufe, Ermitteln der Ausführung 1143
Arbeitsabläufe, Planen 1124
Arbeitsabläufe, Starten 1131
Arbeitsabläufe, Wiederherstellen 1122
Aufgaben, Abbrechen 1103
Aufgaben, Abrufen von Informationen über 1110, 1115
Aufgaben, Abschließen vor der Zurückgabe der Eingabeaufforderung 1141
Aufgaben, Anhalten 1135
Aufgaben, Starten 1127
Ausführen in einer Domäne für verschiedene Versionen 1098
Befehlszeilenmodus 1098
Integration Service, Anpingen 1121
Integration Service, Trennen von 1108
Integration Service, Verbinden mit 1107
Interaktiver Modus 1100
Interaktiver Modus, Beenden 1109
nowait-Modus, Einrichten 1126
Ordner, Festlegen für die Ausführung von Befehlen 1126
Ordner, Kennzeichnen als Nicht-Standardordner 1141
Parameterdateien 1130, 1134
PowerCenter Integration Service, Abrufen der Eigenschaften 1112
Rückgabewerte 1099
Service-Einstellungen, Abrufen 1127
Sitzungen, Abrufen von Informationen über 1109
Sitzungsstatistiken, Abrufen 1113
Skriptdateien 1102
Version, Anzeigen 1141
wait-Modus, Einrichten 1127
pmpasswd
Syntax 56
Verschlüsseln von Passwörtern 56
pmrep
Abfragen, Ausführen 1178
Ausführen in einer Domäne für verschiedene Versionen 1148
Ausgecheckte Objekte, Auflisten 1180
Befehlszeilenmodus 1148
Benachrichtigungsmeldungen, Senden 1205
Benutzer, Auflisten 1188
Benutzereigenschaften, Bearbeiten 1178
Benutzerverbindungen, Auflisten 1197
Benutzerverbindungen, Beenden 1187
Berechtigung, Zuweisen 1158
Berechtigungen, Entfernen 1216
Bereitstellung, Rollback 1216
Bereitstellungs-Steuerdatei-Parameter 1251
Bereitstellungsgruppen, Bereitstellen 1175
Bereitstellungsgruppen, Erstellen 1168
Bereitstellungsgruppen, Hinzufügen von Objekten zu 1153
Bereitstellungsgruppen, Löschen 1173
Bereitstellungsgruppen, Löschen von Objekten aus 1162
Beschriftungen, Anwenden 1155
Beschriftungen, Erstellen 1171
Beschriftungen, Löschen 1173
Checkouts, Rückgängig machen 1219
connections, updating 1223
Deinstallieren des ABAP-Programms 1230
E-Mail-Adressen, Aktualisieren 1225
Generieren des ABAP-Programms 1182
Gruppen, Erstellen 1171
hilfe 1184
Installieren des ABAP-Programms 1184
Interaktiver Modus 1148
Interaktiver Modus, Beenden 1180
Namenspräfixe von Target-Tabellen, Aktualisieren 1228

pmrep *(Fortsetzung)*
Objektabhängigkeiten, Auflisten 1188
Objekte, Ändern des Eigentümers 1161
Objekte, Auflisten 1190
Objekte, Einchecken 1161
Objekte, Exportieren 1205
Objekte, Importieren 1207
Objekte, Löschen 1174
Objekte, Validieren 1231
Objektversionen, Bereinigen 1208
Ordner, Ändern von Eigenschaften 1204
Ordner, Auflisten 1195
Ordner, Bereitstellen 1176
Ordner, Erstellen 1169
Ordner, Löschen 1173
Ordnereigenschaften, Ändern 1204
Persistente Eingabedateien, Erstellen 1236
Plug-Ins, Aufheben der Registrierung 1221
Plug-Ins, Registrieren 1212
PowerCenter-Integrationsdienst, zuweisen 1157
Protokolle, Löschen 1218
Repositories, Aufheben der Registrierung 1220
Repositories, Erstellen 1164
Repositories, Löschen 1171
Repositories, Registrieren 1211
Repositories, Sichern 1160
Repositories, Wiederherstellen 1214
Repository-Statistiken, Aktualisieren 1228
Repository-Verbindungsdatei, Angeben 54
Repositorys, Verbinden mit 1163
Ressourcen, Bereinigen 1162
Sequenzwerte, Aktualisieren 1225
Skriptdateien 1150
Skripts, Ausführen 1216
Steuerparameter für Objektimport 1239
Tabellen, Auflisten nach Sitzung 1196
Tabelleneigentümernamen, Aktualisieren 1227
Übersicht 1148
Verbindungen, Auflisten 1187
Verbindungen, Erstellen 1165
Verbindungen, Löschen 1172
Verbindungsdetails, Auflisten 1182
Verbindungsinformationen, Anzeigen 1217
Verbindungsname, Ändern 1218
Versionsinformationen, Anzeigen 1234
PopulateVCS (infacmd mrs) 709
PowerCenter IntegrationService
Zuweisen mit pmrep 1157
PowerCenter-Dienstprogramme
Installation 28
konfigurieren 29
Sicherheitskonfiguration 31
PowerCenter-Ressourcen
Aktivieren 411
Deaktivieren 400
PowerExchange-Listenerdienst
Aktualisieren von Eigenschaften 840
Anhalten 788
Anzeigen von Überwachungsstatistiken für den Listenerdienst und dessen Aufgaben 819
Auflisten von Aufgaben 828
Beenden von Aufgaben 834
Erstellen 797
Erzwingen des Abbruchs 785
PowerExchange-Protokollierungsdienst
Aktualisieren von Eigenschaften 844
Anzeigen aller Nachrichten 804
Anzeigen der Anzahl an verarbeiteten Änderungsdatensätzen 816
PowerExchange-Protokollierungsdienst *(Fortsetzung)*
Anzeigen der Speichernutzung 813
Anzeigen des Status der Writer-Unteraufgabe 822
Anzeigen von CPU-Informationen 807
Anzeigen von Ereignissen 810
Erstellen 799
Herunterfahren 831
Starten des Protokollierungszyklus 791
Wechseln zu einem neuen Satz an Logdateien. 825
PrintSPNAndKeytabNames (infacmd isp) 528
Profilaufgaben
Abrufen des Status 772, 783
Profile
Auflisten von Ergebnissen für 775
Ausführen 767
Bereinigen von Ergebnissen für 780
Profiling Warehouse-Inhalte
Entfernen 766
Profilmodell
Abrufen des Status 773
ausführen 770
Wird abgebrochen 762
Protokollereignisse
Bereinigen mit infacmd isp 530
Trunkieren mit pmrep 1218
Purge (infacmd ps) 780
PurgeDataObjectCache (infacmd dis) 162
PurgeLog (infacmd isp)
Beschreibung 530
PurgeMonitoringOptions (infacmd isp) 532
PurgeResultSetCache (infacmd dis) 165
PurgeTableCache (infacmd sql) 925
PurgeVersion (pmrep)
Beschreibung 1208

R

reassignCheckedOutObject (infacmd mrs) 711
rebuildDependencyGraph (infacmd mrs) 713
recoverWorkflow
infacmd wfs 984
Referenztabellen
Exportieren 859
Importieren in Modellrepositorys 862
RefreshDataObjectCache (infacmd dis) 166
RefreshTableCache (infacmd sql) 927
Register (pmrep)
Beschreibung 1211
RegisterPlugin (pmrep)
Beschreibung 1212
Registrieren
Plug-In mit pmrep 1212
Sicherheitsmodul mit pmrep 1213
RemoveAlertUser (infacmd isp)
Beschreibung 534
RemoveConnection (infacmd isp)
Beschreibung 536
RemoveConnectionPermissions (infacmd isp)
Beschreibung 538
RemoveDomainLink (infacmd isp)
Beschreibung 540
RemoveFolder (infacmd isp)
Beschreibung 542
RemoveGrid (infacmd isp)
Beschreibung 544
RemoveGroup (infacmd isp)
Beschreibung 545

RemoveGroupPermission (infacmd isp) 547
RemoveGroupPrivilege (infacmd isp)
Beschreibung 549
RemoveLicense (infacmd isp)
Beschreibung 551
RemoveNode (infacmd isp)
Beschreibung 553
RemoveNodeResource (infacmd isp)
Beschreibung 555
RemoveOSProfile (infacmd isp)
Beschreibung 557
RemoveRole (infacmd isp)
Beschreibung 558
RemoveRolePrivilege (infacmd isp)
Beschreibung 560
RemoveService (infacmd cms) 115
RemoveService (infacmd isp)
Beschreibung 562
RemoveServiceLevel (infacmd isp)
Beschreibung 564
RemoveUser (infacmd isp)
Beschreibung 566
RemoveUserFromGroup (infacmd isp)
Beschreibung 568
RemoveUserPermission (infacmd isp) 569
RemoveUserPrivilege (infacmd isp)
Beschreibung 572
RenameApplication (infacmd dis) 168
RenameConnection (infacmd isp) 574
RenameFolder (infacmd mrs) 715
RenameSQLDataService (infacmd sql) 929
RenameWebService
infacmd ws 1006
Repositories
Aufheben der Registrierung 1220
Löschen von Details aus 1218
Registrieren 1211
Sichern mit pmrep 1160
Repository-Dienst
Aktualisieren mit infacmd isp 641
Entfernen mit infacmd isp 562
Erstellen in einer Domäne 380
Repositorys
Erstellen von relationalen 1165
Verbinden mit pmrep 1163
ResetPassword (infacmd isp)
Beschreibung 576
Ressourcen
Anzeigen mit infacmd isp 496
Entfernen mit infacmd isp 555
Exportieren in Objektexportdatei 753
Ressourcenmanager-Dienst
Auflisten von Eigenschaften für 851
Konfigurieren von Eigenschaften für 854
Restore (pmrep)
Beschreibung 1214
RestoreApplication (infacmd dis) 170
RestoreContents (infacmd mrs) 717
RestoreDARepositoryContents (infacmd isp)
Beschreibung 1269
RestoreDomain (infasetup)
Beschreibung 1079
ResumeAll (infacmd sch) 884
ResumeSchedule (infacmd sch) 885
resyncData (infacmd cms) 116
RevertObject (infacmd mrs) 719
RmPrivilege (pmrep)
Beschreibung 1216
RollbackDeployment (pmrep)
Beschreibung 1216
Rollen
Auflisten mit infacmd isp 462
Entfernen aus einer Gruppe mit infacmd isp 602
Entfernen mit infacmd isp 558
Entfernen von einem Benutzer mit infacmd isp 605
Erstellen in einer Domäne 385
Exportieren mit infacmd isp 418
Importieren mit infacmd isp 453
Zuweisen zu einem Benutzer mit infacmd isp 279
Rückgabewerte
infacmd 62
infasetup 1045
pmcmd 1099
Run (pmrep)
Beschreibung 1216
RunCPUProfile (infacmd isp)
Beschreibung 578
RunMapping
infacmd ms 741

S

SAP BW-Dienst
Aktualisieren mit infacmd isp 646
Erstellen in einer Domäne 387
ScheduleWorkflow (pmcmd)
Beschreibung 1124
Schemadateien
infacmd-Steuerdateien 1027
Scorecards
Auflisten von Ergebnissen für 775
Ausführen 767
Bereinigen von Ergebnissen für 780
Migrieren 779
SEQ
infacmd-Verbindungsoptionen 344
SetApplicationObjectPermissions (infacmd dis) 174
SetApplicationPermissions (infacmd dis) 172
SetColumnPermissions (infacmd sql) 931
SetComputeNodeAttributes (infacmd rms) 852
SetConnectionPermissions (infacmd isp) 580
SetFolder (pmcmd)
Beschreibung 1126
SetLDAPConnectivity (infacmd isp)
Beschreibung 582
setMappingPersistedOutputs
infacmd wfs 986
SetNoWait (pmcmd)
Beschreibung 1126
SetOperationPermissions
infacmd ws 1008
SetRepositoryLDAPConfiguration (infacmd isp)
Beschreibung 585
SetSequenceState (infacmd dis) 177
SetSQLDataServicePermissions (infacmd sql) 933
SetStoredProcedurePermissions (infacmd sql) 936
SetTablePermissions (infacmd sql) 939
SetWait (pmcmd)
Beschreibung 1127
SetWebServicePermissions
infacmd ws 1011
ShowConnectionInfo (pmrep)
Beschreibung 1217
ShowLicense (infacmd isp)
Beschreibung 588

ShowSettings (pmcmd)
Beschreibung 1127
ShutDownLogger (infacmd pwx) 831
ShutdownNode (infacmd isp)
Beschreibung 590
Sicherheitsdomänen
Auflisten mit infacmd 506
Sitzungen
Abrufen von Protokollereignissen 441
Skriptdateien
running 1216
Verwenden für pmrep-Befehle 1150
Spalte
Optionen für infacmd 947
Spalte für virtuelle Tabelle
Einrichten von Berechtigungen 931
Spalten
Auflisten von Eigenschaften für 911
SQL-Datendienst
Aktualisieren der Optionen für 948
Anhalten 943
Auflisten für einen Datenintegrationsdienst 918
Auflisten von Berechtigungen 917
Auflisten von Eigenschaften für 915
Einrichten von Berechtigungen 933
Optionen für infacmd 949
Starten 941
Umbenennen 929
StartApplication (infacmd dis) 179
StartSQLDataService (infacmd sql) 941
StartTask (pmcmd)
Beschreibung 1127
Verwenden einer Parameterdatei 1130
StartWebService
infacmd ws 1014
startWorkflow
infacmd wfs 989
StartWorkflow (pmcmd)
Beschreibung 1131
Verwenden einer Parameterdatei 1134
Statistiken
Aktualisieren des Repository 1228
Steuerdatei
Bereitstellung 1249
ObjectImport XML-Beispiel 1242
Objektimport 1238
Steuerdateien
Beispiele für Domänenobjekte 1041
Beispiele für Model Repository-Objekte 1042
Benennungskonventionen 1027
infacmd 1026
Parameter für Domänenobjekte 1028, 1033
Parameter für Modellrepository-Objekte 1030, 1035
Regeln und Richtlinien 1040
Schemadateien 1027
StopApplication (infacmd dis) 181
stopBlazeService (infacmd dis) 183
StopSQLDataService (infacmd sql) 943
StopTask (pmcmd)
Beschreibung 1135
StopTaskListener (infacmd pwx) 834
StopWebService
infacmd ws 1016
StopWorkflow (pmcmd)
Beschreibung 1137
Suchdienst
Auflisten von Eigenschaften für 902
erstellen 899
Suchdienst *(Fortsetzung)*
Konfigurieren von Eigenschaften für 906
Suchdienstprozess
Auflisten von Eigenschaften für 904
Konfigurieren von Eigenschaften für 908
SwitchConnection (pmrep)
Beschreibung 1218
SwitchToGatewayNode (infacmd)
Beschreibung 591
SwitchToKerberosMode (infasetup)
beschreibung 1082
SwitchToWorkerNode (infacmd isp)
Beschreibung 593
synchronizeProfile (infacmd ps) 783
SyncSecurityDomains (infacmd isp) 595
syntax
infacmd-Optionen des Ressourcenmanager-Diensts 856
Syntax
Befehlszeilenprogramme 34
infacmd-Optionen des Datenintegrationsdiensts 199
infacmd-Optionen des Scheduler-Diensts 892, 895

T

Tabelleneigentümername
Aktualisieren mit pmrep 1227
TDM-Dienst
deaktivieren 963
Test Data Manager-Dienst
in einer Domäne erstellen 954, 960
TruncateLog (pmrep)
Beschreibung 1218

U

Überwachungsdaten bereinigen (infacmd isp) 532
Umgebungsvariablen
ICMD_JAVA_OPTS 41
INFA_CLIENT_RESILIENCE_TIMEOUT 42
INFA_CODEPAGENAME 43
INFA_DEFAULT_DATABASE_PASSWORD 43
INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD 45
INFA_DEFAULT_DOMAIN 46
INFA_DEFAULT_DOMAIN_PASSWORD 46
INFA_DEFAULT_DOMAIN_USER 47
INFA_DEFAULT_PWX_OSEPASSWORD 48
INFA_DEFAULT_PWX_OSPASSWORD 49
INFA_JAVA_CMD_OPTS 50
INFA_NODE_KEYSTORE_PASSWORD 52
INFA_NODE_TRUSTSTORE_PASSWORD 53
INFA_PASSWORD 51
INFA_REPCNX_INFO 54
INFA_REPOSITORY_PASSWORD 55
INFATOOL_DATEFORMAT 55
Konfigurieren von Befehlszeilenprogrammen 40
UnassignDefaultOSProfile (infacmd isp) 597
UnassignISMMService (infacmd)
Beschreibung 599
UnassignLicense (infacmd)
Beschreibung 601
UnassignRoleFromGroup (infacmd isp)
Beschreibung 602
UnassignRoleFromUser (infacmd isp)
Beschreibung 605
UnassignRSWSHubService (infacmd isp)
Beschreibung 607

UnassociateDomainNode (infacmd isp)
Beschreibung 608
UndeployApplication (infacmd dis) 185
UndoCheckout (pmrep)
Beschreibung 1219
UninstallAbapProgram (pmrep)
Beschreibung 1230
unlockObject (infacmd mrs) 721
Unregister (pmrep)
Beschreibung 1220
UnregisterPlugin (pmrep)
Beschreibung 1221
UnscheduleWorkflow (pmcmd)
Beschreibung 1139
UnsetFolder (pmcmd)
Beschreibung 1141
UpdateApplication (infacmd dis) 186
UpdateApplicationOptions (infacmd dis) 188
UpdateColumnOptions (infacmd sql) 945
UpdateConnection (infacmd isp)
Beschreibung 610
UpdateConnection (pmrep)
description 1223
UpdateDataObjectsOptions (infacmd dis) 192
UpdateDomainOptions (infacmd isp)
Beschreibung 614
UpdateEmailAddr (pmrep)
Beschreibung 1225
updateExportXML
infacmd xrf 1024
UpdateFolder (infacmd isp)
Beschreibung 616
UpdateGatewayInfo (infacmd isp)
Beschreibung 618
UpdateGatewayInfo (infacmd) 62
UpdateGatewayNode (infasetup)
Beschreibung 1083
UpdateGrid (infacmd isp)
Beschreibung 619
UpdateIntegrationService (infacmd isp)
Beschreibung 621
UpdateKerberosAdminUser (infasetup)
beschreibung 1088
UpdateKerberosConfig (infasetup)
Beschreibung 1089
UpdateLicense (infacmd isp)
Beschreibung 623
UpdateListenerService (infacmd pwx) 840
UpdateLoggerService (infacmd pwx) 844
UpdateMMService (infacmd isp)
Beschreibung 625
UpdateMonitoringOptions (infacmd isp) 627
UpdateNamespace (infacmd isp) 630
UpdateNodeOptions (infacmd isp)
Beschreibung 633
UpdateNodeRole (infacmd isp) 635
UpdateOperationOptions
infacmd ws 1017
UpdateOSProfile (infacmd isp)
Beschreibung 638
UpdateParameterSetEntries (infacmd dis) 195
UpdateReportingService (infacmd isp)
Beschreibung 1271
UpdateRepositoryService (infacmd isp)
Beschreibung 641
UpdateSAPBWService (infacmd isp)
Beschreibung 646
UpdateSchedule (infacmd sch) 887
UpdateSeqGenVals (pmrep)
Beschreibung 1225
UpdateServiceLevel (infacmd isp)
Beschreibung 648
UpdateServiceOptions (infacmd as) 71
UpdateServiceOptions (infacmd cms) 118
UpdateServiceOptions (infacmd dis) 197
UpdateServiceOptions (infacmd mrs) 723
UpdateServiceOptions (infacmd rms) 854
UpdateServiceOptions (infacmd sch) 891
UpdateServiceOptions (infacmd search) 906
UpdateServiceProcess (infacmd isp)
Beschreibung 649
UpdateServiceProcessOptions (infacmd as) 73
UpdateServiceProcessOptions (infacmd cms) 120
UpdateServiceProcessOptions (infacmd dis) 210
UpdateServiceProcessOptions (infacmd mrs) 729
UpdateServiceProcessOptions (infacmd sch) 894
UpdateServiceProcessOptions (infacmd search) 908
UpdateSMTPOptions (infacmd isp)
Beschreibung 652
UpdateSQLDataServiceOptions (infacmd sql) 948
UpdateSrcPrefix (pmrep)
Aktualisieren von nicht wiederverwendbaren Sitzungen 1227
Beschreibung 1227
UpdateStatistics (pmrep)
Beschreibung 1228
UpdateTableOptions (infacmd sql) 951
UpdateTargPrefix (pmrep)
Aktualisieren von nicht wiederverwendbaren Sitzungen 1228
Beschreibung 1228
UpdateWebServiceOptions
infacmd ws 1020
UpdateWorkerNode (infasetup)
Beschreibung 1092
UpdateWSHubService (infacmd isp)
Beschreibung 653
Upgrade (infacmd cms) 122
Upgrade (infacmd sch) 896
UpgradeContents (infacmd mrs) 731
UpgradeDARepositoryContents (infacmd isp)
Beschreibung 1272
UpgradeDARepositoryUsers (infacmd isp)
Beschreibung 1274
UpgradeModels (infacmd pwx) 837
upgradeRepository (infacmd bg) 88

V

Validate (pmrep)
Beschreibung 1231
ValidateandRegisterFeature (infasetup)
beschreibung 1096
validateFeature (infacmd advanced) 655
Validieren von Objekten
Mit pmrep 1231
Verbindung
Web Content-Kapow Katalyst 353
Verbindung des parallelen Teradata-Transporters
infacmd 346
Verbindungen
Aktualisieren mit infacmd isp 610
Auflisten mit infacmd isp 471
Auflisten von Optionen mit infacmd isp 473
Entfernen aus Domänen mit infacmd isp 536
Erstellen mit infacmd 287
Exportieren mit infacmd isp 418

Verbindungen *(Fortsetzung)*
Importieren mit infacmd isp 453
Oracle 338
Umbenennen mit infacmd 574
Verbindungsberechtigungen
Auflisten für Benutzer oder Gruppen 465
Auflisten mit infacmd isp 467
Hinzufügen zu Benutzern oder Gruppen 244
Verbindungsoptionen
DB2 für infacmd 318
SEQ für infacmd 344
VSAM für infacmd 351
Verbindungsstring
Beispiele 1149
Syntax 1149
Version (infacmd)
Beschreibung 657
Version (pmcmd)
Beschreibung 1141
Version (pmrep)
Beschreibung 1234
Virtuelle Schemata
Auflisten von Berechtigungen 910
virtuelle Spalten
Auflisten von Berechtigungen 913
Virtuelle Spalten
Aktualisieren der Optionen 945
Virtuelle Tabellen
Auflisten von Berechtigungen 924
Auflisten von Eigenschaften für 922
Einrichten von Berechtigungen 939
Konfigurieren von Eigenschaften für 951
Optionen für infacmd 953
VSAM
infacmd-Verbindungsoptionen 351

W

Wait-Modus
Konfigurieren mithilfe von pmcmd 1101
WaitTask (pmcmd)
Beschreibung 1141
WaitWorkflow (pmcmd)
Beschreibung 1143
Web Content-Kapow Katalyst
Verbindung 353
Web-Dienst-Optionen
infacmd-Syntax 1022
Webdienst
Aktualisieren von Eigenschaften für 1020
Auflisten mit infacmd 1004
Auflisten von Berechtigungen 1002
Auflisten von Eigenschaften für 1000
Beenden mit infacmd 1016
Festlegen von Berechtigungen mit infacmd 1011
Starten mit infacmd 1014
Umbenennen mit infacmd 1006
Webdienst-Hub
Aktualisieren mit infacmd isp 653
Erstellen in einer Domäne 394
Trennen eines Repository mit infacmd isp 607
Verbinden eines Repository mit infacmd isp 281
Webdienstvorgang
Aktualisieren von Eigenschaften für 1017
Auflisten von Berechtigungen 998
Auflisten von Eigenschaften für 996
Festlegen von Berechtigungen mit infacmd 1008
Wiederherstellen
Repositories mit pmrep Restore 1214

X

XML-Datei
Plug-In-Vorlagen 1213

Z

Zeitzonen
gültige Werte für Zeitplan 869
Zuordnungsausgaben
Aktualisieren mit infacmd 986
Zuordnungsprotokoll
Zugreifen mit infacmd ms 734
Zur Eingabe eines Namens, der ein Leerzeichen oder andere nicht alphanumerische Zeichen enthält, setzen Sie den Namen in Anführungszeichen. (infacmd cms) 112