



Informatica®
9.6.1 HotFix 4

Administrator Guide

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 und zwar einschließlich, 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 © University of 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 GARANTIE ODER KONTINGENTEN IRGEND EINER 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/license.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/jaservice/>, <http://www.postgresql.org/about/license.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.schneider.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: 2018-07-18

Inhalt

Einleitung	15
Informatica-Ressourcen.	15
Informatica-Netzwerk.	15
Informatica-Dokumentation.	16
Informatica-Produktverfügbarkeitsmatrizen.	16
Informatica-Website.	16
Informatica-Ratgeberbibliothek.	16
Informatica-Wissensdatenbank.	16
Informatica Support TV.	16
Informatica Marketplace.	17
Informatica Velocity.	17
Globaler Kundensupport von Informatica.	17
 Kapitel 1: Grundlagen zu den Domänen.....	 18
Grundlagen zu den Domänen - ÜbersichtGrundlagen zum Administrator-Tool.	18
Knoten.	19
Gateway-Knoten.	20
Worker-Knoten.	20
Dienstmanager.	20
Application Services.	23
Analyst-Dienst.	24
Content Management Service.	25
Data Integration Service.	25
Metadata Manager Service.	25
Modellrepository-Dienst.	25
PowerCenter Integration Service.	26
PowerCenter-Repository-Dienst.	26
PowerExchange Listener Service.	26
PowerExchange Logger Service.	26
Reporting Service.	27
Berichterstellungs- und Dashboard-Dienst (veraltet).	27
SAP BW Service.	27
Web Services Hub.	28
Hohe Verfügbarkeit.	28
Informatica Data Usage Policy.	28
Konfigurieren der Informatica-DiscoveryIQ Proxy-Details.	29
Deaktivieren der Informatica-Datennutzung.	29
 Kapitel 2: Eigenes Konto verwalten.....	 30
Eigenes Konto verwalten - Übersicht.	30

Anmelden bei Informatica Administrator.	30
Informatica Administrator-URL.	31
Fehlerbehebung bei der Anmeldung bei Informatica Administrator.	31
Passwortverwaltung.	32
Ändern Ihres Passwortes.. . . .	32
Einstellungen bearbeiten.	32
Einstellungen.	33
Informatica Network Credentials.	33
Informatica Network-Anmeldedaten eingeben.	33
Suchen der Informatica-Wissensdatenbank.	33

Kapitel 3: Informatica Administrator..... 34

Informatica Administrator verwenden - Übersicht.	34
Registerkarte Domäne - Übersicht.	36
Registerkarte Domäne - Ansicht Dienste und Knoten.	36
Domäne.	38
Ordner.	39
Application Services.	39
Knoten KnotenKnoten.	44
Gitter.	45
Lizenzen.	45
Registerkarte „Verwalten“ – Verbindungsansicht.	46
Registerkarte "Protokolle".	46
Registerkarte Berichte.	47
Registerkarte "Überwachen".	47
Registerkarte Sicherheit.	48
Der Suchbereich.	48
Der Sicherheits-Navigator.	48
Gruppen.	49
Benutzer.	50
Rollen.	50
Dienststatus.	51
Prozessstatus.	51
Jobstatus.	53
Tastenkombinationen.	54

Kapitel 4: Domänenverwaltung..... 56

Domänenverwaltung - Übersicht.	56
Alarmverwaltung.	57
Konfigurieren der SMTP-Einstellungen.	58
Alarmer abbonieren.	58
Alarmer anzeigen.	59
Ordnerverwaltung.	59

Erstellen eines Ordners.	60
Objekte in einen Ordner verschieben.	60
Entfernen eines Ordners	61
Domänensicherheitsmanagement.	61
Sicherheitsverwaltung für Benutzer.	62
Anwendungsdienstverwaltung.	62
Aktivieren und Deaktivieren von Diensten und Dienstprozessen.	63
Dienstprozesse anzeigen.	64
Konfigurieren des Neustarts für Dienstprozesse.	64
Anwendungsdienste entfernen.	64
Problembehebung für Anwendungsdienste.	65
Knotenverwaltung.	65
Hinzufügen von Knoten zur Domäne.	66
Konfigurieren der Knoteneigenschaften.	67
Prozesse auf Knoten anzeigen.	70
Herunterfahren und Neustarten des Knotens.	70
Entfernen der Knotenzuordnung.	71
Entfernen eines Knotens.	71
Gateway-Konfiguration.	72
Domänenkonfigurationsverwaltung.	72
Sichern der Domänenkonfiguration.	73
Wiederherstellen der Domänen-Konfiguration.	73
Migrieren der Domänen-Konfiguration.	74
Aktualisieren der Domänenkonfigurationsdatenbankverbindung.	76
Domänenaufgaben.	77
Verwalten und Überwachen von Anwendungsdiensten und Knoten	
Überwachen von Anwendungsdiensten und Knoten	
Verwalten und Überwachen von Anwendungsdiensten und Knoten.	77
Anzeigen von Abhängigkeiten für Anwendungsdienste, Knoten und Gitter	
Anzeigen von Abhängigkeiten	
Abhängigkeiten anzeigen.	79
Herunterfahren einer Domäne.	81
Domäneneigenschaften.	81
Allgemeine Eigenschaften.	82
Datenbankeigenschaften.	83
Gateway-Konfigurationseigenschaften.	84
Dienstebenenverwaltung.	85
SMTP-Konfiguration.	86
Benutzerdefinierte Eigenschaften für die Domäne.	86
Kapitel 5: Hohe Verfügbarkeit.	87
Hohe Verfügbarkeit - Übersicht.	87
Belastbarkeit.	88
Belastbarkeit der Anwendungs-Clients.	88

Anwendungsdienst-Belastbarkeit.	89
Knoten-Belastbarkeit.	89
Beispielkonfiguration für ein Belastbarkeits-Timeout.	90
Neustart und Failover.	91
Domänen-Failover.	91
Anwendungsdienst - Neustart und Failover.	91
Wiederherstellung.	92
Konfiguration für einen hochverfügbare Domäne.	93
Konfiguration der Belastbarkeit für Anwendungsdienste.	94
Failover-Konfiguration für einen Anwendungsdienst.	94
Konfiguration für Failover und Wiederherstellung des PowerCenter-Integrationsdienstes.	95
Konfiguration der Belastbarkeit für Befehlszeilenprogramme.	96
Domänen-Failover-Konfiguration.	96
Konfiguration des Knoten-Neustarts.	97
Netzwerk, hohe Verfügbarkeit.	97
Kapitel 6: Verbindungen.	99
Verbindungen - Übersicht.	99
Verbindungsverwaltung.	99
Erstellen einer Verbindung.	100
Aktualisieren der Verbindungsliste.	101
Anzeigen einer Verbindung.	101
Konfigurieren des Pooling für eine Verbindung.	102
Bearbeiten und Testen einer Verbindung.	102
Löschen einer Verbindung.	102
Pass-Through-Sicherheit.	103
Pass-Through-Sicherheit mit Datenobjekt-Zwischenspeicherung.	104
Pass-Through-Sicherheit hinzufügen	104
Poolingeigenschaften von Verbindungsobjekten.	105
Kapitel 7: Verbindungseigenschaften.	106
Adabas-Verbindungseigenschaften.	106
DataSift-Verbindungseigenschaften.	109
Facebook-Verbindungseigenschaften.	110
Greenplum-Verbindungseigenschaften.	111
HBase Connection Properties.	112
HDFS Connection Properties.	113
Hive-Verbindungseigenschaften.	114
HTTP-Verbindungseigenschaften.	121
Eigenschaften von IBM DB2-Verbindungen.	123
Eigenschaften von IBM DB2 für i5/OS-Verbindungen.	125
Eigenschaften von IBM DB2 für z/OS-Verbindungen.	129
IMS-Verbindungseigenschaften.	132

Propriedades da Conexão do JDBC.	135
LinkedIn-Verbindungseigenschaften.	138
MS SQL Server-Verbindungseigenschaften.	139
ODBC-Verbindungseigenschaften.	142
Eigenschaften für Oracle-Verbindungen.	143
Salesforce-Verbindungseigenschaften.	145
SAP-Verbindungseigenschaften.	146
Eigenschaften sequenzieller Verbindungen.	148
Propriedades de Conexão do Teradata Parallel Transporter.	150
Twitter-Verbindungseigenschaften.	152
Streaming-Verbindungseigenschaften für Twitter.	153
VSAM-Verbindungseigenschaften.	154
Eigenschaften von Web Content-Kapow Katalyst-Verbindungen.	157
Verbindungseigenschaften für Web Services.	158
 Kapitel 8: Exportieren und Importieren von Domänenobjekten.	 161
Export und Import von Domänenobjekten - Übersicht	161
Exportprozess.	162
Regeln und Richtlinien für das Exportieren von Domänenobjekten.	162
Domänenobjekte anzeigen.	162
Darstellbare Domänenobjektnamen.	163
Importprozess.	169
Regeln und Richtlinien für den Import von Domänenobjekten.	169
Konfliktlösung.	170
 Kapitel 9: Lizenzverwaltung.	 171
Lizenzverwaltung - Übersicht.	171
Lizenzvalidierung.	172
Lizenzierungsprotokollereignisse.	172
Lizenzverwaltungstasks.	173
Arten von Lizenzschlüsseln.	173
Originalschlüssel.	173
Inkrementelle Schlüssel.	174
Ein Lizenzobjekt erstellen.	174
Eine Lizenz einem Dienst zuweisen.	175
Regeln und Richtlinien zum Zuweisen von Lizenzen an einen Dienst.	175
Entfernen eine Lizenz von einem Anwendungsdienst.	176
Aktualisieren einer Lizenz.	176
Entfernen einer Lizenz.	177
Lizenzeigenschaften.	178
Lizenzdetails.	178
Unterstützte Plattformen.	180
Repositorys.	181

Dienstoptionen.	181
Verbindungen.	181
Metadaten austausch-Optionen.	181
Kapitel 10: Log-Verwaltung.	182
Protokollverwaltung - Übersicht.	182
Protokoll-Manager-Architektur.	183
Log-Ereignisse der PowerCenter-Sitzung und des Arbeitsablaufs.	184
Protokollmanager-Wiederherstellung.	184
Fehlersuche für den Log Manager.	185
Protokollspeicherort.	185
Log-Verwaltung - Konfiguration.	185
Bereinigen von Log-Ereignissen.	186
Zeitzone.	186
Log-Management-Eigenschaften konfigurieren.	187
Die Registerkarte Logs.	187
Anzeigen von Protokollereignissen.	187
Konfigurieren von Log-Spalten.	189
Speichern von Log-Ereignissen.	190
Exportieren von Log-Ereignissen.	190
Fehlerprotokoll im Administrator Tool.	192
Protokollereignisse.	192
Protokollereignisse - Komponenten.	193
Domänenprotokollereignisse.	194
Log-Ereignisse im Analyst Service.	195
Protokollereignisse des Data Integration Service.	195
Log-Ereignisse des Listener Service.	195
Logger Service Konfigurationseigenschaften.	196
Protokollereignisse des Modellrepository-Dienst.	196
Benutzerdefinierte Rollen für den Metadata Manager Service.	196
Log-Ereignisse des PowerCenter Integration Service.	196
Log-Ereignisse des PowerCenter Repository Service.	197
Log-Ereignisse des Reporting Service.	197
Log-Ereignisse des SAP BW Service.	198
Log-Ereignisse des Web Services Hub.	198
Protokollereignisse der Benutzeraktivität.	198
Protokoll-Aggregator.	199
Aggregieren von Anwendungsdienstprotokollen.	199
Verarbeiten von aggregierten Anwendungsdienstprotokollen.	200
Kapitel 11: Überwachung.	201
Überwachen - Übersicht.	201
Navigator der Registerkarte "Überwachen".	202

Ansichten der Registerkarte "Überwachen".	203
Statistik auf der Registerkarte "Überwachen".	204
Berichte auf der Registerkarte "Überwachen".	205
Konfigurieren der Überwachung.	208
Schritt 1. Konfigurieren der globalen Einstellungen.	208
Schritt 2. Konfigurieren der Ansichten „Berichte“ und „Statistiken“.	209
Data Integration Services überwachen	210
Eigenschaftensicht für einen Data Integration Service.	210
Berichtsansicht für einen Data Integration Service.	211
Überwachen von Jobs.	211
Anzeigen von Protokollen für einen Ad-hoc-Job.	212
Abbrechen eines Ad-hoc-Jobs.	212
Überwachen von Anwendungen.	212
Eigenschaftensicht für eine Anwendung.	213
Berichtsansicht einer Anwendung.	213
Bereitgestellte Mapping-Jobs überwachen.	213
Logs für einen bereitgestellten Mapping-Job anzeigen.	214
Bereitgestellten Zuordnungsjob erneut ausgeben.	214
Bereitgestellten Mapping-Job abbrechen.	214
Logische Datenobjekte überwachen.	215
Eigenschaftensicht für ein logisches Datenobjekt.	215
Ansicht "Cache-Aktualisierungsdurchläufe" für ein logisches Datenobjekt.	215
Logs für Datenobjekt-Cache-Aktualisierungsdurchläufe.	215
SQL-Datendienste überwachen.	216
Eigenschaftensicht für einen SQL-Datendienst.	216
Verbindungsansicht für einen SQL Data Service.	216
Anfrageansicht eines SQL-Datendienstes.	217
Virtuelle Tabellen für einen SQL-Datendienst anzeigen.	218
Berichtsansicht eines SQL-Datendienstes.	219
Web-Dienste überwachen.	219
Eigenschaftensicht für einen Web-Dienst.	219
Berichtsansicht eines Web-Dienstes.	219
Operationsansicht für einen Web-Dienst.	220
Anfrageansicht eines Webdienstes.	220
Überwachen von Arbeitsabläufen.	220
Arbeitsablaufgrafik	221
Anzeigen von Arbeitsablaufobjekten.	221
Arbeitsablaufstatus.	222
Arbeitsablaufobjektstatus.	224
Arbeitselementstatus der Mapping-Aufgabe.	226
Abbrechen eines Arbeitsablaufs.	227
Arbeitsablauf-Wiederherstellung.	227

Wiederherstellen eines Arbeitsablaufs.	229
Arbeitsablaufprotokolle.	229
Überwachen eines Ordners von Objekten.	230
Anzeigen des Kontexts eines Objekts.	231
Konfigurieren des benutzerdefinierten Filters für Datum und Uhrzeit.	231
Konfigurieren des benutzerdefinierten Filters für abgelaufene Zeit.	232
Konfigurieren des benutzerdefinierten Filters Mehrfachauswahl.	232
Überwachen eines Objekts.	232

Kapitel 12: Domänenberichte..... 233

Domänenberichte - Übersicht.	233
Lizenzverwaltungsbericht.	233
Lizenzierung.	234
CPU-Zusammenfassung.	235
CPU-Detail.	235
Repository-Zusammenfassung	236
Benutzerzusammenfassung.	236
Benutzerdetail.	237
Hardwarekonfiguration.	237
Knotenkonfiguration.	238
Lizenzierte Optionen.	238
Lizenzverwaltungsbericht ausführen.	239
Lizenzverwaltungsbericht in einer E-Mail verschicken.	240
Web Services-Bericht.	240
Über den Web-Dienste-Bericht.	240
Allgemeine Eigenschaften und Zusammenfassung für den Web Services Hub	242
Historienstatistik-Tabelle für Web Services.	243
Laufzeitstatistiken für Web Services.	243
Web-Dienst-Eigenschaften.	244
Top IP-Adressen des Web-Dienstes.	244
Historienstatistik-Tabelle für Web-Dienst.	245
Ausführen des Web Services Report.	245
Web Services Report für einen sicheren Web Services Hub ausführen.	246

Kapitel 13: Knotendiagnostiken..... 248

Knotendiagnostiken - Übersicht.	248
Anmeldung beim Informatica MySupport-Portal.	249
Anmelden beim Informatica MySupport-Portal.	249
Generieren der Knotendiagnostik.	250
Knotendiagnostiken herunterladen.	251
Knotendiagnostiken hochladen.	251
Knotendiagnostik analysieren.	252
Fehlerbehebungsmöglichkeiten erkennen.	252

Identifizieren von Empfehlungen.	253
Kapitel 14: Informationen zur Globalisierung.....	254
Globalisierung - Übersicht.	254
Unicode.	255
Mit einem Unicode PowerCenter Repository arbeiten.	255
Gebietsschemata.	256
Systemgebietsschema.	257
Benutzerschema.	257
Eingabe-Gebietsschema.	257
Datenverschiebungsmodi.	257
Zeichendatenverschiebungs-Modes.	258
Ändern der Datenverschiebungsmodi.	258
Codepages - Übersicht.	259
UNIX Codepages.	260
Windows Codepages.	261
Auswählen einer Codepage.	261
Codepage-Kompatibilität.	261
Codepage der Domänenkonfigurationsdatenbank.	263
Codepage des Administrator Tools.	263
Codepage des PowerCenter Client.	264
Codepage des PowerCenter Integration Service-Prozesses.	264
PowerCenter Repository-Codepage.	264
Codepage für Metadaten Manager-Repository.. . . .	265
PowerCenter-Quell-Codepage.	265
PowerCenter-Target-Codepage.	266
Befehlszeilenprogramm-Codepages.	266
Codepage-Kompatibilität - Zusammenfassung.	267
Codepage-Validierung.	269
Entspannte Codepage-Validierung.	270
Konfigurieren des PowerCenter Integration Service.	271
Kompatible Quell- und Target-Codepages auswählen.	271
Fehlerbehebung für Codepage-Lockerung.	271
PowerCenter Codepage-Umwandlung.	272
Auswählen von Zeichen für PowerCenter Repository Metadaten.	272
Fallstudie: ISO 8859-1 Datenverarbeitung.	273
Die ISO 8859-1-Umgebung.	273
ISO 8859-1 Umgebung konfigurieren.	274
Fallstudie: Verarbeiten von Unicode UTF-16LE Daten.	276
Die UTF-8-Umgebung.	276
UTF-16LE Umgebung konfigurieren.	276

Kapitel 15: Informatica Cloud-Verwaltung.....	279
Informatica Cloud-Verwaltung - Übersicht	279
Informatica Cloud-Organisationen	279
Eigenschaften der Informatica Cloud-Organisation.	280
Hinzufügen einer Organisation.	280
Entfernen einer Organisation.	280
Bearbeiten von Informatica Cloud-Anmeldedaten.	280
Informatica Cloud-Sicherheitsagent.	281
Informatica Cloud-Verbindungen.	281
 Anhang A: Codepages.....	 282
Unterstützte Codepages für Anwendungsdienste.	282
Unterstützte Codepages für Quellen und Ziele.	284
 Anhang B: Befehlszeilenberechtigungen.....	 295
infacmd as Befehle.	295
infacmd dis Befehle.	296
infacmd ipc Befehlsprogramme.	298
infacmd isp-Befehle.	298
infacmd mrs Befehlsprogramme.	309
infacmd ms Befehlsprogramme.	310
infacmd oie Befehlsprogramme.	311
infacmd ps Befehlsprogramme.	311
infacmd pwx - Befehle.	312
infacmd rtm Befehlsprogramme.	313
infacmd sql - Befehle.	313
infacmd rds Befehlsprogramme.	315
infacmd wfs-Befehle.	315
pmcmd-Befehle.	315
pmrep Befehlsprogramme.	318
 Anhang C: Benutzerdefinierte Rollen.....	 324
Benutzerdefinierte Rolle für den Analyst-Dienst.	324
Benutzerdefinierte Rollen für den Metadata Manager-Dienst.	325
Benutzerdefinierte Rolle für den Operator.	327
PowerCenter-Repository-Dienst - Benutzerdefinierte Rollen.	328
Benutzerdefinierte Rollen für den Berichterstellungsdienst.	329
Benutzerdefinierte Rollen für den Test Data Manager-Dienst.	336
 Anhang D: Konnektivität der Informatica-Plattform.....	 341
Konnektivität der Informatica-Plattform - Übersicht.	341
Domänen-Konnektivität.	342

Model Repository-Konnektivität.	343
PowerCenter-Konnektivität.	344
Repository Service-Konnektivität.	346
Integration Service-Konnektivität.	346
PowerCenter Client-Konnektivität.	348
Reporting Service- und Metadata Manager Service-Konnektivität.	349
Native Konnektivität.	349
ODBC-Konnektivität.	350
JDBC-Konnektivität.	351
Anhang E: Konfigurieren des Webbrowsers.	352
Konfigurieren des Webbrowsers.	352
Anhang F: Sicherheitskonzepte.	353
Was ist eine Gruppe?.	353
Was ist ein Benutzer?.	353
Was ist eine Rolle?.	354
Was ist eine Berechtigung?.	354
Was ist ein Betriebssystemprofil?.	354
Index.	355

Einleitung

Das *Informatica Administrator-Handbuch* *PowerCenter Express Administrator-Handbuch* richtet sich an Informatica-Benutzer. Es enthält Informationen, die Sie zum Verwalten der Domäne und der Sicherheit benötigen. Das *Informatica Administrator-Handbuch* *PowerCenter Express Administrator-Handbuch* setzt voraus, dass Sie über grundlegende Kenntnisse über Informatica *PowerCenter Express* verfügen.

Das *Administratorhandbuch für Ultra Messaging System Monitoring* wurde für Administratoren verfasst. Es beschreibt die Verwendung von Informatica Administrator (das Administrator-Tool) zur Verwaltung des Monitoring-Tools und der Benutzer. Bei der Lektüre wird vorausgesetzt, dass Sie über grundlegende Kenntnisse des Ultra Messaging-Konzepts verfügen.

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.

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.
- Ihr lokales Informatica-Netzwerk für Benutzergruppen suchen und mit anderen Benutzern zusammenarbeiten.

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. Der Zugriff auf die PAMs erfolgt über das Informatica My Support-Portal unter <https://mysupport.informatica.com/community/my-support/product-availability-matrices>.

Informatica-Website

Auf die Unternehmenswebsite von Informatica können Sie unter <https://www.informatica.com> zugreifen. Auf der Website finden Sie Informationen über Informatica, seinen Hintergrund, bevorstehende Veranstaltungen und Niederlassungen. Darüber hinaus finden Sie dort Produkt- und Partnerinformationen. Der Bereich „Services“ enthält wichtige Informationen zur technischen Unterstützung, zu Schulungen und zu den Implementierungsdienstleistungen.

Informatica-Ratgeberbibliothek

Bei der Ratgeberbibliothek handelt es sich um eine Sammlung aus kurzen Artikeln und Tutorials mit Lösungen zu allgemeinen Problemen, Vergleichsfunktionen und Verhalten. Darüber hinaus finden Sie in der Bibliothek Anleitungen für die Durchführung realer Aufgaben.

Zum Auffinden von Ratgeberartikeln für Ihr Produkt durchsuchen Sie die Informatica-Wissensdatenbank unter <https://kb.informatica.com>.

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 Support TV

Informatica Support TV bietet verschiedene Videos, die Ihnen erklären, wie Sie spezifische Aufgaben erfolgreich bewältigen. Sie können Support TV-Videos in der Informatica-Wissensdatenbank unter <https://kb.informatica.com> durchsuchen.

Wenn Sie Fragen, Anregungen oder Ideen zu Informatica Support TV haben, wenden Sie sich per E-Mail an das Support TV-Team unter supportvideos@informatica.com oder senden Sie einen Tweet an @INFASupport.

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>.

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 <https://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.

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

Grundlagen zu den Domänen

Dieses Kapitel umfasst die folgenden Themen:

- [Grundlagen zu den Domänen - ÜbersichtGrundlagen zum Administrator-Tool, 18](#)
- [Knoten, 19](#)
- [Dienstmanager, 20](#)
- [Application Services, 23](#)
- [Hohe Verfügbarkeit, 28](#)
- [Informatica Data Usage Policy, 28](#)

Grundlagen zu den Domänen - ÜbersichtGrundlagen zum Administrator-Tool

Informatica verfügt über eine dienstorientierte Architektur, die die Fähigkeit zur Skalierung von Diensten und zum gemeinsamen Nutzen von Ressourcen über mehrere Rechner aufweist. Die Funktionalität der hohen Verfügbarkeit minimiert Dienstaussfallzeiten aufgrund unerwarteter Ausfälle und geplanter Wartung in der Informatica-Umgebung.

Die Informatica-Domäne stellt die grundlegende Verwaltungseinheit in Informatica dar. Die Domäne unterstützt die Verwaltung der verteilten Dienste. Eine Domäne ist eine Zusammenstellung von Knoten und Diensten, die Sie auf der Grundlage des Verwaltungseigentumsverhältnisses in Ordnern gruppieren können.

Die Informatica-Domäne stellt die grundlegende Verwaltungseinheit in Informatica dar. Die Domäne unterstützt die Verwaltung der verteilten Dienste. Eine Domäne enthält einen Knoten und Dienste.

Ein Knoten entspricht der logischen Darstellung eines einzelnen Computers in einer Domäne. Ein Knoten in der Domäne fungiert als Gateway für Dienstanforderungen von Clients und leitet sie an den entsprechenden Dienst und Knoten weiter. Dienste und Prozesse laufen auf Knoten in einer Domäne. Die Verfügbarkeit eines Dienstes oder Prozesses auf einem Knoten hängt davon ab, wie Sie den Dienst und den Knoten konfigurieren.

Ein Knoten entspricht der logischen Darstellung eines einzelnen Computers in einer Domäne. Der Knoten fungiert als Gateway, das Client-Anfragen empfängt und diese an den geeigneten Dienst weiterleitet. Dienste und Prozesse werden auf dem Knoten in einer Domäne ausgeführt. Die Verfügbarkeit eines Dienstes oder Prozesses auf einem Knoten hängt davon ab, wie Sie den Dienst und den Knoten konfigurieren.

Im Administrator-Tool werden die administrativen Aufgaben für Domänenobjekte zusammengefasst. Sie verwalten die Domäne und die Sicherheit der Domäne mithilfe des Administrator-Tools.

Die Informatica-Domäne stellt die grundlegende Verwaltungseinheit in Informatica dar. Die Domäne unterstützt die Verwaltung der verteilten Dienste. Eine Domäne enthält einen Knoten und Dienste.

Ein Knoten entspricht der logischen Darstellung eines einzelnen Computers in einer Domäne. Der Knoten fungiert als Gateway, das Client-Anfragen empfängt und diese an den geeigneten Dienst weiterleitet. Dienste und Prozesse werden auf dem Knoten in einer Domäne ausgeführt. Die Verfügbarkeit eines Dienstes oder Prozesses auf einem Knoten hängt davon ab, wie Sie den Dienst und den Knoten konfigurieren.

Zu den Diensten für die Domäne gehören der Service Manager und eine Reihe von Anwendungsdiensten:

- **Dienstmanager.** Ein Dienst, der alle Domänenoperationen verwaltet. Es führt die Anwendungsdienste und Domänenfunktionen auf jedem Knoten in der Domäne aus. Einige Domänenfunktionen beinhalten Authentifizierung, Autorisierung und Protokollierung.
- **Anwendungsdienste** Dienste, die serverbasierte Funktionalität darstellen, wie z. B. der Modellrepository-Dienst und der Datenintegrationsdienst. Die Anwendungsdienste, die auf einem Knoten laufen, hängen davon ab, wie Sie die Dienste konfigurieren.

Zu den Diensten für die Domäne gehören der Dienstmanager und der Ultra Messaging-Dienst:

- **Dienstmanager.** Ein Dienst, der alle Domänenoperationen verwaltet. Es führt die Anwendungsdienste und Domänenfunktionen auf jedem Knoten in der Domäne aus. Einige Domänenfunktionen beinhalten Authentifizierung, Autorisierung und Protokollierung.
- **Ultra Messaging-Dienst.** Ein Anwendungsdienst, der auf einem Knoten ausgeführt wird.

Der Service Manager und die Anwendungsdienste steuern die Sicherheit. Der Service Manager verwaltet die Benutzer und Gruppen, die sich bei den Anwendungs-Clients anmelden können, und authentifiziert die Benutzer, die sich bei den Anwendungs-Clients anmelden. Der Service Manager und die Anwendungsdienste autorisieren Benutzeranfragen von Anwendungs-Clients.

Das Administrator-Tool umfasst die administrativen Aufgaben für Domänenobjekte, wie Dienste, Knoten, Lizenzen und Gitter. Sie verwalten die Domäne und die Sicherheit der Domäne mithilfe des Administrator-Tools.

In Informatica Administrator (dem Administrator-Tool) werden die administrativen Aufgaben für Domänenobjekte zusammengefasst. Sie verwalten die Domäne und die Sicherheit der Domäne mithilfe des Administrator-Tools.

Wenn Sie über die Option der hohen Verfügbarkeit im PowerCenter verfügen, können Sie Dienste skalieren und einzelne Ausfallpunkte für Dienste eliminieren. Dienste können, trotz temporärer Netzwerk- oder Hardware-Ausfälle, weiterhin ausgeführt werden.

Knoten

Ein Knoten entspricht einer logischen Darstellung eines einzelnen Computers in einer Domäne. Fügen Sie während der Installation die Installationsmaschine als Knoten zur Domäne hinzu. Sie können einer Domäne mehrere Knoten hinzufügen.

Jeder Knoten in der Domäne führt den Dienstmanager aus, der die Domänenfunktionen auf dem jeweiligen Knoten verwaltet. Zudem unterstützt der Dienstmanager die auf dem Knoten ausgeführten Anwendungsdienste. Die Domänenfunktionen und Dienste, die ein Knoten ausführt, sind abhängig von den folgenden Knotenkonfigurationen:

Knotentyp

Der Knotentyp legt fest, ob der Knoten als Gateway-Knoten oder als Worker-Knoten dient, und bestimmt die Domänenfunktionen, die der Knoten ausführt. Einer der Gateway-Knoten dient als Master-Gateway-Knoten für die Domäne. Der Master-Gateway-Knoten empfängt Dienstanfragen von Clients und leitet diese an den entsprechenden Dienst und Knoten weiter. Ein Worker-Knoten ist ein Knoten, der nicht als

Gateway konfiguriert ist. Bei der ersten Installation der Informatica-Dienste erstellen Sie einen Gateway-Knoten und die Informatica-Domäne. Beim Installieren der Informatica-Dienste auf anderen Computern erstellen Sie weitere Gateway-Knoten oder Worker-Knoten, die Sie zur Domäne hinzufügen.

Knotenrolle

Die Knotenrolle gibt den Zweck des Knotens an. Ein Knoten mit der Dienstrolle kann Anwendungsdienste ausführen. Ein Knoten mit der Berechnungsrolle kann Berechnungen durchführen, die von Remote-Anwendungsdiensten angefragt werden. Ein Knoten mit beiden Rollen kann Anwendungsdienste ausführen und lokal Berechnungen für diese Dienste durchführen. Standardmäßig sind für alle Gateway- und Worker-Knoten sowohl die Dienst- als auch die Berechnungsrolle aktiviert. 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.

Sie können Alarmer abonnieren, um Benachrichtigungen über Knotenereignisse zu erhalten, wie z. B. Knotenfehler oder die Wahl eines Master-Gateways. Zudem können Sie Knotendiagnostiken generieren und in den Configuration Support Manager hochladen sowie Informationen über verfügbare EBF-Dateien und Informatica-Empfehlungen anzeigen.

Gateway-Knoten

Ein Gateway-Knoten ist ein Knoten, den Sie konfigurieren, damit er als Gateway für die Domäne eingesetzt werden kann. Ein Gateway-Knoten kann Anwendungsdienste und Berechnungen ausführen und als Master-Gateway-Knoten dienen. Zu einem gegebenen Zeitpunkt fungiert nur ein Gateway-Knoten als Master-Gateway. Der Master-Gateway-Knoten ist der Eingangspunkt zur Domäne.

Alle Domänenfunktionen auf dem Master-Gateway-Knoten werden vom Dienstmanager des Master-Gateway-Knotens ausgeführt. Die auf den anderen Gateway-Knoten laufenden Dienstmanager führen eingeschränkte Domänenvorgänge auf diesen Knoten aus.

Sie können mehr als einen Knoten als Gateway konfigurieren. Ist der Master-Gateway-Knoten nicht verfügbar, wählen die Dienstmanager auf anderen Gateway-Knoten einen anderen Master-Gateway-Knoten aus. Wenn Sie nur einen Knoten als Gateway konfigurieren und der Knoten unverfügbar wird, kann die Domäne keine Dienstanfragen annehmen.

Worker-Knoten

Ein Arbeitsknoten ist ein beliebiger Knoten, den Sie nicht als Gateway für die Domäne konfigurieren. Ein Worker-Knoten kann Anwendungsdienste ausführen und Berechnungen durchführen, er kann jedoch nicht als Gateway dienen. Der Dienstmanager führt auf einem Worker-Knoten nur eingeschränkte Domänenfunktionen aus.

Dienstmanager

Der Dienstmanager ist ein Dienst, der alle Domänenoperationen verwaltet. Er wird im Informatica-Dienst ausgeführt. Er läuft als Dienst unter Windows und als Dämon unter UNIX. Beim Starten der Informatica-Dienste wird auch der Dienstmanager gestartet.

Der Dienstmanager wird auf jedem Knoten ausgeführt. Wenn der Dienstmanager nicht läuft, ist der Knoten nicht verfügbar.

Der Dienstmanager läuft auf allen Knoten in der Domäne, um zu Anwendungsdienste und die Domäne zu unterstützen:

- **Anwendungsdienst-Support.** Der Dienstmanager auf den einzelnen Knoten startet Anwendungsdienste, deren Ausführung für den jeweiligen Knoten konfiguriert ist. Er startet und stoppt Dienste und Dienstprozesse entsprechend den Anfragen von Clients. Außerdem leitet er Dienstanfragen an Anwendungsdienste weiter. Der Dienstmanager verwenden TCP/IP für die Kommunikation mit den Anwendungsdiensten.
- **Domänen-Support.** Der Dienstmanager führt auf jedem Knoten Funktionen aus, um die Domäne zu unterstützen. Welche Funktionen der Dienstmanager auf einem Knoten ausführt, hängt von der Art des Knotens ab. Zum Beispiel führt der Dienstmanager, der auf dem Master-Gateway-Knoten läuft, alle Domänenfunktionen auf diesem Knoten aus. Der Dienstmanager, der auf einem anderen Knoten läuft, führt einige Domänenfunktionen auf dem jeweiligen Knoten aus.

Wenn der Computer, auf dem Sie PowerCenter Express Personal Edition installieren, sich im Energiesparmodus oder Ruhezustand befindet, startet der Dienstmanager die Dienste neu, wenn der Computer erneut aktiviert wird. Wenn der Computer, auf dem Sie PowerCenter Express Personal Edition installieren, sich im Energiesparmodus oder Ruhezustand befindet, müssen Sie die Informatica-Dienste neu starten, wenn der Computer aktiviert wird.

Um die Informatica-Dienste über das Windows-Startmenü zu starten, klicken Sie auf **Programme > Informatica PowerCenter Express > Informatica-Dienste starten**.

Führen Sie unter Linux `infaservice.sh` aus, um den Informatica-Dämon zu starten. `infaservice.sh` ist standardmäßig im folgenden Verzeichnis installiert:

```
<PowerCenterExpressInstallationDir>/tomcat/bin
```

Führen Sie den folgenden Befehl im Verzeichnis durch, in dem sich `infaservice.sh` befindet:

```
infaservice.sh startup
```

In der nachstehenden Tabelle sind die vom Dienstmanager ausgeführten Domänenfunktionen beschrieben:

Funktion	Beschreibung
Alarme	Der Dienstmanager sendet Alarme an abonnierte Benutzer. Sie abonnieren Alarme und Benachrichtigung bei Knotenausfall und Master-Gateway-Wahl auf der Domäne und für Dienstprozess-Failover bei Diensten auf der Domäne. Wenn Sie Alarme abonnieren, erhalten Sie Benachrichtigungs-E-Mails.
Authentifizierung	Der Dienstmanager authentifiziert Benutzer, die sich bei Anwendungs-Clients anmelden. Die Authentifizierung findet auf dem Master-Gateway-Knoten statt.
Autorisierung	Der Dienstmanager autorisiert Benutzeranfragen für Domänenobjekte anhand der Berechtigungen und Rollen, die dem Benutzer zugewiesen sind. Anfragen können vom Administrator-Tool ausgehen. Die Domänen-Autorisierung findet auf dem Master-Gateway-Knoten statt. Einige Anwendungsdienste autorisieren Benutzeranforderungen für andere Objekte.
Domänenkonfiguration	Der Dienstmanager verwaltet die Metadaten der Domänenkonfiguration. Die Domänenkonfiguration findet auf dem Master-Gateway-Knoten statt.
Knotenkonfiguration	Der Dienstmanager verwaltet die Metadaten der Knotenkonfiguration in der Domäne. Die Knotenkonfiguration findet auf allen Knoten der Domäne statt.

Funktion	Beschreibung
Lizenzierung	Der Dienstmanager registriert Lizenzinformationen und überprüft diese beim Ausführen der Anwendungsdienste. Die Lizenzierung findet auf dem Master-Gateway-Knoten statt.
Protokollieren	Der Dienstmanager liefert akkumulierte Protokollereignisse von jedem Anwendungsdienst in der Domäne und für Sitzungen und Arbeitsabläufe. Um die Protokollierungsfunktion durchzuführen, führt der Dienstmanager einen Protokollmanager und einen Protokollagenten aus. Der Protokollmanager wird auf dem Master-Gateway-Knoten ausgeführt. Der Protokollagent wird auf allen Knoten ausgeführt, auf denen der PowerCenter-Integrationsdienst läuft.
Benutzerverwaltung	Der Dienstmanager authentifiziert native und LDAP-Benutzer und Gruppen, die sich bei Anwendungs-Clients anmelden. Darüber hinaus verwaltet er die Erstellung von Rollen und die Zuweisung von Rollen und Berechtigungen zu nativen und LDAP-Benutzern und Gruppen. Die Benutzerverwaltung findet auf dem Master-Gateway-Knoten statt.
Überwachung	Der Dienstmanager unternimmt das Halten, Aktualisieren, Abrufen und Veröffentlichen von Laufzeit-Statistiken für Integrationsobjekte im Modellrepository. Der Dienstmanager speichert die Überwachungskonfiguration im Domänenkonfigurations-Repository.

Funktion	Beschreibung
Alarme	Der Dienstmanager sendet Alarme an abonnierte Benutzer.
Authentifizierung	Der Dienstmanager authentifiziert Benutzer, die sich bei Anwendungs-Clients anmelden. Die Authentifizierung findet auf dem Master-Gateway-Knoten statt.
Autorisierung	Der Dienstmanager autorisiert Benutzeranfragen für Domänenobjekte anhand der Berechtigungen und Rollen, die dem Benutzer zugewiesen sind.
Domänenkonfiguration	Der Dienstmanager verwaltet die Metadaten der Domänenkonfiguration.
Knotenkonfiguration	Der Dienstmanager verwaltet die Metadaten der Knotenkonfiguration in der Domäne.
Lizenzierung	Der Dienstmanager registriert Lizenzinformationen und überprüft diese beim Ausführen der Anwendungsdienste.
Protokollieren	Der Dienstmanager liefert akkumulierte Protokollereignisse aus jedem Dienst in der Domäne sowie für Arbeitsabläufe. Um die Protokollierungsfunktion durchzuführen, führt der Dienstmanager einen Protokollmanager und einen Protokollagenten aus.

Funktion	Beschreibung
Benutzerverwaltung	Der Dienstmanager verwaltet die Benutzer und Gruppen, die sich bei Anwendungs-Clients anmelden können. Darüber hinaus verwaltet er die Erstellung von Rollen und die Zuweisung von Rollen und Berechtigungen zu Benutzern und Gruppen.
Überwachung	Der Dienstmanager unternimmt das Halten, Aktualisieren, Abrufen und Veröffentlichen von Laufzeit-Statistiken für Integrationsobjekte im Modellrepository. Der Dienstmanager speichert die Überwachungskonfiguration im Domänenkonfigurations-Repository.

Funktion	Beschreibung
Alarmer	Der Dienstmanager sendet Alarmer an abonnierte Benutzer.
Authentifizierung	Der Dienstmanager authentifiziert Benutzer, die sich bei Anwendungs-Clients anmelden. Die Authentifizierung findet auf dem Master-Gateway-Knoten statt.
Autorisierung	Der Dienstmanager autorisiert Benutzeranfragen für Domänenobjekte anhand der Berechtigungen und Rollen, die dem Benutzer zugewiesen sind.
Domänenkonfiguration	Der Dienstmanager verwaltet die Metadaten der Domänenkonfiguration.
Knotenkonfiguration	Der Dienstmanager verwaltet die Metadaten der Knotenkonfiguration in der Domäne.
Lizenzierung	Der Dienstmanager registriert Lizenzinformationen und überprüft diese beim Ausführen der Anwendungsdienste.
Protokollieren	Der Dienstmanager liefert akkumulierte Protokollereignisse aus jedem Dienst in der Domäne sowie für Arbeitsabläufe. Um die Protokollierungsfunktion durchzuführen, führt der Dienstmanager einen Protokollmanager und einen Protokollagenten aus.
Benutzerverwaltung	Der Dienstmanager verwaltet die Benutzer und Gruppen, die sich bei Anwendungs-Clients anmelden können. Darüber hinaus verwaltet er die Erstellung von Rollen und die Zuweisung von Rollen und Berechtigungen zu Benutzern und Gruppen.

Application Services

Application services represent server-based functionality. Application services include the following services:

- Analyst Service
- Content Management Service
- Data Integration Service
- Metadata Manager Service
- Model Repository Service
- PowerCenter Integration Service
- PowerCenter Repository Service
- PowerExchange Listener Service
- PowerExchange Logger Service

- Reporting Service
- Reporting and Dashboards Service (Deprecated)
- Test Data Manager Service
- SAP BW Service
- Web Services Hub

Application services represent server-based functionality. Application services include the following services:

- Data Integration Service
- Model Repository Service

When you configure an application service, you designate a node to run the service process. When a service process runs, the Service Manager assigns a port number from the range of port numbers assigned to the node.

The service process is the runtime representation of a service running on a node. The service type determines how many service processes can run at a time. For example, the PowerCenter Integration Service can run multiple service processes at a time when you run it on a grid.

The service process is the runtime representation of a service running on a node. The service type determines how many service processes can run at a time.

If you have the high availability option, you can run a service on multiple nodes. Designate the primary node to run the service. All other nodes are backup nodes for the service. If the primary node is not available, the service runs on a backup node. You can subscribe to alerts to receive notification in the event of a service process failover.

If you do not have the high availability option, configure a service to run on one node. If you assign multiple nodes, the service will not start.

Analyst-Dienst

Der Analyst-Dienst ist ein Anwendungsdienst, der die Anwendung Informatica Analyst in der Informatica-Domäne ausführt. Der Analyst-Dienst verwaltet die Verbindungen zwischen DienstkompONENTEN und den Benutzern, die sich bei Informatica Analyst anmelden. Der Analyst-Dienst stellt eine Verbindung zu einem Datenintegrationsdienst, einem Modellrepository-Dienst, einem Metadata Manager- und einem Suchdienst her. Der Analyst-Dienst gibt weiterhin ein Cache-Verzeichnis für Einfachdateien sowie ein Verzeichnis für Exportdateien des Unternehmensglossars an.

Wenn Sie den Analyst-Dienst konfigurieren, verbinden Sie ihn mit einem Datenintegrationsdienst, um Profile, Scorecards und Mapping-Spezifikationen auszuführen. Sie können den Analyst-Dienst auch mit einem Datenintegrationsdienst verbinden, der Human-Aufgaben ausführt. Verbinden Sie den Analyst-Dienst mit einem Modellrepository-Dienst, um ein Modellrepository anzugeben.

Verbinden Sie den Analyst-Dienst mit einem Metadata Manager-Dienst, um Datenherkunftsvorgänge für Scorecards im Analyst-Tool durchzuführen. Verbinden Sie den Analyst-Dienst mit einem Suchdienst, um Suchoperationen im Analyst-Tool zu verwalten.

Geben Sie ein Cache-Verzeichnis für Einfachdateien zum Speichern von temporären Daten aus Einfachdateien an, die von Ihnen hochgeladen werden. Geben Sie ein Unternehmensglossarverzeichnis zum Speichern temporärer Dateien an, die Sie aus Business Glossary exportieren.

Content Management Service

Der Content Management Service ist ein Anwendungsdienst, der die Referenzdaten verwaltet. Er stellt die Referenzdateninformationen für den Data Integration Service und das Developer Tool bereit.

Der Content Management Service stellt die Referenzdateneigenschaften für den Data Integration Service bereit. Der Data Integration Service verwendet diese Eigenschaften beim Ausführen von Mappings, die diese Adressreferenzen benötigen.

Ferner stellt der Content Management Service die Developer Tool-Umwandlungen bereit, die Informationen über die im Dateisystem installierten Adressreferenzdaten und Identitätspopulationen enthalten. Das Developer Tool zeigt die installierten Adressreferenzdatensätze in der Ansicht Inhaltsstatus in den Anwendungseinstellungen an. Das Developer Tool zeigt die installierten Identitätspopulationen in der Entsprechungs- und der Vergleichsumwandlung an.

Data Integration Service

Der Data Integration Service ist ein Anwendungsdienst, der Datenintegrationsaufgaben für Informatica Analyst, Informatica Developer und externe Clients übernimmt. Zu den Datenintegrationsaufgaben gehören die Datenvorschau, die Ausführung von Profilen, SQL-Datendiensten, Web-Diensten und Mappings.

Der Data Integration Service ist ein Anwendungsdienst, der Datenintegrationsaufgaben für Informatica Developer durchführt. Zu den Datenintegrationsaufgaben gehören das Anzeigen von Daten in der Vorschau sowie das Ausführen von Mappings und Profilen.

Wenn Sie einen Befehl aus der Befehlszeile oder einem externen Client ausgegeben haben, um SQL-Datendienste und Mappings in einer Anwendung auszuführen, sendet der Befehl die Anfrage an den Data Integration Service.

Metadata Manager Service

Der Metadata Manager Service ist ein Anwendungsdienst, der die Metadata Manager-Anwendung ausführt und die Verbindungen zwischen den Metadata Manager-Komponenten verwaltet.

Mit Metadata Manager werden Metadaten von unterschiedlichen Metadaten-Repositories durchsucht und analysiert. Sie können Metadaten aus folgenden Quellen laden, durchsuchen und analysieren: Anwendungen, Business Intelligence, Data Integration, Data Modelling und aus relationalen Metadatenquellen.

Der Metadata Manager Service lässt sich für die Ausführung auf nur einem Knoten konfigurieren. Der Metadata Manager Service ist kein Dienst mit hoher Verfügbarkeit. Dennoch können Sie mehrere Metadata Manager Services auf demselben Knoten ausführen.

Modellrepository-Dienst

Der Modellrepository-Dienst ist ein Anwendungsdienst, der das Modellrepository verwaltet. Das Modellrepository ist eine relationale Datenbank zur Speicherung der Metadaten für Projekte, die in Informatica Analyst und Informatica Developer erstellt wurden. Das Modellrepository speichert auch Laufzeit- und Konfigurationsinformationen für Anwendungen, die in einem Data Integration Service bereitgestellt wurden.

Der Modellrepository-Dienst ist ein Anwendungsdienst, der das Modellrepository verwaltet. Das Modellrepository ist eine relationale Datenbank, die die Metadaten für Projekte in Informatica Developer speichert. Das Modellrepository speichert auch Laufzeit- und Konfigurationsinformationen für Anwendungen, die in einem Data Integration Service bereitgestellt wurden.

Der Modellrepository-Dienst lässt sich für die Ausführung auf nur einem Knoten konfigurieren. Der Modellrepository-Dienst ist kein Dienst mit hoher Verfügbarkeit. Dennoch können Sie mehrere

Modellrepository-Dienste auf demselben Knoten ausführen. Wenn der Modellrepository-Dienst fehlerhaft ausgeführt wird, erfolgt der automatische Neustart auf demselben Knoten.

PowerCenter Integration Service

Der PowerCenter Integration Service führt PowerCenter-Sitzungen und -Arbeitsabläufe aus. Bei der Konfiguration des PowerCenter Integration Service können Sie angeben, wo er ausgeführt werden soll:

- Auf einem Gitter. Wenn Sie den Dienst so konfigurieren, dass er auf einem Gitter ausgeführt wird, kann er auf mehreren Knoten gleichzeitig laufen. Der PowerCenter Integration Service sendet Tasks an die verfügbaren Knoten, die dem Gitter zugeordnet sind. Wenn Sie nicht über die Option für hohe Verfügbarkeit verfügen, schlägt der Task fehl, wenn einer der Dienstprozesse oder Knoten nicht mehr verfügbar ist. Wenn Sie über die Option für hohe Verfügbarkeit verfügen, stehen Failover und Wiederherstellung zur Verfügung, wenn einer der Dienstprozesse oder Knoten nicht mehr verfügbar ist.
- Auf Knoten. Wenn Sie über die Option für hohe Verfügbarkeit verfügen, können Sie den Dienst so konfigurieren, dass er auf mehreren Knoten läuft. Standardmäßig läuft er auf dem primären Knoten. Wenn der primäre Knoten nicht verfügbar ist, wird er auf einem Backup-Knoten ausgeführt. Wenn der Dienstprozess fehlschlägt oder der Knoten nicht mehr verfügbar ist, wechselt der Dienst auf einen anderen Knoten. Wenn Sie nicht über die Option für hohe Verfügbarkeit verfügen, können Sie den Dienst so konfigurieren, dass er auf einem Knoten läuft.

PowerCenter-Repository-Dienst

Der PowerCenter-Repository-Dienst verwaltet das PowerCenter-Repository. Er ruft Metadaten ab, fügt sie in die PowerCenter-Repository-Datenbanktabellen ein und aktualisiert sie. Wenn der Dienstprozess fehlschlägt oder die Knoten nicht verfügbar sind, ist der Dienst nicht mehr verfügbar.

Wenn Sie die Option hohe Verfügbarkeit verwenden, können Sie den Dienst so konfigurieren, dass er auf den Primär- oder Backup-Knoten ausgeführt wird. Standardmäßig wird der Dienstprozess auf einem Primärknoten ausgeführt. Wenn der Dienstprozess fehlschlägt, startet ein neuer Prozess auf demselben Knoten. Steht der Knoten nicht mehr zur Verfügung, startet der Dienstprozess auf einem der Backup-Knoten.

PowerExchange Listener Service

Der PowerExchange Listener Service ist ein Anwendungsdienst, der das PowerExchange Listener verwaltet. Der PowerExchange Listener verwaltet die Kommunikation zwischen einem PowerCenter oder PowerExchange Client und einer Datenquelle bei der Datenbestandsverschiebung und der Erfassung von Datenänderungen. Der PowerCenter Integration Service verbindet sich über den Listener Service mit PowerExchange Listener. Um einen Dienst zu verwalten und die Dienst-Logs anzuzeigen, verwenden Sie das Administrator Tool.

Wenn Sie die Option der hohen Verfügbarkeit im PowerCenter verwenden, können Sie den Listener Service auf mehreren Knoten ausführen. Wenn der Listener Service-Prozess auf dem Primärknoten fehlschlägt, wird er auf den Backup-Knoten verlagert.

PowerExchange Logger Service

Der Logger Service ist ein Anwendungsdienst, der den PowerExchange Logger für Linux, UNIX und Windows verwaltet. Der PowerExchange Logger erfasst Änderungsdaten von einer Datenquelle und schreibt die Daten in Log-Dateien des PowerExchange Loggers. Um den Dienst zu verwalten und die Dienst-Logs anzuzeigen, verwenden Sie das Administrator Tool.

Wenn Sie die Option der hohen Verfügbarkeit im PowerCenter verwenden, können Sie den Logger Service auf mehreren Knoten ausführen. Wenn der Logger Service-Prozess auf dem Primärknoten fehlschlägt, wird er auf den Backup-Knoten verlagert.

Reporting Service

Der Berichtsdienst ist ein Anwendungsdienst, der die Anwendung Data Analyzer in der Informatica-Domäne ausführt. Melden Sie sich im Data Analyzer an, um Berichte über Daten in einer relationalen Datenbank zu erstellen und auszuführen, oder um folgende PowerCenter-Berichte auszuführen: PowerCenter Repository-Berichte, Data Profiling-Berichte oder Metadata Manager-Berichte. Auch andere Berichte aus Ihrem Unternehmen lassen sich hier ausführen.

Der Berichtsdienst lässt sich nicht mit einer hohen Verfügbarkeit versehen. Dennoch können Sie mehrere Berichtsdienste auf demselben Knoten ausführen.

Konfigurieren Sie einen Berichtsdienst für jede Datenquelle, gegen die Sie Berichte ausführen möchten. Wenn Sie einen Berichtsdienst auf eine andere Datenquelle verweisen möchten, erstellen Sie diese Datenquelle im Data Analyzer.

Berichterstellungs- und Dashboard-Dienst (veraltet)

Sie können den Berichterstellungs- und Dashboard-Dienst im Informatica Administrator erstellen. Sie können den Dienst dazu verwenden, Berichte aus der Anwendung JasperReports zu erstellen und auszuführen.

JasperReports ist eine Open-Source Berichtsbibliothek, die Benutzer in jede beliebige Java-Anwendung einbetten können. Der JasperReports Server bildet mit seinen JasperReports und Formularen einen Teil der Jaspersoft Business Intelligence Suite des Produkts.

Veraltetes Verhalten

Ab Version 9.6.1 HotFix 4 hat Informatica den Berichterstellungs- und Dashboard-Dienst als veraltet klassifiziert. Informatica wird die Unterstützung für den Berichterstellungs- und Dashboard-Dienst sowie für JasperReports Server in einer künftigen Version einstellen.

Wenn Sie auf Version 9.6.1 HotFix 4 aktualisieren, können Sie den Berichterstellungs- und Dashboard-Dienst weiterhin verwenden. Informatica empfiehlt, zu Berichterstellungstools von Drittanbietern überzugehen, bevor Informatica die Unterstützung einstellt. Sie können die empfohlenen SQL-Abfragen zur Erstellung aller Berichte verwenden, die im Lieferumfang früherer Versionen von PowerCenter enthalten waren.

Wenn Sie Version 9.6.1 HotFix 4 installieren, können Sie keinen Berichterstellungs- und Dashboard-Dienst 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*.

SAP BW Service

Der SAP BW Service wartet auf RFC Abfragen von einem SAP NetWeaver BI und initiiert Arbeitsabläufe, die aus dem SAP NetWeaver BI extrahieren oder dorthin laden. Der SAP BW Service ist nicht hoch verfügbar. Sie können ihn so konfigurieren, dass er auf einem Knoten ausgeführt wird.

Web Services Hub

Der Web Services Hub erhält Anfragen vom Web-Dienst-Client und stellt die PowerCenter-Arbeitsabläufe als Services bereit. Der Web Services Hub lässt sich nicht auf assoziierten Dienstprozessen ausführen. Er wird innerhalb der Dienstverwaltung ausgeführt.

Hohe Verfügbarkeit

Die hohe Verfügbarkeit ist eine Option, die einen einzelnen Fehlerpunkt in einer Domäne entfernt und eine minimale Dienstunterbrechung im Falle eines Fehlers gewährleistet. Die hohe Verfügbarkeit besteht aus zwei Komponenten:

- **Belastbarkeit.** Darunter wird die Fähigkeit eine Anwendung verstanden, vorübergehende Netzwerkfehler zu tolerieren bis entweder das Belastbarkeits-Timeout abgelaufen ist, oder der externe Systemfehler behoben wurde.
- **Failover.** Darunter wird die Migration eines Anwendungsdienstes oder einer Task auf einen andern Knoten verstanden, wenn der Knoten, der den Dienstprozess ausführt, un erreichbar geworden ist.
- **Wiederherstellung.** Dies ist die automatische Vervollständigung einer Task, nachdem ein Dienst unterbrochen worden ist. Die automatische Wiederherstellung steht für die Tasks des PowerCenter Integration Service und des PowerCenter Repository Service zur Verfügung. Sie können die Arbeitsabläufe und Sitzungen des PowerCenter Integration Service aber auch manuell wiederherstellen. Die manuelle Wiederherstellung ist jedoch nicht Teil der hohen Verfügbarkeit.

Informatica Data Usage Policy

Informatica DiscoveryIQ is a monitoring tool that sends routine reports on data usage and system statistics to Informatica Global Customer Support.

Informatica DiscoveryIQ uploads data to Informatica 15 minutes after you install and configure Informatica domain. Thereafter, the domain sends the data every 30 days. Data collection and upload is enabled by default. You can choose to not send any usage statistics to Informatica.

If the network where you install Informatica services need a proxy server to communicate with the external network, configure proxy details.

Informatica DiscoveryIQ enables Informatica Global Customer Support to provide an environment health check after the analysis of system statistics and domain reports. You can receive best practices and recommendations from Informatica Global Customer Support based on the reports. The usage statistics provide Informatica a proactive insight into product implementation.

Informatica DiscoveryIQ reports the following data to Informatica:

- Operating system details
- CPU information
- Informatica license key serial number
- Gateway information
- Domain options

- Node options
- Application service information

Konfigurieren der Informatica-DiscoveryIQ Proxy-Details

Konfigurieren Sie die Proxyserver-Details, wenn das Netzwerk, auf dem Informatica-Dienste installiert sind, einen Proxyserver zur Kommunikation mit dem externen Netzwerk verwendet.

1. Klicken Sie im Überschriftsbereich des Administrator-Tools auf **Verwalten > DiscoveryIQ Proxy Details**.
2. Geben Sie die Domäne, Hostname und Portnummer des Proxyservers ein.
3. Geben Sie den Benutzernamen und Passwort ein, um eine Verbindung zum Proxyserver herzustellen.
4. Klicken Sie auf **OK**, um die Proxyserver-Details zu speichern.

Deaktivieren der Informatica-Datennutzung

Sie können das Hochladen von Nutzungsdaten aus der Informatica-Domäne in das Administrator-Tool deaktivieren.

1. Klicken Sie im Administrator-Tool auf **Hilfe > Info**.
2. Klicken Sie auf **Richtlinie zur Datennutzung**.
3. Löschen Sie **Sammlung von Nutzungsdaten aktivieren**.
4. Klicken Sie auf **OK**.

KAPITEL 2

Eigenes Konto verwalten

Dieses Kapitel umfasst die folgenden Themen:

- [Eigenes Konto verwalten - Übersicht, 30](#)
- [Anmelden bei Informatica Administrator, 30](#)
- [Passwortverwaltung, 32](#)
- [Einstellungen bearbeiten, 32](#)
- [Einstellungen, 33](#)
- [Informatica Network Credentials, 33](#)

Eigenes Konto verwalten - Übersicht

Verwalten Sie Ihr Konto, um Ihr Passwort zu ändern oder Benutzereinstellungen zu bearbeiten.

Wenn Sie ein natives Benutzerkonto haben, können Sie Ihr Passwort jederzeit mit der Anwendung "Passwort ändern" ändern. Wenn jemand anderes Ihr Benutzerkonto angelegt hat, ändern Sie Ihr Passwort, wenn Sie sich zum ersten Mal beim Administrator Tool anmelden.

Die Benutzereinstellungen legen fest, welche Optionen bei der Anmeldung im Administrator Tool angezeigt werden. Die Benutzereinstellungen wirken sich nicht auf die Optionen aus, die angezeigt werden, wenn sich ein anderer Benutzer beim Administrator Tool anmeldet.

Sie können Ihre Anmeldedaten für das Informatica MySupport-Portal für Ihr Konto konfigurieren, um über das Administrator-Tool auf die Informatica-Wissensdatenbank zuzugreifen.

Anmelden bei Informatica Administrator

Sie benötigen ein Benutzerkonto, um sich an der Informatica Administrator-Webanwendung anzumelden.

Wenn die Informatica-Domäne in einem Netzwerk mit Kerberos-Authentifizierung ausgeführt wird, müssen Sie den Browser für den Zugriff auf Informatica-Webanwendungen konfigurieren. Fügen Sie in Microsoft Internet Explorer und Google Chrome die URL der Informatica-Webanwendung zur Liste der vertrauenswürdigen Sites hinzu. Wenn Sie Chrome Version 41 oder höher verwenden, müssen Sie auch die Richtlinien `AuthServerWhitelist` und `AuthNegotiateDelegateWhitelist` festlegen.

1. Starten Sie Microsoft Internet Explorer oder Google Chrome.

2. Geben Sie in der **Adresszeile** die URL für das Administrator-Tool ein:

- Wenn das Administrator-Tool nicht für die Verwendung einer sicheren Verbindung konfiguriert wurde, geben Sie die folgende URL ein:

`http://<fully qualified hostname>:<http port>`

- Wenn das Administrator-Tool für die Verwendung einer sicheren Verbindung konfiguriert wurde, geben Sie die folgende URL ein:

`https://<fully qualified hostname>:<http port>`

Hostnamen und Port in der URL entsprechen dem Hostnamen und der Portnummer des Master-Gateway-Knotens. Wenn Sie für die Domäne die sichere Kommunikation konfiguriert haben, müssen Sie HTTPS in der URL verwenden, um sicherzustellen, dass Sie Zugriff auf das Administrator-Tool haben.

Wenn Sie die Kerberos-Authentifizierung verwenden, verwendet das Netzwerk die einmalige Anmeldung. Sie müssen sich nicht beim Administrator-Tool mit einem Benutzernamen und einem Passwort anmelden.

3. Wenn Sie nicht die Kerberos-Authentifizierung verwenden, geben Sie den Benutzernamen, das Passwort und die Sicherheitsdomäne für Ihr Benutzerkonto ein, und klicken Sie auf **Anmeldung**.

Das Feld **Sicherheitsdomäne** wird eingeblendet, wenn die Informatica-Domäne eine LDAP-Sicherheitsdomäne enthält. Wenn Sie die Sicherheitsdomäne, zu der Ihr Benutzerkonto gehört, nicht kennen, wenn Sie sich an den Domänenadministrator von Informatica.

Hinweis: Wenn Sie sich zum ersten Mal mit dem vom Domänenadministrator erhaltenen Benutzernamen und Passwort anmelden, ändern Sie Ihr Passwort, damit die Sicherheit erhalten bleibt.

Informatica Administrator-URL

In der URL des Administrator-Tools stellt `<Host>:<Port>` den Hostnamen des Master-Gateway-Knotens und die Portnummer des Administrator-Tools dar.

Den Port für das Administrator-Tool konfigurieren Sie beim Definieren der Domäne. Sie können die Domäne beim Installieren oder durch Ausführen des Befehlszeilenprogramms *infasetup* DefineDomain definieren. Wenn Sie den Domänen-Port anstatt des Administrator-Tool-Ports in die URL eingeben, wird der Browser zum Administrator-Tool-Port weitergeleitet.

Hinweis: Bei einem Failover der Domäne zu einem anderen Master-Gateway-Knoten entspricht der Hostname in der URL des Administrator-Tools dem Hostnamen des gewählten Master-Gateway-Knotens.

Fehlerbehebung bei der Anmeldung bei Informatica Administrator

Wenn die Informatica-Domäne Kerberos-Authentifizierung verwendet, können bei der Anmeldung beim Administrator-Tool die folgenden Probleme auftreten:

Ich kann mich nicht auf demselben Computer beim Administrator-Tool anmelden, auf dem ich den Domänen-Gateway-Knoten erstellt habe.

Wenn Sie sich nach der Installation nicht auf demselben Computer beim Administrator-Tool anmelden können, auf dem Sie den Domänen-Gateway-Knoten erstellt haben, löschen Sie den Browsercache. Wenn Sie sich beim Administrator-Tool nach der Installation zum ersten Mal anmelden, können Sie sich nur mit dem Administratorbenutzerkonto anmelden, das Sie während der Installation erstellt haben. Wenn im Browsercache andere Benutzeranmeldedaten gespeichert sind, kann die Anmeldung fehlschlagen.

Eine leere Seite wird angezeigt, nachdem ich mich beim Administrator-Tool angemeldet habe.

Wenn nach Ihrer Anmeldung beim Administrator-Tool eine leere Seite angezeigt wird, überprüfen Sie, ob Sie die Delegation für alle Benutzerkonten mit in der Informatica-Domäne verwendeten

Dienstprinzipalen aktiviert haben. Zum Aktivieren der Delegation legen Sie im Microsoft Active Directory Service die Option **Benutzer bei Delegationen aller Dienste vertrauen (nur Kerberos)** für jedes Benutzerkonto fest, für das Sie einen SPN festgelegt haben.

Passwortverwaltung

Sie können das Passwort mithilfe der Anwendung "Passwort ändern" ändern.

Sie können die Anwendung "Passwort ändern" über das Administrator-Tool oder mit der folgenden URL öffnen: `http://<host>:<port>/passwordchange`

Der Service Manager verwendet das Benutzerpasswort, das einem Worker-Knoten zugewiesen ist, um den Domänen-Benutzer zu authentifizieren. Wenn Sie ein Benutzerpasswort ändern, das einem oder mehreren Worker-Knoten zugewiesen ist, aktualisiert der Service Manager das Passwort für jeden Worker-Knoten. Der Service Manager kann nur Knoten aktualisieren, die ausgeführt werden. Bei Knoten, die nicht ausgeführt werden, aktualisiert der Service Manager das Passwort, wenn die Knoten neu gestartet werden.

Hinweis: Für ein LDAP-Benutzerkonto ändern Sie das Passwort im LDAP-Verzeichnisdienst.

Ändern Ihres Passwortes.

Das Passwort für ein natives Benutzerkonto können Sie jederzeit ändern. Das Passwort für ein Benutzerkonto, das von einer anderen Person erstellt wurde ändern Sie, wenn Sie sich zum ersten Mal beim Administrator Tool anmelden.

1. Klicken Sie im Überschriftsbereich des Administrator Tools auf **Verwalten > Passwort ändern**.
Die Anwendung "Passwort ändern" öffnet ein neues Browserfenster.
2. Geben Sie das aktuelle Passwort in das Feld **Passwort** ein und das neue Passwort in die Felder **Neues Passwort** und **Passwort bestätigen**.
3. Klicken Sie auf **Aktualisieren**.

Einstellungen bearbeiten

Sie können die Einstellungen ändern, um die Optionen festzulegen, die nach der Anmeldung im Administrator Tool erscheinen.

1. Im Kopfbereich des Administrator Tools klicken Sie auf **Verwalten > Einstellungen**.
Das Fenster **Einstellungen** erscheint.
2. Klicken Sie auf **Bearbeiten**.
Das Dialogfeld **Einstellungen bearbeiten** erscheint.

Einstellungen

Ihre Einstellungen legen fest, welche Optionen bei der Anmeldung im Administrator Tool angezeigt werden. Ihre Einstellungen wirken sich nicht auf die Optionen aus, die angezeigt werden, wenn sich ein anderer Benutzer beim Administrator Tool anmeldet.

Die folgende Tabelle beschreibt die Optionen, die Sie in Ihren Einstellungen konfigurieren können:

Option	Beschreibung
Alarmer abonnieren	Abonnieren Sie für Domänen- und Dienst-Alarmer. Für Ihr Benutzerkonto muss eine gültige E-Mail-Adresse konfiguriert sein. Die Standardeinstellung ist Nein.
Benutzerdefinierte Eigenschaften anzeigen	Zeigt benutzerdefinierte Eigenschaften im Inhaltsbereich an, wenn Sie auf ein Objekt im Navigator klicken. Mit benutzerdefinierten Eigenschaften konfigurieren Sie das Verhalten von Informatica für besondere Fälle oder um die Leistung zu erhöhen. Blenden Sie die benutzerdefinierten Eigenschaften aus, um zu vermeiden, dass die Werte versehentlich geändert werden. Verwenden Sie benutzerdefinierte Eigenschaften, wenn Sie vom globalen Benutzersupport darauf hingewiesen werden.

Informatica Network Credentials

You can enter your Informatica Network credentials in the Administrator tool to access the Informatica Knowledge Base from the Administrator tool.

You can also view the search results for an error message in the Informatica Knowledge Base by clicking the error message code in the Administrator tool.

Informatica Network-Anmeldedaten eingeben

Geben Sie Ihre Anmeldedaten für Informatica Network ein, um mit dem Administrator Tool auf die Informatica-Wissensdatenbank zuzugreifen.

1. Klicken Sie auf **Verwalten > Anmeldedaten für Supportportal**.
Daraufhin wird das **Anmeldefenster für Informatica Network** angezeigt.
2. Geben Sie Ihre Anmeldedaten für Informatica Network und die Kundenprojekt-ID ein.
3. Klicken Sie auf **OK**.

Suchen der Informatica-Wissensdatenbank

Sie können direkt über das Administrator-Tool nach Begriffen in der Informatica-Wissensdatenbank suchen.

1. Klicken Sie auf **Hilfe > Wissensdatenbank durchsuchen**.
Das Fenster **Wissensdatenbank durchsuchen** wird angezeigt.
2. Geben Sie den Begriff für die Suche im Textfeld ein.
3. Klicken Sie auf **OK**.
Die Suchergebnisse werden in einem anderen Browserfenster angezeigt.

KAPITEL 3

Informatica Administrator

Dieses Kapitel umfasst die folgenden Themen:

- [Informatica Administrator verwenden - Übersicht, 34](#)
- [Registerkarte Domäne - Übersicht, 36](#)
- [Registerkarte Domäne - Ansicht Dienste und Knoten, 36](#)
- [Registerkarte „Verwalten“ – Verbindungsansicht, 46](#)
- [Registerkarte "Protokolle", 46](#)
- [Registerkarte Berichte, 47](#)
- [Registerkarte "Überwachen", 47](#)
- [Registerkarte Sicherheit, 48](#)
- [Dienststatus, 51](#)
- [Prozessstatus, 51](#)
- [Jobstatus, 53](#)
- [Tastenkombinationen, 54](#)

Informatica Administrator verwenden - Übersicht

Der Informatica Administrator ist das Administrator-Tool, das Sie zur Verwaltung der Informatica-Domäne und der Informatica-Sicherheit benötigen.

Nutzen Sie das Administrator-Tool, um die folgenden Aufgaben auszuführen:

Administrative Domänenaufgaben

Verwalten von Protokollen, Domänenobjekten, Benutzerberechtigungen und Domänenberichten. Erzeugen und Hochladen der Knotendiagnose. Überwachen von Jobs und Anwendungen, die auf dem Data Integration Service ausgeführt werden. Zu den Domänenobjekten gehören Anwendungsdienste, Knoten, Gitter, Ordner, Datenbankverbindungen, Betriebssystemprofile und Lizenzen.

Administrative Domänenaufgaben

Verwalten von Protokollen, Domänenobjekten und Benutzerberechtigungen. Überwachen von Jobs und Anwendungen, die auf dem Data Integration Service ausgeführt werden.

Administrative Domänenaufgaben

Verwalten von Protokollen, Domänenobjekten und Benutzerberechtigungen.

Administrative Sicherheitsaufgaben:

Verwalten von Benutzern, Gruppen, Rollen und Berechtigungen.

Im Administrator-Tool gibt es folgende Registerkarten:

Domäne

Anzeigen und Bearbeiten der Eigenschaften der Domäne und der Objekte innerhalb der Domäne.

Protokolle

Anzeigen von Protokollereignissen für die Domäne und die Dienste innerhalb der Domäne.

Überwachung

Anzeigen des Status von Profil-Jobs, Vorschau-Jobs, Mapping-Jobs, SQL-Datendiensten und Webdiensten für jeden Datenintegrationsdienst.

Überwachung

Anzeigen des Status von Profil-Jobs, Scorecard-Jobs, Vorschau-Jobs, Mapping-Jobs, SQL-Datendiensten, Webdiensten und Arbeitsabläufen für jeden Datenintegrationsdienst.

Überwachung

Anzeigen des Status von Profil-Jobs, Vorschau-Jobs, Mapping-Jobs und Arbeitsabläufen für jeden Data Integration Service.

Überwachung

Ansicht und Überwachen von Ultra Messaging-Bereitstellungen.

Berichte

Ausführen eines Webdienstberichts oder eines Lizenzverwaltungsberichts.

Sicherheit

Verwalten von Benutzern, Gruppen, Rollen und Berechtigungen.

Sicherheit

Verwalten von Benutzern, Gruppen, Rollen und Berechtigungen. Wenn Sie PowerCenter Express Personal Edition verwenden, haben Sie keinen Zugriff auf die Registerkarte "Sicherheit".

Sicherheit

Verwalten von Benutzern, Gruppen, Rollen und Berechtigungen.

Das Administrator-Tool besitzt die folgenden Kopfzeileneinträge:

Abmelden

Abmelden vom Administrator-Tool.

Verwalten

Verwalten Ihres Kontos.

Hilfe

Zugriff auf die Hilfe für die aktuelle Registerkarte und Festlegen der Informatica-Version.

Hilfe

Zugriff auf die Hilfe für die aktuelle Registerkarte, Festlegen der Informatica-Version und Konfigurieren der Datennutzungsrichtlinie.

Hilfe

Zugriff auf die Hilfe für die aktuelle Registerkarte, Festlegen der Informatica-Version und Konfigurieren der Datennutzungsrichtlinie.

Registerkarte Domäne - Übersicht

Auf der Registerkarte **Domäne** können Sie Informationen zur Domäne anzeigen und Objekte in der Domäne anzeigen und verwalten.

Die Inhalte, die erscheinen und die Aufgaben, die Sie auf der Registerkarte **Domain** ausführen können, variieren je nach gewählter Ansicht. Sie können die folgenden Ansichten wählen:

- **Dienste und Knoten** Anzeigen und Verwalten von Anwendungsdiensten und Knoten des Knotens.
- **Verbindungen** Zur Anzeige und Verwaltung von Verbindungen.

Die Inhalte, die erscheinen und die Aufgaben, die Sie auf der Registerkarte **Domain** ausführen können, variieren je nach gewählter Ansicht. Sie können die Ansicht **Dienste und Knoten** auswählen, um den Ultra Messaging-Dienst zu verwalten.

Sie können das Erscheinungsbild der Ansichten konfigurieren.

Registerkarte Domäne - Ansicht Dienste und Knoten

In der Ansicht **Dienste und Knoten** werden alle Anwendungsdienste und Knoten angezeigt, die der Knoten in der Domäne definiert hat.

Die Ansicht **Dienste und Knoten** hat folgende Komponenten:

Navigator

Auf der linken Seite der Registerkarte **Domäne**. Der Navigator zeigt die folgenden Objekttypen an:

- Domäne. Sie können eine Domäne anzeigen, die das höchste Objekt in der Navigator-Hierarchie darstellt.
- Ordner. Ordner sind zum Organisieren von Domänenobjekten im Navigator bestimmt. Wählen Sie einen Ordner aus, um Informationen über den Ordner und die Objekte im Ordner anzuzeigen.
- Anwendungsdienste Ein Anwendungsdienst stellt serverbasierte Funktionalität dar. Wählen Sie einen Anwendungsdienst aus, um Informationen über den Dienst und dessen Prozesse anzuzeigen.
- Knoten. Bei einem Knoten handelt es sich um einen Computer in der Domäne. Sie weisen den Knoten Ressourcen zu und konfigurieren Dienstprozesse, die auf den Knoten laufen sollen.
- Knoten. Bei einem Knoten handelt es sich um einen Computer in der Domäne. Sie weisen einem Knoten Ressourcen zu und konfigurieren Dienstprozesse zum Ausführen auf dem Knoten.
- Knoten. Bei einem Knoten handelt es sich um einen Computer in der Domäne. Sie weisen einem Knoten Ressourcen zu und konfigurieren Dienstprozesse zum Ausführen auf dem Knoten.
- Gitter. Erstellen Sie ein Gitter, um den Data Integration Service oder PowerCenter Integration Service auf mehreren Knoten auszuführen. Wählen Sie ein Gitter, um zu sehen, welche Knoten dem Gitter zugewiesen sind.
- Lizenzen. Erstellen Sie auf der Registerkarte **Domäne** basierend auf der von Informatica zur Verfügung gestellten Lizenzschlüsseldatei eine Lizenz. Wählen Sie eine Lizenz aus, um zu sehen, welche Dienste der Lizenz zugewiesen sind.
- Lizenz. Anzeigen der Lizenz und der Dienste, die der Lizenz zugeordnet sind.
- Lizenz. Anzeigen der Lizenz und der Dienste, die der Lizenz zugeordnet sind.

Inhaltsübersicht

Steht auf der rechten Seite der Registerkarte **Domäne** und umfasst Informationen über die Domäne oder Domänenobjekte, die Sie im Navigator ausgewählt haben.

Menü "Aktionen" im Navigator

Beim Auswählen der Domäne im Navigator können Sie einen Ordner, einen Dienst, einen Knoten, ein Gitter oder eine Lizenz erstellen.

Wenn Sie ein Domänenobjekt im Navigator auswählen, können Sie das Objekt löschen, es in einen Ordner verschieben, oder das Objekt aktualisieren.

Menü "Aktionen" im Navigator

Wenn Sie ein Domänenobjekt im Navigator auswählen, können Sie das Objekt aktualisieren.

Menü "Aktionen" im Navigator

Wenn Sie ein Domänenobjekt im Navigator auswählen, können Sie einen Ordner, Dienst, Knoten oder eine Lizenz erstellen.

Menü "Aktionen" auf der Registerkarte "Domäne"

Wenn Sie die Domäne im Navigator auswählen, können Sie die Domäne herunterfahren oder Protokolle für sie anzeigen.

Wenn Sie einen Knoten im Navigator auswählen, können Sie eine Knotenzuordnung entfernen, den Benchmark des CPU-Profiles neu berechnen oder den Knoten herunterfahren.

Wenn Sie einen Dienst im Navigator auswählen, können Sie den Dienst recyceln oder deaktivieren, Sicherungsdateien im Repository anzeigen oder dessen Inhalte sichern, die Repository-Domäne verwalten, Benutzer benachrichtigen und Protokolle anzeigen.

Wenn Sie eine Lizenz im Navigator auswählen, können Sie der Lizenz einen inkrementellen Schlüssel hinzufügen.

Menü "Aktionen" auf der Registerkarte "Domäne"

Wenn Sie die Domäne im Navigator auswählen, können Sie Protokolle für die Domäne anzeigen.

Wenn Sie einen Dienst im Navigator auswählen, können Sie den Dienst recyceln oder deaktivieren, Sicherungsdateien im Repository anzeigen oder dessen Inhalte sichern, die Repository-Domäne verwalten, Benutzer benachrichtigen und Protokolle anzeigen.

Wenn Sie eine Lizenz im Navigator auswählen, können Sie der Lizenz einen inkrementellen Schlüssel hinzufügen.

Menü "Aktionen" auf der Registerkarte "Domäne"

Wenn Sie die Domäne im Navigator auswählen, können Sie die Domäne herunterfahren oder Protokolle für sie anzeigen.

Wenn Sie eine Lizenz im Navigator auswählen, können Sie der Lizenz einen inkrementellen Schlüssel hinzufügen.

Domäne

Sie haben die Möglichkeit, eine Domäne in der Ansicht **Dienste und Knoten** auf der Registerkarte **Domäne** anzuzeigen. Hierbei handelt es sich um das höchste Objekt in der Navigator-Hierarchie.

Beim Auswählen der Domäne im Navigator enthält die Inhaltsübersicht folgende Ansichten und Schaltflächen, mit denen Sie die folgenden Aufgaben ausführen können:

- Ansicht **Übersicht**. Zeigen Sie alle in der Domäne nach Objekttyp organisierten Anwendungsdienste, Knoten und Gitter an. Sie können den Status von Anwendungsdiensten und Knoten sowie Informationen über Gitter anzeigen. Außerdem besteht die Möglichkeit, gegenseitige Abhängigkeiten der Anwendungsdienste, Knoten und Gitter anzuzeigen und die Eigenschaften für Domänenobjekte einzublenden. Anwendungsdienste können auch recycelt werden.

Klicken Sie auf einen Anwendungsdienst, um seinen Namen, die Version, den Status und die Statusangaben seiner einzelnen Prozesse anzuzeigen. Klicken Sie auf einen Knoten, um dessen Namen, Status, die Anzahl der auf dem Knoten laufenden Dienstprozesse und den Namen etwaiger Gitter anzuzeigen, zu denen der Knoten gehört. Klicken Sie auf ein Gitter, um den Namen des Gitters, die Anzahl der im Gitter laufenden Dienstprozesse und die Namen der Knoten im Gitter einzublenden. Der Status kann verfügbar, deaktiviert und nicht verfügbar sein.

Standardmäßig zeigt die Ansicht **Übersicht** eine Abkürzung für jeden einzelnen Domänennamen an. Klicken Sie auf die Schaltfläche **Details anzeigen**, um die vollständigen Namen der Objekte anzuzeigen. Klicken Sie auf die Schaltfläche **Details ausblenden**, um Abkürzungen der Objektnamen anzuzeigen.

Um die gegenseitigen Abhängigkeiten der Anwendungsdienste, Knoten und Gitter anzuzeigen, klicken Sie mit der rechten Maustaste auf ein Objekt und anschließend auf **Abhängigkeit einblenden**. Das Diagramm **Abhängigkeiten** wird aufgerufen.

Um die Eigenschaften für einen Anwendungsdienst, einen Knoten oder ein Gitter anzuzeigen, klicken Sie mit der rechten Maustaste auf ein Objekt und anschließend auf **Eigenschaften einblenden**. In der Inhaltsübersicht stehen die Objekteigenschaften.

Wenn Sie einen Anwendungsdienst recyceln möchten, klicken Sie mit der rechten Maustaste auf einen Dienst und anschließend auf **Dienst recyceln**.

- Ansicht **Übersicht**. Anzeigen aller Domänenobjekte nach Objekttyp. Sie können Statusangaben der Anwendungsdienste und des Knotens anzeigen. Darüber hinaus können Sie Eigenschaften zu Domänenobjekten anzeigen. Anwendungsdienste können auch recycelt werden.

Klicken Sie auf einen Anwendungsdienst, um seinen Namen, die Version, den Status und die Statusangaben seiner einzelnen Prozesse anzuzeigen. Klicken Sie auf einen Knoten, um den Namen, den Status und die Anzahl der auf dem Knoten ausgeführten Dienstprozesse anzuzeigen. Der Status kann verfügbar, deaktiviert und nicht verfügbar sein.

Standardmäßig zeigt die Ansicht **Übersicht** eine Abkürzung für den Namen jedes einzelnen Domänenobjekts an. Klicken Sie auf die Schaltfläche **Details anzeigen**, um die vollständigen Namen der Objekte anzuzeigen. Klicken Sie auf die Schaltfläche **Details ausblenden**, um Abkürzungen der Objektnamen anzuzeigen.

- Ansicht **Übersicht**. Anzeigen aller Domänenobjekte nach Objekttyp. Sie können Statusangaben der Anwendungsdienste und des Knotens anzeigen. Darüber hinaus können Sie Eigenschaften zu Domänenobjekten anzeigen.

Klicken Sie auf einen Anwendungsdienst, um dessen Namen und Beschreibung anzuzeigen. Klicken Sie auf einen Knoten, um den Namen, den Status und die Anzahl der auf dem Knoten ausgeführten Dienstprozesse anzuzeigen.

Klicken Sie auf einen Anwendungsdienst, um seinen Namen, die Version, den Status und die Statusangaben seiner einzelnen Prozesse anzuzeigen. Klicken Sie auf einen Knoten, um den Namen, den Status und die Anzahl der auf dem Knoten ausgeführten Dienstprozesse anzuzeigen.

Standardmäßig zeigt die Ansicht **Übersicht** eine Abkürzung für den Namen jedes einzelnen Domänenobjekts an. Klicken Sie auf die Schaltfläche **Details anzeigen**, um die vollständigen Namen der Objekte anzuzeigen. Klicken Sie auf die Schaltfläche **Details ausblenden**, um Abkürzungen der Objektamen anzuzeigen.

- Ansicht **Eigenschaften**. Anzeigen oder Bearbeiten der Domänen-Belastbarkeitseigenschaften.
- Ansicht **Ressourcen**. Anzeigen der verfügbaren Ressourcen für jeden Knoten in der Domäne.
- Ansicht **Berechtigungen**. Anzeigen oder Bearbeiten der Gruppen- und Benutzerberechtigungen für die Domäne.
- **Ansicht Diagnostik**. Anzeigen der Knotendiagnostik, Generieren und Hochladen der Knotendiagnostik auf den Customer Support Manager oder Bearbeiten der Anmeldedaten für das Kundenportal.
- Ansicht **Plug-Ins**. In der Domäne registrierte Plug-Ins anzeigen.
- Schaltfläche "Protokolle für Domäne anzeigen". Anzeigen von Protokollen für die Domäne und Dienste innerhalb der Domäne.

Im Menü **Aktionen** des Navigators können Sie einen Knoten, ein Gitter, einen Anwendungsdienst oder eine Lizenz zur Domäne hinzufügen.. Außerdem haben Sie die Möglichkeit, Ordner hinzuzufügen, die Sie zum Ordnen der Domänenobjekte verwenden können.

Im Menü **Aktionen** auf der Registerkarte **Domäne** können Sie herunterfahren, Protokolle anzeigen oder auf die Hilfe zur aktuellen Ansicht zugreifen.

Im Menü **Aktionen** auf der Registerkarte **Domäne** können Sie Protokolle anzeigen oder auf die Hilfe zur aktuellen Ansicht zugreifen.

Im Menü **Aktionen** auf der Registerkarte **Domäne** können Sie herunterfahren, Protokolle anzeigen oder auf die Hilfe zur aktuellen Ansicht zugreifen.

Ordner

Sie können die Ordner in einer Domäne dazu verwenden, die Sicherheit zu organisieren.

Die Ordner können Knoten, Dienste, Gitter, Lizenzen und andere Ordner enthalten.

Wenn Sie im Navigator einen Ordner wählen, wird der Navigator geöffnet und zeigt die Objekte im Ordner an. Der Inhaltsbereich zeigt die folgenden Informationen an:

- Ansicht **Eigenschaften**. Zeigt den Namen und die Beschreibung des Ordners an.
- Ansicht **Berechtigungen**. Dient zum Bearbeiten von Gruppen und Benutzerberechtigungen in dem Ordner.

Im Menü **Aktionen** im Navigator können Sie den Ordner löschen, in einen anderen Ordner verschieben, die Inhalte auf der Registerkarte **Verwalten** aktualisieren oder Hilfe zur aktuellen Registerkarte anzeigen.

Hinweis: Der Ordner System_Services wird bei Erstellung der Domäne für Sie erstellt und enthält alle Systemdienste. Ein Systemdienst ist ein Anwendungsdienst, der in der Domäne eine einzelne Instanz haben kann. Die Eigenschaften oder Inhalte des Ordners System_Services können nicht gelöscht, verschoben oder bearbeitet werden.

Application Services

Application services are a group of services that represent Informatica server-based functionality.

In the **Services and Nodes** view on the **Domain** tab, you can create and manage the following application services:

In the **Services and Nodes** view on the **Domain** tab, you can create and manage the following application services:

In the **Services and Nodes** view on the **Domain** tab, you can create and manage the Ultra Messaging Service.

Analyst Service

Runs Informatica Analyst in the Informatica domain. The Analyst Service manages the connections between service components and the users that log in to Informatica Analyst.

The Analyst Service connects to a Data Integration Service, a Model Repository Service, a Metadata Manager Service, and a Search Service. The Analyst Service also specifies a flat file cache directory and a directory for business glossary export files.

You can create and recycle the Analyst Service in the Informatica domain to access the Analyst tool. You can launch the Analyst tool from the Administrator tool.

When you select an Analyst Service in the Navigator, the contents panel displays the following information:

- Service and service process status. View the status of the service and the service process for each node. The contents panel also displays the URL of the Analyst Service instance.
- **Properties** view. Manage general, model repository, data integration, metadata manager, flat file cache, business glossary export, logging, and custom properties.
- **Processes** view. View and edit service process properties on each assigned node.
- **Permissions** view. View or edit the group and user permissions on the Analyst Service.
- **Actions** menu. Manage the service and repository contents.

Content Management Service

Manages reference data and compiles rule specifications into mapplets. Stores properties for address reference data and identity population data.

When you select a Content Management Service in the Navigator, the contents panel displays the following information:

- Service and service process status. View the status of the service and the service process for each node.
- **Properties** view. Manage general, master, data integration, model repository, logging, and custom properties.
- **Processes** view. View and edit service process properties on each assigned node.
- **Permissions** view. View or edit the group and user permissions on the Content Management Service.
- **Actions** menu. Manage the service.

Data Integration Service

Completes data integration tasks for Informatica Analyst, Informatica Developer, and external clients. When you preview or run data profiles, SQL data services, and mappings in Informatica Analyst or Informatica Developer, the application sends requests to the Data Integration Service to perform the data integration tasks. When you start a command from the command line or an external client to run SQL data services and mappings in an application, the command sends the request to the Data Integration Service.

When you select a Data Integration Service in the Navigator, the contents panel displays the following information:

- Service and service process status. View the status of the service and the service process for each node.
- **Properties** view. Manage general, model repository, logging, logical data object and virtual table cache, profiling, data object cache, and custom properties. Set the default deployment option.

- **Processes** view. View and edit service process properties on each assigned node.
- **Applications** view. Start and stop applications and SQL data services. Back up applications. Manage application properties.
- **Actions** menu. Manage the service and repository contents.

Data Integration Service

Completes data integration tasks for Informatica Developer. When you preview or run mappings in Informatica Developer, the application sends requests to the Data Integration Service to perform the data integration tasks. When you start a command from the command line or an external client to run mappings in an application, the command sends the request to the Data Integration Service.

- Service and service process status. View the status of the service and the service process for each node.
- **Properties** view. Manage general, model repository, logging, logical data object cache, profiling, data object cache, and custom properties. Set the default deployment option.
- **Processes** view. View and edit service process properties on each assigned node.
- **Applications** view. Start, stop, and back up applications. Manage application properties.
- **Actions** menu. Manage the service and repository contents.

Metadata Manager Service

Runs the Metadata Manager application and manages connections between the Metadata Manager components.

When you select a Metadata Manager Service in the Navigator, the contents panel displays the following information:

- Service and service process status. View the status of the service and the service process for each node. The contents panel also displays the URL of the Metadata Manager Service instance.
- **Properties** view. View or edit Metadata Manager properties.
- **Associated Services** view. View and configure the Integration Service associated with the Metadata Manager Service.
- **Permissions** view. View or edit the group and user permissions on the Metadata Manager Service.
- **Actions** menu. Manage the service and repository contents.

Model Repository Service

Manages the Model repository. The Model repository stores metadata created by Informatica products, such as Informatica Developer, Informatica Analyst, the Data Integration Service, and Informatica Administrator. The Model repository enables collaboration among the products.

When you select a Model Repository Service in the Navigator, the contents panel displays the following information:

- Service and service process status. View the status of the service and the service process for each node.
- **Properties** view. Manage general, repository database, search, and custom properties.
- **Processes** view. View and edit service process properties on each assigned node.
- **Actions** menu. Manage the service and repository contents.

Model Repository Service

Manages the Model repository. The Model repository stores metadata created by Informatica Developer, Data Integration Service, and Informatica Administrator. The Model repository enables collaboration among the products.

When you select a Model Repository Service in the Navigator, the contents panel displays the following information:

- Service and service process status. View the status of the service and the service process for each node.
- **Properties** view. Manage general, repository database, search, and custom properties.
- **Processes** view. View and edit service process properties on each assigned node.
- **Actions** menu. Manage the service and repository contents.

PowerCenter Integration Service

Runs PowerCenter sessions and workflows. Select a PowerCenter Integration Service in the Navigator to access information about the service.

When you select a PowerCenter Integration Service in the Navigator, the contents panel displays the following information:

- Service and service processes status. View the status of the service and the service process for each node.
- **Properties** view. View or edit Integration Service properties.
- **Associated Repository** view. View or edit the repository associated with the Integration Service.
- **Processes** view. View or edit the service process properties on each assigned node.
- **Permissions** view. View or edit group and user permissions on the Integration Service.
- **Actions** menu. Manage the service.

PowerCenter Repository Service

Manages the PowerCenter repository. It retrieves, inserts, and updates metadata in the repository database tables. Select a PowerCenter Repository Service in the Navigator to access information about the service.

When you select a PowerCenter Repository Service in the Navigator, the contents panel displays the following information:

- Service and service process status. View the status of the service and the service process for each node. The service status also displays the operating mode for the PowerCenter Repository Service. The contents panel also displays a message if the repository has no content or requires upgrade.
- **Properties** view. Manage general and advanced properties, node assignments, and database properties.
- **Processes** view. View and edit service process properties on each assigned node.
- **Connections and Locks** view. View and terminate repository connections and object locks.
- **Plug-ins** view. View and manage registered plug-ins.
- **Permissions** view. View or edit group and user permissions on the PowerCenter Repository Service.
- **Actions** menu. Manage the contents of the repository and perform other administrative tasks.

PowerExchange Listener Service

Runs the PowerExchange Listener.

When you select a Listener Service in the Navigator, the contents panel displays the following information:

- Service and service process status. Status of the service and service process for each node. The contents panel also displays the URL of the PowerExchange Listener instance.
- **Properties** view. View or edit Listener Service properties.
- **Actions** menu. Contains actions that you can perform on the Listener Service, such as viewing logs or enabling and disabling the service.

PowerExchange Logger Service

Runs the PowerExchange Logger for Linux, UNIX, and Windows.

When you select a Logger Service in the Navigator, the contents panel displays the following information:

- Service and service process status. Status of the service and service process for each node. The contents panel also displays the URL of the PowerExchange Logger instance.
- **Properties** view. View or edit Logger Service properties.
- **Actions** menu. Contains actions that you can perform on the Logger Service, such as viewing logs or enabling and disabling the service.

Reporting Service

Runs the Data Analyzer application in an Informatica domain. You log in to Data Analyzer to create and run reports on data in a relational database or to run the following PowerCenter reports: PowerCenter Repository Reports, Data Profiling Reports, or Metadata Manager Reports. You can also run other reports within your organization.

When you select a Reporting Service in the Navigator, the contents panel displays the following information:

- Service and service process status. Status of the service and service process for each node. The contents panel also displays the URL of the Data Analyzer instance.
- **Properties** view. The Reporting Service properties such as the data source properties or the Data Analyzer repository properties. You can edit some of these properties.
- **Permissions** view. View or edit group and user permissions on the Reporting Service.
- **Actions** menu. Manage the service and repository contents.

Reporting and Dashboards Service (Deprecated)

Runs reports from the JasperReports application.

SAP BW Service

Listens for RFC requests from SAP BW and initiates workflows to extract from or load to SAP BW. Select an SAP BW Service in the Navigator to access properties and other information about the service.

When you select an SAP BW Service in the Navigator, the contents panel displays the following information:

- Service and service process status. View the status of the service and the service process.
- **Properties** view. Manage general properties and node assignments.
- **Associated Integration Service** view. View or edit the Integration Service associated with the SAP BW Service.
- **Processes** view. View or edit the directory of the BWParam parameter file.

- **Permissions** view. View or edit group and user permissions on the SAP BW Service.
- **Actions** menu. Manage the service.

Web Services Hub

A web service gateway for external clients. It processes SOAP requests from web service clients that want to access PowerCenter functionality through web services. Web service clients access the PowerCenter Integration Service and PowerCenter Repository Service through the Web Services Hub.

When you select a Web Services Hub in the Navigator, the contents panel displays the following information:

- Service and service process status. View the status of the service and the service process.
- **Properties** view. View or edit Web Services Hub properties.
- **Associated Repository** view. View the PowerCenter Repository Services associated with the Web Services Hub.
- **Permissions** view. View or edit group and user permissions on the Web Services Hub.
- **Actions** menu. Manage the service.

Ultra Messaging Service

Runs the Ultra Messaging System Monitoring in the Informatica domain. It manages the connections between service components and the users that have access to Ultra Messaging System Monitoring.

When you select the Ultra Messaging Service in the Navigator, the contents panel displays the following information:

- Service
- **Properties** view. View or edit the Ultra Messaging service properties.
- **Configurations** view. View or edit configurations of the Monitoring components.
- **Actions** menu. Access help on the current view.

Knoten KnotenKnoten

Ein Knoten ist eine logische Darstellung eines physischen Computers in der Domäne. Auf der Registerkarte "Domäne" können Sie Knoten Ressourcen zuweisen und Dienstprozesse konfigurieren, die auf Knoten ausgeführt werden sollen.

Wenn Sie einen Knoten im Navigator auswählen, erscheinen im Inhaltsbereich folgende Informationen:

- Knotenstatus: Anzeige des Status des Knotens.
- **Eigenschaftensicht** Anzeigen oder Bearbeiten der Knoteneigenschaften, wie z. B. Repository-Backup-Verzeichnis oder Bereich von Portnummern für die Prozesse, die auf dem Knoten ausgeführt werden.
- Ansicht **Prozesse** Anzeigen des Status aller Prozesse, die zur Ausführung auf dem Knoten konfiguriert sind.
- Ansicht **Ressourcen**. Anzeigen oder Bearbeiten der dem Knoten zugeordneten Ressourcen.
- **Berechtigungen**-Ansicht. Anzeigen oder Bearbeiten von Gruppen- und Benutzerberechtigungen für den Knoten.

Im Menü **Aktionen** Menü im Navigator können Sie den Knoten löschen, ihn in einen Ordner verschieben, den Inhalt auf der Registerkarte **Domäne** aktualisieren oder die Hilfe zur aktuellen Registerkarte öffnen.

Im Menü **Aktionen** im Navigator können Sie die Inhalte auf der Registerkarte **Domäne** aktualisieren oder auf die Hilfe zur aktuellen Registerkarte zugreifen.

Im Menü **Aktionen** im Navigator können Sie die Inhalte auf der Registerkarte **Domäne** aktualisieren, den Knoten löschen oder auf die Hilfe zur aktuellen Registerkarte zugreifen.

Im Menü **Aktionen** der Registerkarte **Domäne** können Sie die Knotenzuordnung löschen, das CPU-Benchmark-Profil neu berechnen oder den Knoten abschalten.

Gitter

Ein Gitter ist ein Alias für eine Gruppe von Knoten, auf denen PowerCenter Integration Service- oder Data Integration Service-Jobs ausgeführt werden.

Wenn Sie einen Job auf einem Gitter ausführen, verteilt der Integration Service die Verarbeitung über mehrere Knoten im Gitter. Wenn Sie zum Beispiel ein Profil auf einem Gitter ausführen, teilt der Data Integration Service die Arbeit in mehrere Jobs und weist jeden Job zu einem Knoten im Gitter zu. Sie weisen die Knoten einem Gitter in der Ansicht **Dienste und Knoten** auf der Registerkarte **Domäne** zu.

Wenn Sie ein Gitter im Navigator auswählen, erscheinen im Inhaltsbereich folgende Informationen:

- Ansicht **Eigenschaften**. Hier können Sie die Knotenzuweisungen an ein Gitter anzeigen oder bearbeiten.
- Ansicht **Berechtigungen**. Hier können Sie die Gruppen- und Benutzerberechtigungen in einem Gitter anzeigen oder bearbeiten.

Im Menü **Aktionen** des Navigators können Sie das Gitter löschen, das Gitter in einen Ordner verschieben, die Inhalte auf der Registerkarte **Domäne** aktualisieren oder Hilfe zur aktuellen Registerkarte anzeigen.

Lizenzen

Die Erstellung eines Lizenzobjekts auf der Registerkarte **Domäne** erfordert eine von Informatica zur Verfügung gestellte Lizenzschlüsseldatei.

Nachdem Sie eine Lizenz erstellt haben, können Sie ihr Dienste zuordnen.

Beim Auswählen einer Lizenz im Navigator werden in der Inhaltsübersicht folgende Informationen eingeblendet:

- Ansicht **Eigenschaften**. Sie können Lizenzeigenschaften wie beispielsweise unterstützte Plattformen, Repositories und lizenzierte Optionen anzeigen. Außerdem können Sie die Lizenzbeschreibung bearbeiten.
- Ansicht **Zugeordnete Dienste**. Anzeigen oder Bearbeiten der Dienste, die der Lizenz zugeordnet sind.
- **Ansicht Optionen**. Anzeigen der lizenzierten PowerCenter-Optionen.
- **Ansicht Optionen**. Anzeigen der lizenzierten Ultra Messaging-Optionen.
- **Berechtigungen**-Ansicht. Anzeigen oder Bearbeiten von Benutzerberechtigungen für die Lizenz.

Im Menü **Aktionen** des Navigators können Sie die Lizenz löschen, zu einem Ordner verschieben, den Inhalt auf der Registerkarte **Domäne** aktualisieren oder auf die Hilfe für die aktuelle Registerkarte zugreifen.

Im Menü **Aktionen** im Navigator können Sie die Inhalte auf der Registerkarte **Domäne** aktualisieren oder auf die Hilfe zur aktuellen Registerkarte zugreifen.

Im Menü **Aktionen** des Navigators können Sie die Lizenz löschen, zu einem Ordner verschieben, den Inhalt auf der Registerkarte **Domäne** aktualisieren oder auf die Hilfe für die aktuelle Registerkarte zugreifen.

Im Menü **Aktionen** auf der Registerkarte **Domäne** können Sie einer Lizenz einen inkrementellen Schlüssel hinzufügen.

Registerkarte „Verwalten“ – Verbindungsansicht

Die Ansicht **Verbindungen** zeigt die Domäne und alle Verbindungen in der Domäne.

Die Ansicht **Verbindungen** hat folgende Komponenten:

Navigator

Zeigt die Domäne und die Verbindungen in der Domäne an.

Menü Aktionen im Navigator

Wenn Sie die Domäne im Navigator auswählen, können Sie eine Verbindung erstellen.

Wählen Sie eine Verbindung im Navigator, können Sie die Verbindung löschen.

Inhaltsübersicht

Zeigt Informationen über die Domäne oder die Verbindung an, die Sie im Navigator auswählen.

Wenn Sie die Domäne im Navigator auswählen, enthält die Inhaltsübersicht alle Verbindungen in der Domäne. In der Inhaltsübersicht können Sie Verbindungen filtern bzw. sortieren oder nach bestimmten Verbindungen suchen.

Wenn Sie eine Verbindung im Navigator auswählen, erscheinen im Inhaltsbereich folgende Informationen zu der Verbindung. Die Aufgaben, die Sie für die Verbindung abschließen können, hängt davon ab, welche der folgenden Ansichten Sie auswählen:

- Ansicht **Eigenschaften**. Anzeigen oder Bearbeiten von Eigenschaften.
- Ansicht **Pooling**. Anzeigen oder Bearbeiten von Pooling-Eigenschaften für die Verbindung.
- Ansicht **Berechtigungen**. Anzeigen oder Bearbeiten von Gruppen- oder Benutzerberechtigungen für die Verbindung.

Menü „Aktionen“ auf der Registerkarte „Verwalten“

Wenn Sie eine Verbindung im Navigator auswählen, können Sie die Verbindung testen.

Registerkarte "Protokolle"

Die Registerkarte **Protokolle** zeigt Protokolle an.

Auf der Registerkarte **Protokolle** können Sie die folgenden Arten von Protokollen anzeigen:

- Domänenprotokoll. Domänenprotokollereignisse sind Protokollereignisse, die anhand der vom Service Manager ausgeführten Domänenfunktionen generiert werden.
- Dienstprotokoll. Dienstprotokollereignisse sind Ereignisse, die von jedem Anwendungsdienst generiert werden.
- Benutzeraktivitätsprotokoll. Benutzeraktivitätsprotokollereignisse zum Überwachen der Benutzeraktivitäten in der Domäne.

Auf der Registerkarte **Protokolle** werden für jede Art von Protokoll die folgenden Komponenten angezeigt.

- Filter Zum Konfigurieren der Filteroptionen für die Protokolle.
- Log Viewer. Zeigt Protokollereignisse entsprechend den Filterkriterien.
- Filter zurücksetzen Zum Zurücksetzen der Filterkriterien.
- Zeilen kopieren. Zum Kopieren des Protokolltexts der ausgewählten Zeilen.

- Menü **Aktionen** Enthält Optionen zum Speichern, Löschen und Verwalten von Protokollen. Es enthält auch Filteroptionen.

Registerkarte Berichte

Die Registerkarte **Berichte** zeigt die Domänenberichte an.

Auf der Registerkarte **Berichte** können Sie folgende Domänenberichte ausführen:

- Lizenzverwaltungsbericht Führen Sie einen Bericht aus, um die Anzahl der Softwareoptionen zu überwachen, die für die Lizenz erworben wurden, sowie die mit der Lizenz verbundene Anzahl an Benutzerbeschränkungen. Führen Sie einen Bericht aus, um die Verwendung logischer CPUs und der PowerCenter Repository Services zu überwachen. Für die Ausführung des Berichts ist eine Lizenz erforderlich.
- Lizenzverwaltungsbericht Führen Sie einen Bericht aus, um die Anzahl der Softwareoptionen zu überwachen, die für die Lizenz erworben wurden, sowie die mit der Lizenz verbundene Anzahl an Benutzerbeschränkungen.
- Web-Dienste-Bericht. Führen Sie einen Bericht aus, um die Performance der Web-Dienste zu analysieren, die auf einem Web-Dienste-Hub ausgeführt werden. Ein Bericht wird während eines bestimmten Zeitintervalls ausgeführt.

Registerkarte "Überwachen"

Auf der Registerkarte **Überwachen** können Sie Data Integration Services und Integrationsobjekte überwachen, die auf dem Data Integration Service laufen.

Integrationsobjekte umfassen Jobs und Anwendungen, bereitgestellte Mappings, logische Datenobjekte, SQL-Datendienste, Web-Dienste und Arbeitsabläufe. Die Registerkarte **Überwachen** zeigt Laufzeit-Statistiken und Laufzeit-Berichte über die Integrationsobjekte an.

Integrationsobjekte umfassen Jobs, Anwendungen, bereitgestellte Mappings, logische Datenobjekte und Arbeitsabläufe. Die Registerkarte **Überwachen** zeigt Laufzeit-Statistiken und Laufzeit-Berichte über die Integrationsobjekte an.

Die Registerkarte **Überwachen** enthält folgende Komponenten:

- Navigator. Erscheint im linken Bereich der Registerkarte **Überwachen** und zeigt Jobs, Anwendungen und Anwendungskomponenten an. Anwendungskomponenten enthalten bereitgestellte Mappings, logische Datenobjekte, Web-Dienste und Arbeitsabläufe.
- Navigator. Befindet sich im linken Bereich der Registerkarte **Überwachen** und zeigt Jobs, Anwendungen und Anwendungskomponenten an. Anwendungskomponenten umfassen bereitgestellte Mappings, logische Datenobjekte und Arbeitsabläufe.
- Inhaltsbereich. Erscheint auf der rechten Seite der Registerkarte **Überwachen**. Er enthält Informationen über das Objekt, das im Navigator ausgewählt ist.
Wenn Sie im Navigator einen Ordner auswählen, werden alle im Ordner enthaltenen Objekte im Inhaltsbereich angezeigt.
Wenn Sie im Navigator eine Anwendungskomponente auswählen, werden mehrere Ansichten der Objektinformationen im Inhaltsbereich angezeigt.

- Detailbereich. Erscheint in einigen Fällen unterhalb des Inhaltsbereichs. Mithilfe des Detailbereichs können Sie Details über das Objekt anzeigen, das im Inhaltsbereich ausgewählt wurde.
- Menü "Aktionen". Erscheint auf der Registerkarte **Überwachen**. Ermöglicht Ihnen das Anzeigen des Kontexts, das Zurücksetzen von Suchfiltern, das Abbrechen eines ausgewählten Jobs und das Anzeigen der Protokolle für ein ausgewähltes Objekt.

Registerkarte Sicherheit

Sie verwalten die Informatica-Sicherheit auf der Registerkarte Sicherheit im Administrator-Tool.

Die Registerkarte Sicherheit besteht aus folgenden Komponenten:

- Suchbereich. Suche nach Benutzern, Gruppen oder Rollen anhand des Namens.
- Navigator Der Navigator erscheint im linken Bereich und zeigt Gruppen, Benutzer und Rollen an.
- Inhaltsbereich. Der Inhaltsbereich zeigt die Eigenschaften und Optionen des im Navigator gewählten Objekts an, sowie entsprechend der gewählten Registerkarte.
- Menü "Sicherheitsaktionen". Enthält Optionen zum Erstellen oder Löschen einer Gruppe, eines Benutzers oder einer Rolle. Sie können die LDAP-Profilen und die Betriebssystemprofile verwalten. Sie können auch Benutzer anzeigen, die Berechtigungen für einen Dienst besitzen.
- Menü "Sicherheitsaktionen". Enthält Optionen zum Erstellen oder Löschen einer Gruppe, eines Benutzers oder einer Rolle.
- Menü "Sicherheitsaktionen". Enthält Optionen zum Erstellen oder Löschen einer Gruppe, eines Benutzers oder einer Rolle.

Hinweis: Wenn Sie PowerCenter Express Personal Edition verwenden, haben Sie keinen Zugriff auf die Registerkarte "Sicherheit".

Der Suchbereich

Im Suchbereich können Sie anhand von Namen nach Benutzern, Gruppen oder Rollen suchen. Die Groß-/Kleinschreibung spielt bei der Suche keine Rolle.

1. Legen Sie im Suchbereich fest, wo Sie nach Benutzern, Gruppen oder Rollen suchen möchten.
2. Geben Sie den Namen oder einen Teil des Namens ein, nach dem gesucht werden soll.

Für die Suche können Sie auch ein Sternchen (*) als Platzhalter im Namen verwenden. Zum Beispiel: Wenn Sie nach allen Objekten suchen möchten, die mit "ad" beginnen, geben Sie "ad*" ein. Wenn Sie nach allen Objekten suchen möchten, die mit "ad" aufhören, geben Sie "*ad" ein.

3. Klicken Sie auf Los.

Im Abschnitt Suchergebnis können maximal 100 Objekte angezeigt werden. Wenn die Suche mehr als 100 Objekte ergibt, schränken Sie die Suchergebnisse durch weitere Suchkriterien ein.

4. Wählen Sie ein Objekt im Abschnitt Suchergebnisse aus, um weitere Informationen zu diesem Objekt im Inhaltsfenster anzuzeigen.

Der Sicherheits-Navigator

Der Navigator erscheint im Inhaltsbereich der Registerkarte Sicherheit. Wenn Sie ein Objekt im Navigator auswählen, erscheinen im Inhaltsbereich folgende Informationen zu dem Objekt:

Auf der Registerkarte „Sicherheit“ im Navigator wird abhängig von Ihrer Ansicht einer der folgenden Bereiche angezeigt:

- Abschnitt Gruppen. Um die Eigenschaften einer Gruppe, die zugewiesenen Benutzer, Rollen und Privilegien anzuzeigen, wählen Sie die Gruppe aus.
- Abschnitt Benutzer. Um die Eigenschaften eines Benutzers, die zugehörigen Gruppen, Rollen und Privilegien anzuzeigen, wählen Sie den Benutzer aus.
- Abschnitt Rollen. Um die Eigenschaften einer Rolle, sowie die zu dieser Rolle gehörenden Benutzer, Gruppen und Privilegien anzuzeigen, wählen Sie die Rolle aus.

Der Navigator bietet verschiedene Möglichkeiten an, eine Task auszuführen. Zum Verwalten von Gruppen, Benutzern und Rollen können Sie eine der folgenden Methoden verwenden:

- Klicken Sie auf das Menü Aktionen. Jeder Abschnitt des Navigators enthält das Menü Aktionen zur Verwaltung von Gruppen, Benutzern oder Rollen. Wählen Sie im Navigator ein Objekt aus und klicken Sie auf das Menü Aktionen, um Gruppen, Benutzer oder Rollen zu erstellen bzw. zu löschen.
- Rechter Mausklick auf Objekt. Wenn Sie ein Objekt im Navigator mit der rechten Maustaste anklicken, erscheinen die Optionen aus dem Menü Aktionen zum Erstellen, Löschen und Verschieben des Objekts.
- Tastenkombinationen verwenden. Mit Hilfe von Tastenkombinationen können Sie die verschiedenen Abschnitte des Navigators ansteuern.

Gruppen

Eine Gruppe ist eine Anhäufung von Benutzern und Gruppen mit denselben Rechten, Rollen und Berechtigungen.

Im Abschnitt "Gruppen" des Navigators sind Gruppen in Sicherheitsdomänenordner eingeteilt. Eine Sicherheitsdomäne ist eine Ansammlung von Benutzerkonten und Gruppen in einer Informatica-Domäne. Zur nativen Authentifizierung wird die native Sicherheitsdomäne verwendet. Sie enthält die im Administrator-Tool erstellten und verwalteten Benutzer und Gruppen. Die LDAP-Authentifizierung nutzt LDAP-Sicherheitsdomänen, die aus dem LDAP-Verzeichnisdienst importierte Benutzer und Gruppen enthält.

Im Abschnitt "Gruppen" des Navigators sind Gruppen in Sicherheitsdomänenordner eingeteilt. Eine Sicherheitsdomäne ist eine Ansammlung von Benutzerkonten und Gruppen in einer Informatica-Domäne. Zur nativen Authentifizierung wird die native Sicherheitsdomäne verwendet. Sie enthält die im Administrator-Tool erstellten und verwalteten Benutzer und Gruppen.

Im Abschnitt "Gruppen" des Navigators sind Gruppen in Sicherheitsdomänenordner eingeteilt. Eine Sicherheitsdomäne ist eine Ansammlung von Benutzerkonten und Gruppen in einer Informatica-Domäne. Zur nativen Authentifizierung wird die native Sicherheitsdomäne verwendet. Sie enthält die im Administrator-Tool erstellten und verwalteten Benutzer und Gruppen.

Wenn Sie einen Sicherheitsdomänen-Ordner im Abschnitt Gruppen des Navigators auswählen, werden in der Inhaltsübersicht alle zu dieser Sicherheitsdomäne gehörenden Gruppen eingeblendet. Durch Rechtsklick auf eine Gruppe und Auswählen von Zum Element navigieren können Sie die Gruppendetails in der Inhaltsübersicht anzeigen.

Nach Auswählen einer Gruppe im Navigator sind in der Inhaltsübersicht folgende Registerkarten zu sehen:

- Übersicht. Anzeige allgemeiner Eigenschaften der Gruppe und der dieser Gruppe zugeordneten Benutzer.
- Berechtigungen. Blendet die der Gruppe zugeordneten Berechtigungen und Rollen für die Domäne und für Anwendungsdienste in der Domäne ein.

Benutzer

Ein Benutzer mit einem Konto in der Informatica-Domäne kann sich an folgenden Anwendungs-Clients anmelden:

- Informatica Administrator
- PowerCenter-Client
- Metadata Manager
- Data Analyzer
- Informatica Developer
- Informatica Analyst
- Jaspersoft

Ein Benutzer mit einem Konto in der Informatica-Domäne kann sich an folgenden Anwendungs-Clients anmelden:

- Informatica Administrator
- Informatica Developer

Ein Benutzer mit einem Benutzerkonto in der Informatica-Domäne kann sich bei Informatica Administrator anmelden.

Im Abschnitt "Benutzer" des Navigators sind die Benutzer in Sicherheitsdomänenordnern zusammengefasst. Eine Sicherheitsdomäne ist eine Sammlung von Benutzerkonten und Gruppen innerhalb einer Informatica-Domäne. Zur nativen Authentifizierung wird die native Sicherheitsdomäne verwendet. Sie enthält die im Administrator-Tool erstellten und verwalteten Benutzer und Gruppen. Die LDAP-Authentifizierung verwendet LDAP-Sicherheitsdomänen, die jene Benutzer und Gruppen enthält, die aus dem LDAP-Verzeichnisdienst importiert wurden.

Im Abschnitt "Benutzer" des Navigators sind die Benutzer in Sicherheitsdomänenordnern zusammengefasst. Eine Sicherheitsdomäne ist eine Ansammlung von Benutzerkonten und Gruppen in einer Informatica-Domäne.

Im Abschnitt "Benutzer" des Navigators sind die Benutzer in Sicherheitsdomänenordnern zusammengefasst. Eine Sicherheitsdomäne ist eine Ansammlung von Benutzerkonten und Gruppen in einer Informatica-Domäne.

Wenn Sie im Abschnitt Benutzer des Navigators einen Ordner für eine Sicherheitsdomäne auswählen, erscheinen im Bereich Inhalt alle Benutzer, die zu dieser Sicherheitsdomäne gehören. Klicken Sie einen Benutzer mit der rechten Maustaste an und wählen Sie "Zu Eintrag navigieren", um die Benutzerdetail im Bereich Inhalt anzuzeigen.

Wenn Sie einen Benutzer im Navigator auswählen, erscheinen im Inhaltsbereich folgende Registerkarten:

- Übersicht. Listet die allgemeinen Eigenschaften des Benutzer auf und alle Gruppen, zu denen er gehört.
- Berechtigungen. Listet die Berechtigungen und Rollen auf, die dem Benutzer für die Domäne und die Anwendungsdienste in der Domäne zugewiesen wurden.

Rollen

Eine Rolle ist eine Sammlung von Berechtigungen, die Sie einem Benutzer oder einer Gruppe zuordnen. Berechtigungen bestimmen die Aktionen, die Benutzer ausführen können. Sie ordnen Benutzern und Gruppen für die Domäne und für Anwendungsdienste in der Domäne eine Rolle zu.

Der Abschnitt Rollen im Navigator organisiert die Rollen in folgende Ordner:

- Systemdefinierte Rollen Enthält Rollen, die Sie nicht ändern oder löschen können. Die Administrator-Rolle ist eine vom System definierte Rolle.

- Benutzerdefinierte Rollen Enthält Rollen, die Sie erstellen, bearbeiten und löschen können. Das Administrator Tool enthält einige benutzerdefinierte Rollen, die Sie bearbeiten und an Benutzer und Gruppen zuweisen können.

Wenn Sie im Abschnitt Rollen des Navigators einen Ordner auswählen, zeigt der Inhaltsbereich alle Benutzer an, die zu diesem Ordner gehören. Klicken Sie mit der rechten Maustaste auf eine Rolle, und wählen Sie "Zu Eintrag navigieren", um die Rollendetails im Inhaltsbereich anzuzeigen.

Wenn Sie eine Rolle im Navigator auswählen, erscheinen im Inhaltsbereich folgende Registerkarten:

- Übersicht. Zeigt allgemeine Eigenschaften der Rolle und der Benutzer und Gruppen, denen die Rolle für diese Domäne und Anwendungsdienste zugewiesen wurden.
- Berechtigungen Zeigt die Berechtigungen, die der Rolle für die Domäne und die Anwendungsdienste zugewiesen wurden.

Dienststatus

Sie können den Status der Informatica-Dienste über das im Administrator-Tool angezeigte Symbol ermitteln.

Die folgende Tabelle zeigt die mit jedem Dienststatus verbundenen Symbole an:



Status	Symbol
Verfügbar	
Nicht verfügbar	
Deaktiviert	

Prozessstatus

Sie können den Status eines Data Integration Service-Prozesses oder PowerCenter Integration Service-Prozesses über das im Administrator-Tool angezeigte Symbol ermitteln.

Die Symbole für den Status richten sich auch nach dem Knoten, in dem der Prozess ausgeführt wird. Eine gelbe Raute zeigt das Prozessstatus-Symbol an, wenn der primäre Knoten eine hohe Verfügbarkeit aufweist. Ein Gittersymbol überlagert das Prozessstatus-Symbol, wenn der Prozess ein Gitter ausführt.

Die folgende Tabelle zeigt die mit dem jeweiligen Prozessstatus verknüpften Symbole an:

Status	Symbol
Abgebrochen	
Abgebrochen (mit hoher Verfügbarkeit)	










Status	Symbol
Abgebrochen (Gitter)	
Deaktiviert	
Deaktiviert (mit hoher Verfügbarkeit)	
Deaktiviert (Gitter)	
Fehlgeschlagen	
Fehlgeschlagen (mit hohe Verfügbarkeit)	
Fehlgeschlagen (Gitter)	
Ausführen	
Ausführen (mit hoher Verfügbarkeit)	
Ausführen (Gitter)	
Standby oder Verzögert	
Standby oder Verzögert (mit hoher Verfügbarkeit)	
Standby oder Verzögert (Gitter)	
Starten	
Starten (mit hoher Verfügbarkeit)	
Starten (Gitter)	
Gestoppt	
Gestoppt (mit hoher Verfügbarkeit)	
Gestoppt (Gitter)	

Status	Symbol
Stoppen	
Stoppen (mit hoher Verfügbarkeit)	
Stoppen (Gitter)	

Jobstatus

Sie können den Status eines Jobs über das im Administrator-Tool angezeigte Symbol ermitteln.

Die folgende Tabelle zeigt die Symbole für jeden Jobstatus an:

Status	Symbol
Abgebrochen	
Abgeschlossen	
Fehlgeschlagen	
In Warteschlange oder Ausstehend	
Ausführen	
Starten	
Gestoppt	
Stoppen	
Beendet	

Tastenkombinationen

Sie können Tastenkombinationen verwenden, um mit der Administrator-Tool-Schnittstelle zu navigieren und darin zu arbeiten.

Sie können die Werte im Administrator-Tool hinzufügen, bearbeiten und ändern. Der Tastaturfokus im Administrator-Tool wird durch einen blauen Rahmen um die Schnittstellenbeschriftung angegeben. Wenn das Objekt im Fokus steht, wird es ebenfalls mit einer gepunkteten Linie umrandet. Wenn ein Beschriftungselement mit der Tastatur fokussiert wird oder wenn die Maus darüber bewegt wird, werden Quickinfos angezeigt.

Hinweis: Die Navigationsreihenfolge der Objekte im Editor verläuft von oben nach unten und von links nach rechts.

Sie können die folgenden Aufgaben mit Tastenkombinationen durchführen:

So navigieren Sie zwischen verschiedenen Elementen und wählen ein Element im Administrator-Tool aus.

Drücken Sie die TAB-Taste.

Wählen Sie das vorherige Objekt aus.

Drücken Sie UMSCHALT+TAB.

Navigieren Sie zwischen Perspektive-Registerkarten.

Drücken Sie die Pfeiltaste nach links oder nach rechts, um zwischen Perspektive-Registerkarten zu navigieren.

Aktivieren oder deaktivieren Sie das Kontrollkästchen und die Optionsschaltfläche.

Drücken Sie die Leertaste.

Laden Sie Dateien mit der Schaltfläche Datei hochladen hoch.

Drücken Sie die Leertaste.

Navigieren Sie durch Datensätze in einem Dialogfeld.

Drücken Sie die Pfeiltasten nach oben oder nach unten, um durch verschiedene Datensätze zu navigieren.

Wählen Sie und öffnen Sie ein Dropdown-Menüelement mit Untermenüs.

Drücken Sie auf die Taste Pfeil nach unten. Mit der Taste Esc gelangen Sie zurück zum Hauptmenü.

Bearbeiten Sie den Wert des Gitterinhalts, wie z. B. das Feld „Zugriff“ und das Feld „Widerrufen“ im Dialogfeld „Berechtigung zuweisen“ und im Dialogfeld „Berechtigung bearbeiten“.

Drücken Sie die Leertaste.

Hinweis: Geben Sie entsprechende Werte für alle Formularelemente ein, die mit einem Sternchen (*) gekennzeichnet sind.

Verschieben Sie den Fokus aus dem Dropdown-Menü „Aktualisierungshäufigkeit“ zum Kontrollkästchen „Zeitbereich im Listengitter „Statistiken und Berichte“ im Dialogfeld „Einstellungen“ auf der Registerkarte „Überwachen“ oder dem URL.

Drücken Sie die ESC-Taste.

Über die Tastatur können Sie nicht auf die Ansicht „Abhängigkeitsgrafik“ oder auf die Ansicht „Graphischer Arbeitsablauf“ zugreifen. Über die Tastatur können Sie nicht auf die Fensterleiter im Administrator-Tool zugreifen und die Fenstergröße anpassen. Auf der Registerkarte „Auditberichte“ unter „Sicherheit“ können Sie mehrere Elemente mit der Strg-Taste auswählen.

Hinweis: Zur Verwendung der Zugänglichkeitsfunktionen in Internet Explorer 9 und 10 müssen Sie den Browsermodus IE9 oder den IE10-Kompatibilitätsmodus festlegen. Drücken Sie zum Festlegen des

Kompatibilitätsmodus die Taste F12 und ändern Sie die Browsermodus-Einstellung passend zu Ihrer Internet Explorer-Version.

KAPITEL 4

Domänenverwaltung

Dieses Kapitel umfasst die folgenden Themen:

- [Domänenverwaltung - Übersicht, 56](#)
- [Alarmverwaltung, 57](#)
- [Ordnerverwaltung, 59](#)
- [Domänensicherheitsmanagement, 61](#)
- [Sicherheitsverwaltung für Benutzer, 62](#)
- [Anwendungsdienstverwaltung, 62](#)
- [Knotenverwaltung, 65](#)
- [Gateway-Konfiguration, 72](#)
- [Domänenkonfigurationsverwaltung, 72](#)
- [Domänenaufgaben, 77](#)
- [Domäneneigenschaften, 81](#)

Domänenverwaltung - Übersicht

Eine Informatica-Domäne besteht aus einer Reihe von Knoten und Diensten zur Definition der Informatica-Umgebung. Um die Domäne zu verwalten, müssen Sie die Knoten und Dienste in der Domäne verwalten.

Eine Informatica-Domäne besteht aus mehreren Diensten und einem Knoten, die die Informatica-Umgebung definieren. Um die Domäne zu verwalten, müssen Sie den Knoten und die Dienste in der Domäne verwalten.

Eine Informatica-Domäne besteht aus mehreren Diensten und einem Knoten, die die Informatica-Umgebung definieren. Um die Domäne zu verwalten, müssen Sie den Knoten und die Dienste in der Domäne verwalten.

Mit dem Administrator-Tool können Sie folgenden Aufgaben durchführen:

- Alarme verwalten. Konfigurieren, Aktivieren und Deaktivieren von Domänen- und Dienstalarmen für Benutzer.
- Ordner erstellen. Erstellen von Ordnern zum Organisieren von Domänenobjekten und für die Sicherheitsverwaltung durch Einstellen von Ordnerberechtigungen.
- Domänensicherheits-Verwaltung. Konfigurieren sicherer Kommunikation zwischen Domänenkomponenten.
- Benutzersicherheits-Verwaltung. Zuweisen von Berechtigungen zu Benutzern und Gruppen.
- Verwalten von Anwendungsdiensten. Aktivieren, Deaktivieren und Entfernen von Anwendungsdiensten. Aktivieren, Deaktivieren und Neustarten von Dienstprozessen.

- Verwalten von Knoten. Konfigurieren der Knoteneigenschaften, wie Sicherungsverzeichnis und Ressourcen, sowie Herunterfahren der Knoten.
- Verwalten eines Knotens. Konfigurieren Sie Knoteneigenschaften, wie das Backup-Verzeichnis und Ressourcen.
- Verwalten eines Knotens. Konfigurieren Sie Knoteneigenschaften, wie das Backup-Verzeichnis und Ressourcen.
- Konfigurieren von Gateway-Knoten. Konfigurieren von Knoten, die als Gateway fungieren sollen.
- Herunterfahren der Domäne. Herunterfahren der Domäne zwecks Ausführung administrativer Aufgaben in der Domäne.
- Verwalten der Domänenkonfiguration. Sichern Sie die Domänenkonfiguration regelmäßig. Es kann erforderlich sein, die Domänenkonfiguration aus der Sicherung wieder herzustellen, um die Konfiguration zu einem anderen Datenbank-Benutzerkonto zu migrieren. Vielleicht müssen Sie auch die Datenbank-Informationen für die Domänenkonfiguration zurücksetzen, falls sie sich ändern.
- Abschließen von Domänenaufgaben. Sie können den Status aller Anwendungsdienste und Knoten überwachen, gegenseitige Abhängigkeiten der Anwendungsdienste und Knoten anzeigen und die Domäne herunterfahren.
- Abschließen von Domänenaufgaben. Sie können die Statusangaben aller Anwendungsdienste und des Knotens überwachen sowie Abhängigkeiten zwischen den Anwendungsdiensten und dem Knoten anzeigen.
- Abschließen von Domänenaufgaben. Sie können die Statusangaben aller Anwendungsdienste und des Knotens überwachen sowie Abhängigkeiten zwischen den Anwendungsdiensten und dem Knoten anzeigen.
- Konfigurieren von Domäneneigenschaften. Zum Beispiel können Sie die Datenbankeigenschaften, die SMTP-Eigenschaften für Alarme und die Domänenbelastbarkeitseigenschaften ändern.
- Konfigurieren von Domäneneigenschaften. Zum Beispiel können Sie die SMTP-Eigenschaften für Alarme und die Domänenbelastbarkeitseigenschaften ändern.
- Konfigurieren von Domäneneigenschaften. Zum Beispiel können Sie die SMTP-Eigenschaften für Alarme und die Domänenbelastbarkeitseigenschaften ändern.

Um Knoten und Dienste über eine einzige Schnittstelle zu verwalten, müssen sich alle Knoten und Dienste in derselben Domäne befinden. Der Zugriff auf mehrere Informatica-Domänen in ein- und demselben Fenster des Administrator-Tools ist nicht möglich. Das Einrichten von Metadaten für die gemeinsame Nutzung durch mehrere Domänen ist möglich, indem Sie ein lokales Repository in der lokalen Informatica-Domäne mit einem globalen Repository in einer anderen Informatica-Domäne registrieren oder deregistrieren.

Alarmverwaltung

Alarme stellen dem Benutzer Domänen- und Dienstalarme bereit. Domänenalarme enthalten Informationen zu fehlerhaften Knoten und Master-Gateway-Auswahl. Dienstalarme enthalten Informationen zu fehlerhaften Dienstprozessen.

Alarme stellen dem Benutzer Domänen- und Dienstalarme bereit. Mit Domänenalarmen werden Sie über Knotenfehler und mit Dienstalarmen über Fehler im Dienstprozess informiert.

Alarme stellen dem Benutzer Domänen- und Dienstalarme bereit. Mit Domänenalarmen werden Sie über Knotenfehler und mit Dienstalarmen über Fehler im Dienstprozess informiert.

Um Alarme zu verwenden, führen Sie folgende Aufgaben durch:

- Konfigurieren Sie die SMTP-Einstellungen für den ausgehenden Mailserver.
- Abonnieren Sie Alarme.

Nachdem Sie die SMTP-Einstellungen konfiguriert haben, können die Benutzer die Domänen- und Dienstalarme abonnieren.

Konfigurieren der SMTP-Einstellungen

Konfigurieren Sie die SMTP-Einstellungen für den ausgehenden Mailserver, um Alarme zu aktivieren.

Die SMTP-Einstellungen konfigurieren Sie in der Domänenansicht **Eigenschaften**.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Domäne**.
2. Wählen Sie die Domäne im Navigator aus.
3. Klicken Sie im Inhaltsbereich auf die Ansicht **Eigenschaften**.
4. Klicken Sie im Abschnitt „SMTP-Konfiguration“ auf **Bearbeiten**.
5. Bearbeiten Sie die SMTP-Einstellungen.

Eigenschaft	Beschreibung
Hostname	Hostname für ausgehenden SMTP-Mailserver. Geben Sie zum Beispiel den Microsoft Exchange-Server für Microsoft Outlook ein.
Port	Vom ausgehenden Mailserver verwendeter Port. Die gültigen Werte liegen zwischen 1 und 65535. Standardwert ist 25.
Benutzername	Benutzername für die Authentifizierung beim Senden, wenn dies vom ausgehenden Mailserver gefordert wird.
Passwort	Benutzerpasswort für die Authentifizierung beim Senden, wenn dies vom ausgehenden Mailserver gefordert wird.
E-Mail-Adresse des Absenders	E-Mail-Adresse, die der Dienstmanager im Feld „Von“ beim Senden von Benachrichtigungs-E-Mails verwendet. Wenn Sie dieses Feld leer lassen, verwendet der Dienstmanager Administrator@<Hostname> als Absender.

6. Klicken Sie auf **OK**.

Alarme abonnieren

Nachdem Sie die SMTP-Konfiguration abgeschlossen haben, können Sie Alarme abonnieren.

1. Überprüfen Sie, ob der Domänenadministrator eine gültige E-Mail-Adresse für Ihr Benutzerkonto auf der Seite **Sicherheit** eingegeben hat.
Wenn die E-Mail-Adresse oder die SMTP-Konfiguration ungültig ist, kann der Service Manager keine Warnmeldung liefern.
2. Klicken Sie im Kopfbereich des Administrator-Tools auf **Einstellungen > verwalten**.
Die Seite **Einstellungen** erscheint.
3. Klicken Sie im Abschnitt "Benutzereinstellungen" auf **Bearbeiten**.
Das Dialogfeld **Einstellungen bearbeiten** erscheint.

4. Wählen Sie **Alarmer abonnieren** aus.
5. Klicken Sie auf **OK**.
6. Klicken Sie auf **OK**.

Der Service Manager schickt E-Mails mit Warnmeldungen entsprechend Ihren Domänen-Berechtigungen.

Die folgende Tabelle listet die Alarmtypen und Ereignisse für Benachrichtigungs-E-Mails auf:

Alarmtyp	Ereignis
Domäne	Knotenfehler Master Gateway Election
Dienst	Dienstprozess Failover

Alarmer anzeigen

Wenn Sie Alarmer abonnieren, erhalten Sie zu bestimmten Ereignissen Domänen- und Dienstbenachrichtigungen per E-Mail. Tritt in der Domäne oder dem Dienst ein Ereignis auf, das die Benachrichtigung auslöst, können Sie den Alarmstatus wie folgt nachverfolgen:

- Der Service Manager schickt an alle Abonnenten, die für diese Domäne oder diesen Dienst die entsprechenden Berechtigungen haben, eine E-Mail mit der Alarmbenachrichtigung.
- Der Log-Manager protokolliert die erfolgreiche oder fehlgeschlagene Zustellung der Alarmbenachrichtigung im Domänen- oder Dienstprotokoll.

Zum Beispiel: Der Service Manager schickt die folgende Benachrichtigung an alle Abonnenten, die für den fehlerhaften Dienst die entsprechenden Berechtigungen haben:

```
From: Administrator@<database host>
To: Jon Smith
Subject: Alert message of type [Service] for object [HR_811].
The service process on node [node01] for service [HR_811] terminated unexpectedly.
```

Ferner schreibt der Protokoll-Manager die folgende Meldung in das Dienstprotokoll:

```
ALERT_10009 Alert message [service process failover] of type [service] for object
[HR_811] was successfully sent.
```

Sie können die Protokolle der Domäne oder des Dienstes nach unzustellbaren E-Mails für Alarmbenachrichtigungen durchsehen. Im Domänenprotokoll filtern Sie nach der Kategorie Alarmer. Im Dienstprotokoll suchen Sie nach dem Meldungscode ALERT. Wenn der Service Manager keine E-Mail zur Alarmbenachrichtigung versenden kann, erscheint folgende Meldung im Domänen- oder Dienstprotokoll:

```
ALERT_10004: Unable to send alert of type [alert type] for object [object name], alert
message [alert message], with error [error].
```

Ordnerverwaltung

Verwenden Sie Ordner in der Domäne, um Objekte zu organisieren und die Sicherheit zu verwalten.

Ordner können Knoten, Dienste, Gitter, Lizenzen und andere Ordner enthalten. Möglicherweise brauchen Sie Ordner ebenfalls zum Gruppieren der Dienste nach Typ. So können Sie zum Beispiel einen Ordner anlegen, den Sie IntegrationServices nennen, und alle Integration Services dort hineinschieben. Oder Sie erstellen Ordner zum Gruppieren aller Dienste für einen Funktionsbereich, wie Vertrieb oder Finanzen.

Wenn Sie eine Benutzerberechtigung für den Ordner festlegen, erbt der Benutzer die Berechtigung für sämtliche Objekte in diesem Ordner.

Mit Ordnern können Sie folgende Tasks durchführen:

- Anzeigen von Diensten und Knoten. Anzeigen aller Dienste in dem Ordner und der Knoten, auf denen sie ausgeführt werden. Anklicken eines Konten- oder Dienstnamens für den Zugriff auf die Eigenschaften dieses Knotens oder Dienstes.
- Ordner erstellen. Ordner zum Gruppieren von Objekten in der Domäne erstellen.
- Verschieben von Objekten in Ordner. Wenn Sie ein Objekt in einen Ordner verschieben, erben die Benutzer des Ordners die Berechtigung für das Objekt im Ordner. Beim Verschieben eines Ordners in einen anderen Ordner wird der andere Ordner zum übergeordneten Ordner des verschobenen Ordners.
- Entfernen von Ordnern. Wenn Sie einen Ordner entfernen, können Sie die Objekte in dem Ordner löschen oder in den übergeordneten Ordner verschieben.

Hinweis: Der Ordner System_Services wird bei Erstellung der Domäne für Sie erstellt und enthält alle Systemdienste. Ein Systemdienst ist ein Anwendungsdienst, der in der Domäne eine einzelne Instanz haben kann. Die Eigenschaften oder Inhalte des Ordners System_Services können nicht gelöscht, verschoben oder bearbeitet werden.

Erstellen eines Ordners

Sie können einen Ordner in der Domäne oder in einem anderen Ordner erstellen.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten** > Ansicht **Dienste und Knoten**.
2. Wählen Sie im Domänen-Navigator die Domäne oder den Ordner aus, in der bzw. dem Sie einen Ordner erstellen möchten.
3. Im Menü Navigator-Aktionen klicken Sie auf Neu > Ordner.
4. Bearbeiten Sie die folgenden Eigenschaften:

Eigenschaft „Knoten“	Beschreibung
Name	Name des Ordners. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Er darf nicht länger als 80 Zeichen sein oder mit @ beginnen. Außerdem darf er weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () []
Beschreibung	Beschreibung des Ordners. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Pfad	Speicherort im Navigator.

5. Klicken Sie auf OK.

Objekte in einen Ordner verschieben

Wenn Sie ein Objekt in einen Ordner verschieben, erben die Ordnerbenutzer die Berechtigung für das Objekt. Wenn Sie einen Ordner in einen anderen Ordner verschieben, wird der verschobene Ordner zu einem untergeordneten Objekt des Ordners, in dem er sich befindet.

Hinweis: Die Domäne dient als Ordner, wenn Sie Objekte in Ordner und aus Ordnern verschieben.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten** > Ansicht **Dienste und Knoten**.

2. Wählen Sie im Domänen-Navigator ein Objekt aus.
3. Im Menü Aktionen des Navigation wählen Sie "In Ordner verschieben".
4. Im Dialogfeld Ordner auswählen, markieren Sie einen Ordner und klicken auf OK.

Entfernen eines Ordners

Wenn Sie einen Ordner entfernen, können Sie die Objekte im Ordner löschen oder in den übergeordneten Ordner verschieben.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten** > Ansicht **Dienste und Knoten**.
2. Wählen Sie im Domänen-Navigator einen Ordner aus.
3. Im Menü Aktionen des Navigators wählen Sie "Löschen".
4. Bestätigen Sie, dass Sie den Ordner löschen möchten.

Sie können die Inhalte nur löschen, wenn Sie die entsprechenden Berechtigungen für alle Objekte in dem Ordner besitzen.

5. Wählen Sie aus, ob Sie warten möchten, bis alle Prozesse abgeschlossen sind, oder ob alle Prozesse abgebrochen werden sollen.
6. Klicken Sie auf OK.

Domänensicherheitsmanagement

Sie können die Informatica-Domänenkomponenten so konfigurieren, dass diese das Protokoll Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) zur Verschlüsselung der Verbindungen mit anderen Komponenten verwenden. Wenn Sie für die Domänenkomponenten SSL oder TLS aktivieren, gewährleisten Sie eine sichere Kommunikation.

Eine sichere Kommunikation lässt sich wie folgt konfigurieren:

Zwischen den Diensten innerhalb der Domäne

Konfigurieren Sie die Kommunikation zwischen den Diensten innerhalb einer Domäne sicher.

Zwischen Domäne und externen Komponenten

Sie können die sichere Kommunikation zwischen Informatica-Domänenkomponenten und Web-Browsern oder Web-Dienst-Clients konfigurieren.

Jeder Methode zur Konfigurierung einer sicheren Kommunikation ist unabhängig von den anderen Methoden. Wenn Sie für eine Zusammenstellung von Komponenten eine sichere Kommunikation herstellen, so müssen Sie diese nicht für alle anderen Komponentenzusammenstellungen konfigurieren.

Hinweis: Wenn Sie eine sichere Domäne in eine ungesicherte Domäne oder eine ungesicherte Domäne in eine sichere Domäne ändern, müssen Sie die Domänenkonfiguration im Developer-Tool und in den PowerCenter-Clienttools löschen und die Domäne im Client neu konfigurieren.

Sicherheitsverwaltung für Benutzer

Sie verwalten die Benutzersicherheit innerhalb der Domäne anhand von Berechtigungen.

Berechtigungen bestimmen die Aktionen, die Benutzer an Domänenobjekten durchführen können. Mit Berechtigungen wird die Zugriffsebene eines Benutzers für ein Domänenobjekt festgelegt. Zu den Domänenobjekten zählen Domäne, Ordner, Knoten, Gitter, Lizenzen, Datenbankverbindungen, Betriebssystemprofile und Anwendungsdienste.

Berechtigungen bestimmen die Aktionen, die Benutzer an Domänenobjekten durchführen können. Mit Berechtigungen wird die Zugriffsebene eines Benutzers für ein Domänenobjekt festgelegt. Domänenobjekte umfassen die Domäne, den Knoten, die Lizenz, Datenbankverbindungen und Anwendungsdienste.

Auch wenn ein Benutzer über die Domänenberechtigung zum Abschließen bestimmter Aktionen verfügt, benötigt er ggf. die Berechtigung zum Abschließen der Aktion für ein bestimmtes Objekt. Ein Benutzer verfügt beispielsweise über die Domänenberechtigung "Dienste verwalten", die dem Benutzer die Möglichkeit einräumt, Anwendungsdienste zu bearbeiten. Doch muss der Benutzer auch über die Berechtigung für den Anwendungsdienst haben. Ein Benutzer mit der Domänenberechtigung "Dienste verwalten" und der Berechtigung für den Development Repository Service, aber nicht für den Production Repository Service, kann den Development Repository Service bearbeiten, aber nicht den Produktion Repository Service.

Auch wenn ein Benutzer über die Domänenberechtigung zum Abschließen bestimmter Aktionen verfügt, benötigt er ggf. die Berechtigung zum Abschließen der Aktion für ein bestimmtes Objekt.

Um sich beim Administrator-Tool anmelden zu können, muss ein Benutzer über die Domänenberechtigung "Informatica Administrator öffnen" verfügen. Wenn ein Benutzer über die Berechtigung "Informatica Administrator öffnen" und über die Berechtigung für ein Objekt verfügt, nicht aber über die Domänenberechtigung, die ihm eine Änderung des Objekttyps ermöglicht, kann der Benutzer das Objekt anzeigen. Zum Beispiel: Wenn ein Benutzer über die Berechtigung für einen Knoten verfügt, aber nicht für das Verwalten von Knoten und Gittern, kann er die Eigenschaften des Knotens anzeigen, ihn aber nicht konfigurieren, herunterfahren oder entfernen.

Um sich beim Administrator-Tool anmelden zu können, muss ein Benutzer über die Domänenberechtigung "Informatica Administrator öffnen" verfügen. Wenn ein Benutzer über die Berechtigung "Informatica Administrator öffnen" und über die Berechtigung für ein Objekt verfügt, nicht aber über die Domänenberechtigung, die ihm eine Änderung des Objekttyps ermöglicht, kann der Benutzer das Objekt anzeigen.

Wenn ein Benutzer keine Berechtigung für ein ausgewähltes Objekt im Navigator hat, zeigt der Inhaltsbereich eine Meldung, dass die Berechtigung für das Objekt verweigert wird.

Anwendungsdienstverwaltung

Folgende Verwaltungstasks lassen sich für Anwendungsdienste ausführen:

- Dienste und Dienstprozesse aktivieren und deaktivieren.
- Die Domäne für den Neustart von Dienstprozessen konfigurieren.
- Anwendungsdienste entfernen.
- Probleme mit einem Anwendungsdienst beheben.

Hinweis: Sie können alle allgemeinen Verwaltungsaufgaben für Systemdienste ausführen, bis auf das Entfernen des Systemdiensts.

Aktivieren und Deaktivieren von Diensten und Dienstprozessen

Anwendungsdienste und Dienstprozesse aktivieren und deaktivieren können Sie im Administrator-Tool. Ist ein Dienst aktiviert, muss mindesten ein Dienstprozess aktiviert sein und ausgeführt werden, damit der Dienst verfügbar ist. Per Standard sind alle Dienstprozesse aktiviert.

Das Verhalten eines Dienstes beim Starten von Dienstprozessen ist von seiner Konfiguration abhängig:

- Ist der Dienst für hohe Verfügbarkeit konfiguriert, startet der Dienst den Dienstprozess auf dem Primärknoten. Alle Backup-Knoten sind in Standby
- Ist der Dienst für die Ausführung auf einem Gitter konfiguriert, startet er auf allen Knoten Dienstprozesse.

Einen deaktivierten Dienstprozess startet ein Dienst unter keinen Umständen.

Der Status eines Dienstes ist vom Status der Dienstprozesse abhängig, aus denen er sich zusammensetzt. Ein Dienst kann folgenden Status haben:

- Verfügbar. Sie haben den Dienst aktiviert und mindestens ein Dienstprozess wird ausgeführt. Der Dienst steht für die Bearbeitung von Anfragen zur Verfügung.
- Nicht verfügbar. Sie haben den Dienst aktiviert, aber es werden keine Dienstprozesse ausgeführt. Dies kann darauf zurückzuführen sein, dass Dienstprozesse deaktiviert wurden oder nicht starten können. Der Dienst steht nicht zur Bearbeitung von Anfragen zur Verfügung.
- Deaktiviert. Sie haben den Dienst deaktiviert.

Sie können einen Dienst deaktivieren, um einen Verwaltungsaufgaben durchzuführen, wie Ändern des Datenverschiebungsmodus für einen PowerCenter Integration Service. Vielleicht müssen Sie den Dienstprozess auf einem Knoten deaktivieren, wenn Sie den Knoten zu Wartungszwecken herunterfahren müssen. Wenn Sie einen Dienst deaktivieren, werden alle zugeordneten Dienstprozesse angehalten, bleiben aber aktiviert.

Sie können einen Dienst deaktivieren, um eine Verwaltungsaufgabe durchzuführen. Wenn Sie einen Dienst deaktivieren, werden alle zugeordneten Dienstprozesse angehalten, bleiben aber aktiviert.

Folgende Tabelle beschreibt, welchen Status ein Dienstprozess haben kann:

Dienstprozessstatus	Prozesskonfiguration	Beschreibung
Wird ausgeführt	Aktiviert	Der Dienstprozess läuft auf dem Knoten.
In Standby	Aktiviert	Der Dienstprozess ist aktiviert, wird jedoch nicht ausgeführt, da ein anderer Dienstprozess als primärer Dienstprozess ausgeführt wird. Er befindet sich im Standby, um bei Failover des Dienstes ausgeführt zu werden. Hinweis: Läuft der PowerCenter Integration Service auf einem Gitter, können Dienstprozesse keinen Standby-Status haben. Wenn Sie den PowerCenter Integration Service auf einem Gitter ausführen, werden alle Dienstprozesse gleichzeitig ausgeführt.
Deaktiviert	Deaktiviert	Der Dienst ist aktiviert, aber der Dienstprozess ist angehalten und wird nicht auf dem Knoten ausgeführt.
Gestoppt	Aktiviert	Der Dienst ist nicht verfügbar.
Fehlgeschlagen	Aktiviert	Dienst und Dienstprozess sind aktiviert, aber der Dienstprozess konnte nicht starten.

Hinweis: Kann ein Dienstprozess nicht auf dem zugeordneten Knoten starten, befindet er sich im Fehlerstatus.

Dienstprozesse anzeigen

Sie können den Status eines Dienstprozesses anzeigen, indem Sie in die Prozessansicht eines Dienstes wechseln. Sie können den Status aller Dienstprozesse in der Übersichtsansicht der Domäne anzeigen. Um den Status aller Dienstprozesse anzuzeigen verfahren Sie wie folgt:

1. Klicken Sie im Administrator-Tool auf die Registerkarte "Domäne".
2. Wählen Sie im Navigator einen Dienst aus.
3. Klicken Sie im Inhaltsbereich auf die Ansicht "Prozesse".

In der Prozessansicht wird der Status der Prozesse dargestellt.

Konfigurieren des Neustarts für Dienstprozesse

Wird ein Anwendungsdienstprozess bei laufendem Knoten nicht verfügbar, versucht die Domäne, den Prozess auf demselben Knoten basierend auf den in den Domäneneigenschaften konfigurierten Neustartoptionen neu zu starten.

1. Klicken Sie im Administrator-Tool auf die Registerkarte "Domäne".
2. Wählen Sie die Domäne im Navigator aus.
3. Konfigurieren Sie in der Ansicht "Eigenschaften" die folgenden Neustarteigenschaften:

Domäneneigenschaft	Beschreibung
Maximale Anzahl Neustartversuche	Gibt an, wie oft die Domäne im angegebenen Zeitraum versucht, einen Anwendungsdienstprozess zu starten, der fehlschlägt. Der Wert muss größer oder gleich 1 sein. Voreingestellt ist 3.
Innerhalb des Neustartzeitraums (Sek.)	Maximaler Zeitraum, in dem die Domäne versucht, einen fehlschlagenden Anwendungsdienstprozess neu zu starten. Wenn ein Dienst nicht nach der angegebenen Anzahl von Versuchen in diesem Zeitraum startet, startet er überhaupt nicht. Voreingestellt ist 900.

Anwendungsdienste entfernen

Sie können einen Anwendungsdienst über das Administrator Tool löschen. Bevor Sie einen Anwendungsdienst entfernen, müssen Sie ihn deaktivieren.

Hinweis: Sie können einen Systemdienst nicht entfernen.

Deaktivieren Sie den Dienst, bevor Sie ihn löschen, um sicherzustellen, dass der Dienst keine Prozesse ausführt. Wenn Sie den Dienst nicht deaktivieren, können beim Löschen des Dienstes wählen zu warten, bis alle Prozesse abgeschlossen sind, oder alle Prozesse abubrechen.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten** > Ansicht **Dienste und Knoten**.
2. Wählen Sie im Domänen-Navigator den Anwendungsdienst aus.
3. Wählen Sie auf der Registerkarte **Verwalten** im Menü „Aktionen“ **Löschen** aus.
4. Klicken Sie in der daraufhin angezeigten Warnmeldung auf **Ja**, um andere Dienste zu stoppen, die von dem Anwendungsdienst abhängig sind.

5. Wenn das Dialogfeld **Dienst deaktivieren** angezeigt wird, warten Sie entweder, bis alle Prozesse abgeschlossen sind, oder brechen Sie alle Prozesse ab und klicken Sie dann auf **OK**.

Problembehebung für Anwendungsdienste

Ich habe den Eindruck, dass ein Dienst falsche Werte für die Umgebungsvariablen benutzt. Wie kann ich herausfinden, welche Umgebungsvariablenwerte von einem Dienst verwendet werden?

Setzen Sie den Fehlerschweregrad für den Knoten auf Debug. Wenn der Dienst auf dem Knoten startet, zeigt der Domänen-Log die Umgebungsvariablen an, die der Dienst verwendet.

Knotenverwaltung

Ein Knoten ist eine logische Darstellung eines physischen Computers in der Domäne. Während der Installation definieren Sie mindestens einen Knoten, der als Gateway für die Domäne dient. Sie können mit dem Installationsprogramm oder dem *infasetup* Befehlszeilenprogramm andere Knoten definieren.

Ein Knoten ist eine logische Darstellung eines physischen Computers in der Domäne. Der Knoten wird im Navigator angezeigt, in dem Sie die Knoteneigenschaften anzeigen und bearbeiten können. Verwenden Sie die Registerkarte „Domäne“ des Administrator-Tools zum Verwalten der Knoteneigenschaften.

Ein Knoten ist eine logische Darstellung eines physischen Computers in der Domäne. Der Knoten wird im Navigator angezeigt, in dem Sie die Knoteneigenschaften anzeigen und bearbeiten können. Verwenden Sie die Registerkarte „Domäne“ des Administrator-Tools zum Verwalten der Knoteneigenschaften.

Nachdem Sie einen Knoten definiert haben, müssen Sie den Knoten in die Domäne aufnehmen. Wenn Sie einen Knoten zur Domäne hinzufügen, erscheint der Knoten im Navigator, und Sie können seine Eigenschaften ansehen und bearbeiten. Verwenden Sie die Registerkarte „Domäne“ im Administrator-Tool, um Knoten, einschließlich der Konfiguration von Knoteneigenschaften und dem Entfernen von Knoten aus einer Domäne, zu verwalten.

Mit den folgenden Aufgaben verwalten Sie einen Knoten:

- Definieren Sie den Knoten und fügen Sie ihn der Domäne hinzu. Fügt den Knoten der Domäne hinzu und ermöglicht es der Domäne, mit dem Knoten zu kommunizieren. Nachdem Sie einen Knoten zu einer Domäne hinzugefügt haben, können Sie den Knoten starten.
- Konfigurieren der Eigenschaften. Konfigurieren Sie die Knoteneigenschaften, wie z. B. das Repository-Backup-Verzeichnis und Ports, die verwendet werden, um Prozesse auszuführen.
- Anzeigen von Prozessen. Zeigen Sie die Prozesse an, die für die Ausführung auf dem Knoten konfiguriert wurden, sowie deren Status. Bevor Sie einen Knoten entfernen oder herunterfahren, stellen Sie sicher, dass alle laufenden Prozesse gestoppt wurden.
- Knoten herunterfahren. Fahren Sie den Knoten herunter, wenn Sie Wartungsarbeiten auf dem Computer ausführen müssen, oder um sicherzustellen, dass Änderungen an der Domänenkonfiguration wirksam werden.
- Knoten entfernen. Entfernen Sie einen Knoten aus der Domäne, wenn Sie ihn nicht mehr benötigen.
- Ressourcen definieren. Wenn der PowerCenter-Integrationsdienst auf einem Gitter läuft, können Sie ihn konfigurieren, um die verfügbaren Ressourcen auf jedem Knoten zu überprüfen. Zuweisen von Verbindungsressourcen und Definieren von benutzerdefinierten und Datei-/Verzeichnisressourcen auf einem Knoten.

- Bearbeiten von Berechtigungen. Zeigen Sie geerbte Berechtigungen für den Knoten an und verwalten Sie die Objektberechtigungen für den Knoten.

Hinweis: Wenn Sie einen Knoten hinzufügen oder entfernen, müssen Sie die Domänenkonfiguration im Developer-Tool und in den PowerCenter-Clienttools löschen und die Domäne erneut im Client konfigurieren.

Mit den folgenden Aufgaben verwalten Sie einen Knoten:

- Konfigurieren der Eigenschaften. Konfigurieren Sie Knoteneigenschaften, wie z. B. das Backup-Verzeichnis des Repositorys.
- Anzeigen von Prozessen. Zeigen Sie die Prozesse an, die für die Ausführung auf dem Knoten konfiguriert wurden, sowie deren Status.
- Bearbeiten von Berechtigungen. Zeigen Sie geerbte Berechtigungen für den Knoten an und verwalten Sie die Objektberechtigungen für den Knoten.

Mit den folgenden Aufgaben verwalten Sie einen Knoten:

- Konfigurieren der Eigenschaften. Konfigurieren Sie Knoteneigenschaften, wie z. B. das Backup-Verzeichnis des Repositorys.
- Anzeigen von Prozessen. Zeigen Sie die Prozesse an, die für die Ausführung auf dem Knoten konfiguriert wurden, sowie deren Status.
- Bearbeiten von Berechtigungen. Zeigen Sie geerbte Berechtigungen für den Knoten an und verwalten Sie die Objektberechtigungen für den Knoten.

Hinzufügen von Knoten zur Domäne

Sie können das Administrator tool verwenden, um einen Knoten zur Domäne hinzuzufügen.

Verwenden Sie das Administrator tool zum Hinzufügen eines Knotens zur Domäne in den folgenden Situationen:

- Nach dem Ausführen der Befehle „infasetup DefineGatewayNode“ oder „infasetup DefineWorkerNode“.
- Wenn Sie den Knoten vor Ausführen des Informatica-Installationsprogramms oder des infasetup-Befehlszeilenprogramms hinzufügen möchten, um den Knoten zu definieren.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten** > Ansicht **Dienste und Knoten**.
2. Wählen Sie im Domänen-Navigator den Ordner aus, dem Sie den Knoten hinzufügen möchten. Wenn der Knoten nicht in einem Ordner erscheinen soll, wählen Sie die Domäne aus.
3. Klicken Sie im Navigator-Menü „Aktionen“ auf **Neu > Knoten**.
Das Dialogfeld **Knoten erstellen** wird angezeigt.
4. Geben Sie den Knotennamen ein.
Der Name muss mit dem Knotennamen übereinstimmen, den Sie bei der Definition des Knotens verwenden.
5. Wenn Sie den Ordner für den Knoten ändern möchten, klicken Sie auf **Durchsuchen** und wählen Sie einen neuen Ordner oder die Domäne.
6. Optional können Sie die Knotenrolle aktualisieren.
Standardmäßig verfügt jeder Knoten sowohl über die Dienstrolle als auch die Berechnungsrolle. Wenn ein Knoten einem Datenintegrationsdienst-Gitter zugewiesen ist, können Sie die Knotenrolle aktualisieren, um den Knoten zum Ausführen von Mappings oder des Datenintegrationsdienst-Prozesses zu bestimmen.

7. Klicken Sie auf **OK**.

Wenn Sie einen Knoten hinzufügen, bevor Sie den Knoten mit dem Informatica-Installationsprogramm oder mit „infasetup“ definiert haben, zeigt das Administrator tool eine Meldung an mit der Information, dass Sie das Installationsprogramm ausführen müssen, um dem Knoten einen physischen Hostnamen und eine Portnummer zuzuweisen.

Konfigurieren der Knoteneigenschaften

Knoteneigenschaften werden in der Ansicht „Eigenschaften“ des Knotens konfiguriert. Sie können Eigenschaften, wie die Fehlerdringlichkeitsstufe und die niedrigste und höchste Portnummer, konfigurieren.

1. Klicken Sie im Administrator-Tool auf die Registerkarte **Domäne**.
2. Wählen Sie im Navigator einen Knoten aus.
3. Klicken Sie auf die Ansicht „Eigenschaften“.

In der Ansicht Eigenschaften stehen die Knoteneigenschaften in separaten Abschnitten.

4. Klicken Sie in der Ansicht „Eigenschaften“ für den Abschnitt mit der einzurichtenden Eigenschaft auf **Bearbeiten**.

Sie können die allgemeinen Eigenschaften des Knotens nicht bearbeiten.

5. Bearbeiten Sie die folgenden Eigenschaften:

Eigenschaft „Knoten“	Beschreibung
Name	Name des Knotens Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Er darf weder mehr als 128 Zeichen enthalten noch mit @ beginnen. Außerdem darf er weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () []
Beschreibung	Beschreibung des Knotens Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Hostname	Hostname des vom Knoten dargestellten Computers.
Port	Die vom Knoten verwendete Portnummer.
Gateway-Knoten	Gibt an, ob der Knoten als Gateway eingesetzt werden kann. Wenn diese Eigenschaft auf Nein gesetzt wurde, handelt es sich um einen Worker-Knoten.
Backup-Verzeichnis	Verzeichnis zum Speichern der Backup-Dateien des Repositorys. Der Zugriff auf das Verzeichnis muss über den Knoten möglich sein.

Eigenschaft „Knoten“	Beschreibung
Fehlerdringlichkeitsstufe	<p>Ebene der Fehlerprotokollierung für den Knoten. Diese Meldungen werden in den Protokollmanager-Anwendungsdienst und die Dienstmanager-Protokolldateien geschrieben. Legen Sie eine der folgenden Meldungsebenen fest:</p> <ul style="list-style-type: none"> - ERROR Schreibt ERROR-Codemeldungen in das Protokoll. - WARNING Schreibt WARNING- und ERROR-Codemeldungen in das Protokoll. - INFO Schreibt INFO-, WARNING- und ERROR-Codemeldungen in das Protokoll. - TRACING Schreibt TRACE-, INFO-, WARNING- und ERROR-Codemeldungen in das Protokoll. - DEBUG Schreibt DEBUG-, TRACE-, INFO-, WARNING- und ERROR-Codemeldungen in das Protokoll. <p>Standardwert ist WARNING.</p>
Niedrigste Portnummer	Niedrigste von den Dienstprozessen auf dem Knoten verwendete Portnummer. Starten Sie Informatica-Dienste neu, um die Änderungen zu übernehmen. Der Standardwert ist der bei der Definition des Knotens eingegebene Wert.
Höchste Portnummer	Höchste von den Dienstprozessen auf dem Knoten verwendete Portnummer. Starten Sie Informatica-Dienste neu, um die Änderungen zu übernehmen. Der Standardwert ist der bei der Definition des Knotens eingegebene Wert.
CPU-Profil-Benchmark	<p>Stuft die CPU-Leistung des Knotens im Vergleich zu einem Baseline-System ein. Beispiel: Wenn die CPU 1,5 Mal schneller als der Baseline-Computer ausgeführt wird, beträgt der Wert dieser Eigenschaft 1,5. Sie können den Benchmark berechnen, indem Sie auf Aktionen > CPU-Profil-Benchmark neu berechnen klicken. Die Berechnung dauert ca. fünf Minuten und lastet eine CPU des Computers zu 100% aus. Sie können den Wert jedoch auch manuell aktualisieren.</p> <p>Der Standardwert ist 1,0. Der Minimalwert beträgt 0,001. Der Maximalwert beträgt 1.000.000.</p> <p>Wird im adaptiven Sendemodus verwendet. Im Sendemodus auf Zufallsbasis (Round-Robin) oder im messgrößenbasierten Sendemodus wird die Eigenschaft ignoriert.</p>
Maximale Anzahl der Prozesse	<p>Maximale Anzahl der ausgeführten Sitzungs- oder Befehlsaufgaben, die für jeden auf dem Knoten ausgeführten PowerCenter-Integrationsdienstprozess zulässig sind. Wenn Sie den Wert beispielsweise auf 5 setzen, können bis zu 5 Befehlsaufgaben und 5 Sitzungsaufgaben ausgeführt werden.</p> <p>Damit der Load Balancer diesen Schwellenwert ignoriert, müssen Sie ihn auf einen hohen Wert, wie etwa 200, einstellen. Damit der Load Balancer keine Aufgaben an diesen Knoten sendet, stellen Sie diesen Schwellenwert auf 0 ein.</p> <p>Standardwert ist 10. Der Minimalwert beträgt 0. Der Maximalwert beträgt 1.000.000.000.</p> <p>Wird in allen Sendemodi verwendet.</p>
Maximale Länge der CPU-Ausführungswarteschlange	<p>Maximale Anzahl an ausführbaren Threads, die auf CPU-Ressourcen auf dem Knoten warten. Setzen Sie diesen Schwellenwert auf einen niedrigen Wert, wenn Sie Ressourcen für andere Anwendungen aufbewahren möchten. Setzen Sie diesen Schwellenwert auf einen hohen Wert (z. B. 200), wenn er vom Load Balancer ignoriert werden soll.</p> <p>Standardwert ist 10. Der Minimalwert beträgt 0. Der Maximalwert beträgt 1.000.000.000.</p> <p>Wird im metrisch basierten und adaptiven Sendemodus eingesetzt. Im Runklaufmodus wird der Wert ignoriert.</p>

Eigenschaft „Knoten“	Beschreibung
Maximaler Speicher %	<p>Maximaler Prozentsatz des virtuellen Speichers, der auf dem Knoten relativ zur Gesamtgröße des virtuellen Speichers zugeordnet ist.</p> <p>Setzen Sie diesen Schwellenwert auf einen Wert größer 100%, wenn Sie zulassen möchten, dass beim Senden von Aufgaben mehr virtuelle Speicherkapazität als physische Speicherkapazität zugewiesen werden kann. Setzen Sie diesen Schwellenwert auf einen hohen Wert (z. B. 1.000), wenn er vom Load Balancer ignoriert werden soll.</p> <p>Standardwert ist 150. Der Minimalwert beträgt 0. Der Maximalwert beträgt 1.000.000.000.</p> <p>Wird im metrisch basierten und adaptiven Sendemodus eingesetzt. Im Runklaufmodus wird der Wert ignoriert.</p>
Verzeichnis für die Protokollsammlung	<p>Das Verzeichnis, in dem die Protokolle für den Anwendungsdienst gespeichert werden, wenn der Protokoll-Aggregator ausgeführt wird. Der Zugriff auf das Verzeichnis muss von allen Knoten in der Domäne aus möglich sein. Wenn andere Knoten nicht auf das Verzeichnis für die Protokollsammlung zugreifen können, werden die zusammengefassten Protokolle nicht im Listengitter der zusammengefassten Protokolle angezeigt. Die Benutzer, die Knotenprozesse ausführen, müssen über Lese-/Schreibberechtigungen für das Verzeichnis verfügen.</p> <p>Konfigurieren Sie das Verzeichnis für die Protokollsammlung für den Master-Gateway-Knoten in der Domäne.</p>
Hauptspeicherverzeichnis	<p>Das Verzeichnis, in dem die Hauptspeicherdateien für die Domänenprozesse gespeichert werden, wenn der Protokoll-Aggregator ausgeführt wird.</p> <p>Konfigurieren Sie das Hauptspeicherverzeichnis für alle Knoten in der Domäne.</p>

Eigenschaft „Knoten“	Beschreibung
Backup-Verzeichnis	Das Verzeichnis, in dem Repository-Backup-Dateien gespeichert werden. Der Zugriff auf das Verzeichnis muss über den Knoten möglich sein.
Fehlerdringlichkeitsstufe	<p>Ebene der Fehlerprotokollierung für den Knoten. Diese Meldungen werden in den Protokollmanager-Anwendungsdienst und die Dienstmanager-Protokolldateien geschrieben. Legen Sie eine der folgenden Meldungsebenen fest:</p> <ul style="list-style-type: none"> - ERROR Schreibt ERROR-Codemeldungen in das Protokoll. - WARNING Schreibt WARNING- und ERROR-Codemeldungen in das Protokoll. - INFO Schreibt INFO-, WARNING- und ERROR-Codemeldungen in das Protokoll. - TRACING Schreibt TRACE-, INFO-, WARNING- und ERROR-Codemeldungen in das Protokoll. - DEBUG Schreibt DEBUG-, TRACE-, INFO-, WARNING- und ERROR-Codemeldungen in das Protokoll. <p>Standardwert ist WARNING.</p>
Niedrigste Portnummer	Niedrigste von den Dienstprozessen auf dem Knoten verwendete Portnummer. Starten Sie Informatica-Dienste neu, um die Änderungen zu übernehmen. Der Standardwert ist der bei der Definition des Knotens eingegebene Wert.
Höchste Portnummer	Höchste von den Dienstprozessen auf dem Knoten verwendete Portnummer. Starten Sie Informatica-Dienste neu, um die Änderungen zu übernehmen. Der Standardwert ist der bei der Definition des Knotens eingegebene Wert.

6. Klicken Sie auf **OK**.

Prozesse auf Knoten anzeigen

Sie können den Status aller Prozesse, die zur Ausführung auf einem Knoten konfiguriert sind, anzeigen. Vor dem Herunterfahren oder Entfernen eines Knotens können Sie den Status der einzelnen Prozesse anzeigen, um die zu deaktivierenden Prozesse festzulegen.

Um einen Prozess auf einem Knoten anzuzeigen, führen Sie diese Schritte aus:

1. Klicken Sie im Administrator-Tool auf die Registerkarte "Domäne".
2. Wählen Sie im Navigator einen Knoten aus.
3. Klicken Sie im Inhaltsbereich auf die Ansicht "Prozesse".

Die Registerkarte zeigt den Status aller Prozesse, die zur Ausführung auf einem Knoten konfiguriert sind, an.

Herunterfahren und Neustarten des Knotens

Für einige administrative Aufgaben ist es möglicherweise erforderlich, dass Sie einen Knoten herunterfahren. Zum Beispiel müssen Sie möglicherweise eine Wartung oder ein Benchmarking auf einem Computer durchführen. Möglicherweise müssen Sie auch einen Knoten herunterfahren und neu starten, damit einige Änderungen an der Konfiguration wirksam werden können. Zum Beispiel, wenn Sie das freigegebene Verzeichnis für den Protokollmanager oder die Domäne ändern, müssen Sie den Knoten herunterfahren und neu starten, um die Konfigurationsdateien zu aktualisieren.

Sie können einen Knoten aus dem Administrator-Tool oder aus dem Betriebssystem heraus herunterfahren. Wenn Sie einen Knoten herunterfahren, werden die Informatica-Dienste gestoppt und alle auf dem Knoten ausgeführten Anwendungsdienstprozesse und Berechnungen abgebrochen.

Um einen Knoten neu zu starten, starten Sie die Informatica-Dienste auf dem Knoten.

Warnhinweis: Um beim Herunterfahren von Knoten den Verlust von Daten oder Metadaten zu vermeiden, deaktivieren Sie alle aktuell ausgeführten Prozesse im vollständigen Modus.

Herunterfahren eines Knotens über das Administrator tool

Wenn Sie einen Knoten über das Administrator tool herunterfahren, können Sie alle auf dem Knoten ausgeführten Anwendungsdienstprozesse anzeigen.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten** > Ansicht **Dienste und Knoten**.
2. Wählen Sie im Domänen-Navigator einen Knoten aus.
3. Wählen Sie im Navigator-Menü **Aktionen** die Option **Knoten herunterfahren** aus.

Wenn der Knoten über die Dienstrolle verfügt, zeigt das Administrator tool die Liste der auf dem Knoten ausgeführten Anwendungsdienstprozesse an.

4. Wählen Sie optional aus, ob das Herunterfahren geplant oder ungeplant sein soll.
5. Fügen Sie optional Kommentare über das Herunterfahren hinzu.
6. Klicken Sie auf **OK**, um alle Dienstprozesse zu stoppen und den Knoten herunterzufahren, oder klicken Sie auf **Abbrechen**, um den Vorgang abzubrechen.

Starten oder Anhalten eines Knotens unter Windows

Um einen Knoten unter Windows zu starten und anzuhalten, führen Sie die folgenden Schritte aus:

1. Öffnen Sie die Windows-Systemsteuerung.
2. Wählen Sie **Verwaltung**.

3. Klicken Sie mit der rechten Maustaste auf **Dienste** und wählen Sie **Als Administrator ausführen** aus.
4. Klicken Sie mit der rechten Maustaste auf den Informatica-Dienst.
5. Wenn der Dienst ausgeführt wird, klicken Sie auf **Beenden**.
Wenn der Dienst angehalten ist, klicken Sie auf **Starten**.

Einen Knoten unter UNIX starten und anhalten

Unter UNIX wird der Informatica-Dämon durch Ausführen von `infaservice.sh` gestartet und beendet. `infaservice.sh` ist standardmäßig im folgenden Verzeichnis installiert:

```
<InformaticaInstallationDir>/tomcat/bin
```

1. Gehen Sie zu dem Verzeichnis, in dem sich `infaservice.sh` befindet.
2. Geben Sie nach der Befehlseingabeaufforderung den folgenden Befehl ein, um den Dämon zu starten:

```
infaservice.sh startup
```

Geben Sie den folgenden Befehl ein, um den Dämon zu beenden:

```
infaservice.sh shutdown
```

Hinweis: Wenn Sie den Speicherort von `infaservice.sh` mithilfe eines Softlinks festlegen, stellen Sie die Umgebungsvariable `INFA_HOME` auf den Speicherort des Informatica-Installationsverzeichnisses ein.

Entfernen der Knotenzuordnung

Sie können den Hostnamen und die Portnummer entfernen, die einem Knoten zugeordnet ist. Wenn Sie die Knotenzuordnungen entfernt haben, bleibt der Knoten in der Domäne, ist aber nicht mehr mit einer Hostmaschine verbunden.

Um dem Knoten einen anderen Hostcomputer zuzuordnen, müssen Sie auf dem neuen Hostcomputer das Installationsprogramm oder den Befehl „`infasetup DefineGatewayNode`“ bzw. „`infasetup DefineWorkerNode`“ ausführen. Anschließend starten Sie den Knoten auf der neuen Hostmaschine erneut.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten** > Ansicht **Dienste und Knoten**.
2. Wählen Sie im Navigator einen Knoten aus.
3. Wählen Sie in der Ansicht **Dienste und Knoten** im Menü **Aktionen** die Option **Knotenzuordnung entfernen** aus.

Entfernen eines Knotens

Wenn Sie einen Knoten aus einer Domäne entfernen, ist er im Navigator nicht mehr sichtbar. Wenn der Knoten ausgeführt wird, während Sie ihn entfernen, wird er heruntergefahren und bricht alle Anwendungsdienstprozesse ab.

Hinweis: Um beim Entfernen von Knoten den Verlust von Daten oder Metadaten zu vermeiden, deaktivieren Sie alle aktuell ausgeführten Prozesse im vollständigen Modus.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten** > Ansicht **Dienste und Knoten**.
2. Wählen Sie im Domänen-Navigator einen Knoten aus.
3. Wählen Sie im Navigator-Menü **Aktionen** die Option **Löschen** aus.
4. Klicken Sie in der angezeigten Warnmeldung auf **OK**.

Gateway-Konfiguration

Ein Gateway-Knoten in der Domäne dient als Master-Gateway-Knoten für die Domäne. Der Dienstmanager auf dem Master-Gateway-Knoten nimmt Dienstanfragen entgegen und verwaltet die Domäne und die Dienste in der Domäne.

Während der Installation erstellen Sie einen Gateway-Knoten. Nach der Installation können Sie weitere Gateway-Knoten erstellen. Vielleicht möchten Sie weitere Gateway-Knoten zu Sicherungszwecken erstellen. Wenn Sie einen Gateway-Knoten haben und dieser unverfügbar wird, kann die Domäne keine Dienstanfragen annehmen. Haben Sie mehrere Gateway-Knoten und der Master-Gateway-Knoten wird unverfügbar, wählen die Dienstmanager der anderen Gateway-Knoten einen neuen Master-Gateway-Knoten. Der neue Master-Gateway-Knoten nimmt Dienstanfragen entgegen. Zu jedem gegebenen Zeitpunkt kann nur ein Gateway-Knoten der Master-Gateway-Knoten sein. Sie müssen immer mindestens einen als Gateway-Knoten definierten Knoten haben. Andernfalls ist die Domäne nicht arbeitsfähig.

Mit dem Befehl `infasetup SwitchGatewayNode` können Sie einen Worker-Knoten als Gateway-Knoten konfigurieren. Der Worker-Knoten muss ausgeführt werden, wenn Sie ihn für die Funktion eines Gateway-Knotens konfigurieren.

Hinweis: Zur Erstellung eines Gateway-Knotens können Sie auch den Befehl `infasetup DefineGatewayNode` verwenden. Wenn Sie einen Worker-Knoten als Gateway-Knoten konfigurieren, müssen Sie das Log-Verzeichnis angeben. Bei mehreren Gateway-Knoten müssen Sie alle zum Schreiben von Log-Dateien in dasselbe Verzeichnis auf einem gemeinsamen Laufwerk konfigurieren.

Nachdem Sie den Gateway-Knoten konfiguriert haben, schreibt der Dienstmanager des Master-Gateway-Knotens die Verbindung der Domänen-Konfigurationsdatenbank in die Datei `nodemeta.xml` des neuen Gateway-Knotens.

Wenn Sie einen Master-Gateway-Knoten als Worker-Knoten konfigurieren, müssen Sie den Knoten neu starten, damit die Dienstmanager einen neuen Master-Gateway-Knoten wählen. Ohne Neustart des Knotens behält der Knoten die Funktion des Master-Gateway-Knotens, bis Sie den Knoten neu starten oder der Knoten unverfügbar wird.

1. Klicken Sie im Administrator-Tool auf die Registerkarte "Domäne".
2. Wählen Sie die Domäne im Navigator aus.
3. Wählen Sie der Inhaltsübersicht die Ansicht „Eigenschaften“ aus.
4. Klicken Sie in der Ansicht „Eigenschaften“ im Abschnitt „Gateway-Konfigurationseigenschaften“ auf „Bearbeiten“.
5. Aktivieren Sie das Kontrollkästchen neben dem Knoten, der der Gateway-Knoten sein soll.
Es können mehrere Knoten als Gateway-Knoten ausgewählt werden.
6. Konfigurieren Sie den Verzeichnispfad für die Protokolldateien.
Bei mehreren Gateway-Knoten konfigurieren Sie alle Gateway-Knoten so, dass sie auf denselben Speicherort für Log-Dateien zeigen.
7. Klicken Sie auf „OK“.

Domänenkonfigurationsverwaltung

Der Service Manager auf dem Master-Gateway-Knoten verwaltet die Domänenkonfiguration. Die Domänenkonfiguration besteht aus einer Reihe von Metadatentabellen, die in einer für alle Gateway-Knoten in der Domäne zugänglichen relationalen Datenbank gespeichert sind. Immer wenn Sie eine Änderung an der

Domäne vornehmen, schreibt der Service Manager die Änderung in die Domänenkonfiguration. Beispiel: Beim Hinzufügen eines Knotens zur Domäne fügt der Service Manager die Knoteninformationen zur Domänenkonfiguration hinzu. Die Gateway-Knoten greifen mittels JDBC-Verbindung auf die Domänenkonfigurations-Datenbank zu.

Sie können folgenden Domänenkonfigurations-Verwaltungstasks ausführen:

- Domänenkonfiguration sichern Sichern Sie die Domänenkonfiguration regelmäßig. Ist die Domänenkonfiguration in der Datenbank verfälscht, müssen Sie die Domänenkonfiguration möglicherweise aus einer Sicherung wiederherstellen.
- Stellen Sie die Domänenkonfiguration wieder her. Vielleicht müssen Sie die Domänenkonfiguration auch wiederherstellen, wenn Sie die Domänenkonfiguration zu einem anderen Datenbank-Benutzerkonto migrieren. Oder Sie müssen die Sicherungs-Domänenkonfiguration in einem Datenbankbenutzerkonto wiederherstellen.
- Migrieren Sie die Domänenkonfiguration. Unter Umständen müssen Sie die Domänenkonfiguration zu einem anderen Datenbank-Benutzerkonto migrieren.
- Konfigurieren Sie die Verbindung zur Domänenkonfigurations-Datenbank. Jeder Gateway-Knoten muss Zugriff auf die Domänenkonfigurations-Datenbank haben. Die Datenbankverbindung wird beim Erstellen der Domäne konfiguriert. Wenn Sie die Datenbank-Verbindungsinformationen ändern oder die Domänenkonfiguration in eine neue Datenbank migrieren, müssen Sie die Datenbank-Verbindungsinformationen für jeden Gateway-Knoten aktualisieren.
- Konfigurieren Sie benutzerdefinierte Eigenschaften. Konfigurieren Sie Domäneneigenschaften, die für Ihre Umgebung eindeutig sind oder in bestimmten Fällen angewendet werden. Benutzerdefinierte Eigenschaften dürfen Sie nur verwenden, wenn Sie vom globalen Kundensupport von Informatica entsprechende Anweisungen erhalten.

Hinweis: Die Domänenkonfigurations-Datenbank und das Model Repository dürfen nicht dasselbe Datenbankbenutzerschema verwenden.

Sichern der Domänenkonfiguration

Sichern Sie die Domänenkonfiguration regelmäßig. Sie können die Domänenkonfiguration von einer Sicherungsdatei wiederherstellen, wenn die Domänenkonfiguration in der Datenbank korrupt wird.

Führen Sie den Befehl `infasetup BackupDomain` aus, um die Domänenkonfiguration in einer Binärdatei zu sichern.

Hinweis: Wenn der `infasetup`-Befehl „BackupDomain“ mit einem Java-Speicherfehler fehlschlägt, stellen Sie für „infasetup“ mehr Systemspeicher zur Verfügung. Um den Systemspeicher zu vergrößern, legen Sie den -Xmx-Wert in der Umgebungsvariablen `INFA_JAVA_COMD_OPTS` fest.

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.

Verwenden Sie zusätzlich das Dienstprogramm zur Datenbanksicherung, um zusätzliche Repository-Tabellen manuell zu sichern, die vom `infasetup`-Befehl nicht gesichert werden.

Wiederherstellen der Domänen-Konfiguration

Sie können eine Domänenkonfiguration aus einer Repository-Backup-Datei wiederherstellen. Unter Umständen müssen Sie die Domänenkonfiguration wiederherstellen, wenn die Domänenkonfiguration in der Datenbank inkonsistent wird oder Sie die Domänenkonfiguration in eine andere Datenbank migrieren möchten.

Informatica stellt die Domänenkonfiguration aus der aktuellen Version wieder her. Wenn Sie über eine Backup-Datei aus einer früheren Produktversion verfügen, müssen Sie die frühere Produktversion verwenden, um die Domänenkonfiguration wiederherzustellen.

Sie können die Domänenkonfiguration in dasselbe oder ein anderes Datenbankbenutzerkonto migrieren. Bei der Wiederherstellung der Domänenkonfiguration in ein Datenbankbenutzerkonto mit einer vorhandenen Domänenkonfiguration müssen Sie den Befehl so konfigurieren, dass die bestehende Domänenkonfiguration überschrieben wird. Wenn Sie den Befehl nicht für das Überschreiben der bestehenden Domänenkonfiguration konfigurieren, schlägt der Befehl fehl.

Jeder Knoten in einer Domäne verfügt über einen Hostnamen und eine Portnummer. Wenn Sie die Domänenkonfiguration wiederherstellen, können Sie die Verknüpfung mit Hostnamen und Portnummern für alle Knoten in der Domäne aufheben. Dies ist sinnvoll, wenn Sie die Knoten auf unterschiedlichen Rechnern laufen lassen möchten. Nachdem Sie die Domänenkonfiguration wiederhergestellt haben, können Sie neue Hostnamen und Portnummern mit den Knoten verknüpfen. Führen Sie den Befehl *infasetup* DefineGatewayNode oder DefineWorkerNode aus, um einem Knoten einen neuen Hostnamen und eine neue Portnummer zuzuweisen.

Wenn Sie die Domänenkonfiguration in eine andere Datenbank wiederherstellen, müssen Sie die Datenbankverbindungen für alle Gateway-Knoten zurücksetzen.

Wichtig: Sie verlieren alle Daten in den Übersichtstabellen, wenn Sie die Domänenkonfiguration wiederherstellen.

Führen Sie folgende Tasks durch, um die Domäne wiederherzustellen:

1. Deaktivieren Sie den Dienst. Fahren Sie die Anwendungsdienste im vollständigen Modus herunter, um sicherzustellen, dass Sie keine laufenden Dienstprozesse abbrechen. Sie müssen die Anwendungsdienste deaktivieren, um sicherzustellen, dass beim Herunterfahren der Domäne kein Dienstprozess ausgeführt wird.
2. Abschalten der Domäne. Sie müssen die Domäne abschalten, um sicherzustellen, dass während der Wiederherstellung der Domäne keine Änderungen an der Domäne vorgenommen werden.
3. Führen Sie den Befehl *infasetup* RestoreDomain aus, um die Domänenkonfiguration in eine Datenbank wiederherzustellen. Der Befehl RestoreDomain stellt die Domänenkonfiguration aus der Backup-Datei im angegebenen Datenbankbenutzerkonto wieder her.
4. Weisen Sie nach der Wiederherstellung der Domänenkonfiguration den Knoten in der Domäne neue Hostnamen und Portnummern zu, wenn Sie die Verknüpfung mit den vorherigen Hostnamen und Portnummern aufgehoben haben. Führen Sie den Befehl *infasetup* DefineGatewayNode oder DefineWorkerNode aus, um einem Knoten einen neuen Hostnamen und eine neue Portnummer zuzuweisen.
5. Setzen Sie die Datenbankverbindungen für alle Gateway-Knoten zurück, wenn Sie die Domänenkonfiguration in eine andere Datenbank wiederherstellen. Alle Gateway-Knoten müssen eine Verbindung zur Domänenkonfigurationsdatenbank haben.

Migrieren der Domänen-Konfiguration

Sie können die Domänenkonfiguration in ein anderes Datenbankbenutzerkonto migrieren. Unter Umständen müssen Sie die Domänenkonfiguration migrieren, wenn Sie das vorhandene Datenbankbenutzerkonto nicht mehr unterstützen. Zum Beispiel: Wenn in Ihrem Unternehmen alle Abteilungen auf einen neuen Datenbanktyp migrieren müssen, müssen Sie auch die Domänenkonfiguration migrieren.

1. Abschalten aller Anwendungsdienste in der Domäne.
2. Abschalten der Domäne.
3. Backup der Domänenkonfiguration erstellen.

4. Erstellen Sie das Datenbankbenutzerkonto dort, wo die Domänenkonfiguration wiederhergestellt werden soll.
5. Stellen Sie das Backup der Domänenkonfiguration im Datenbankbenutzerkonto wieder her.
6. Aktualisieren Sie die Datenbankverbindung für jeden Gateway-Knoten.
7. Starten Sie alle Knoten in der Domäne.
8. Aktivieren Sie alle Anwendungsdienste in der Domäne.

Wichtig: Zusammenfassungstabellen gehen verloren, wenn Sie die Domänenkonfiguration wiederherstellen.

Schritt 1. Herunterfahren aller Anwendungsdienste

Sie müssen alle Anwendungsdienste deaktivieren, um alle Dienstprozesse zu deaktivieren. Wenn Sie einen Anwendungsdienst nicht deaktivieren, und ein Benutzer einen Dienstprozess startet, während Sie die Domäne sichern und wiederherstellen, können die Änderungen des Dienstprozesses verloren gehen, und die Daten können beschädigt werden.

Tipp: Fahren Sie die Anwendungsdienste im vollständigen Modus herunter, um sicherzustellen, dass Sie keine laufenden Dienstprozesse abbrechen.

Schließen Sie die Anwendungsdienste in der nachstehenden Reihenfolge:

1. Webdienst-Hub
2. SAP BW-Dienst
3. Metadata Manager-Dienst
4. PowerCenter-Integrationsdienst
5. PowerCenter-Repository-Dienst
6. Berichterstellungsdienst
7. Suchdienst
8. Analyst-Dienst
9. Content-Managementdienst
10. Datenintegrationsdienst
11. Modellrepository-Dienst
12. Berichterstellungs- und Dashboard-Dienst

Schritt 2. Domäne herunterfahren

Sie müssen die Domäne herunterfahren, um sicherzustellen, dass die Benutzer die Domäne nicht verändern, während Sie die Domänenkonfiguration migrieren. Zum Beispiel: Wenn die Domäne ausgeführt wird, während Sie die Domänenkonfiguration sichern, können Benutzer einen neuen Dienst und neue Objekte erstellen. Hinzu kommt: Wenn Sie die Domäne nicht herunterfahren und die Domänenkonfiguration in einer anderen Datenbank wiederherstellen, ist die Domäne nicht mehr betriebsfähig. Die Verbindungen zwischen den Gateway-Knoten und der Domänenkonfigurationsdatenbank werden ungültig. Die Gateway-Knoten werden heruntergefahren, denn sie können keine Verbindung zur Domänenkonfigurationsdatenbank herstellen. Eine Domäne ist nicht betriebsfähig, wenn sie nicht über einen ausgeführten Gateway-Knoten verfügt.

Schritt 3. Domänenkonfiguration sichern

Führen Sie den Befehl `infasetup BackupDomain` aus, um die Domänenkonfiguration in einer Binärdatei zu sichern.

Schritt 4. Benutzerkonto für Datenbank erstellen

Erstellen Sie ein Datenbankbenutzerkonto, wenn Sie die Domänenkonfiguration in einem neuen Datenbankbenutzerkonto wiederherstellen möchten.

Schritt 5. Domänenkonfiguration wiederherstellen

Führen Sie den Befehl *infasetup RestoreDomain* aus, um die Domänenkonfiguration in einer Datenbank wiederherzustellen. Der Befehl *RestoreDomain* stellt die Domänenkonfiguration aus der Sicherungsdatei im angegebenen Benutzerkonto der Datenbank wieder her.

Schritt 6. Datenbankverbindung prüfen

Wenn Sie die Domänenkonfiguration in einem anderen Datenbankbenutzerkonto wiederherstellen, müssen Sie die Datenbankverbindungsinformationen für jeden Gateway-Knoten in der Domäne aktualisieren. Gateway-Knoten müssen eine Verbindung zur Domänenkonfigurationsdatenbank haben, um die Domänenkonfiguration laden und aktualisieren zu können.

Schritt 7. Knoten in der Domäne starten

Starten Sie alle Knoten in der Domäne. Sie müssen die Knoten starten, um die Dienste für die Ausführung zu aktivieren.

1. Fahren Sie den Gateway-Knoten herunter, den Sie aktualisieren möchten.
2. Führen Sie den Befehl *infasetup UpdateGatewayNode* aus, um den Gateway-Knoten zu aktualisieren.
3. Starten Sie den Gateway-Knoten.
4. Wiederholen Sie diesen Vorgang für jeden Gateway-Knoten.

Schritt 8. Alle Anwendungsdienste aktivieren

Aktivieren Sie alle Anwendungsdienste, die Sie zuvor heruntergefahren haben. Die Anwendungsdienste müssen aktiv sein, um die Dienstprozesse auszuführen.

Aktualisieren der Domänenkonfigurationsdatenbankverbindung

Alle Gateway-Knoten müssen eine Verbindung zur Domänenkonfigurationsdatenbank haben, um die Domänenkonfiguration abzurufen und zu aktualisieren. Wenn Sie einen Gateway-Knoten erstellen oder einen Knoten als Gateway konfigurieren, geben Sie die Datenbankverbindung einschließlich des Benutzernamens und Passworts der Datenbank ein. Wenn Sie die Domäne auf eine andere Datenbank migrieren oder den Datenbankbenutzernamen oder das Passwort ändern, müssen Sie die Datenbankverbindung für jede Gateway-Knoten aktualisieren. Zum Beispiel könnte Ihr Unternehmen im Rahmen einer Sicherheitspolitik verlangen, dass Sie das Passwort für die Domänen-Konfigurationsdatenbank alle drei Monate ändern.

Um den Knoten mit dem neuen Datenbankverbindung zu aktualisieren, führen Sie folgende Schritte durch:

1. Abschalten des Gateway-Knotens.
2. Ausführen des Befehls *infasetup UpdateGatewayNode*.

Wenn Sie den Benutzernamen und das Passwort ändern, müssen Sie den Knoten aktualisieren.

Um den Knoten nach der Änderung des Benutzers oder Passworts zu aktualisieren, führen Sie folgende Schritte durch:

1. Abschalten des Gateway-Knotens.
2. Ausführen des Befehls *infasetup UpdateGatewayNode*.

Wenn Sie den Hostnamen oder die Portnummer ändern, müssen Sie den Knoten neu definieren.

Um den Knoten nach der Änderung des Hostnamens oder der Portnummer neu zu definieren, führen Sie folgende Schritte durch:

1. Abschalten des Gateway-Knotens.
2. Entfernen der Knotenzuweisung im Administrator Tool.
3. Ausführen des Befehls `infasetup DefineGatewayNode`.

Domänenaufgaben

Auf der Registerkarte "Domäne" können Sie Domänenaufgaben wie das Überwachen von Anwendungsdiensten und Knoten, das Verwalten von Domänenobjekten und Protokollen sowie das Anzeigen von Abhängigkeiten zwischen Dienst und Knoten durchführen.

Sie können alle Anwendungsdienste und Knoten in einer Domäne überwachen. Sie können Domänenobjekte auch verwalten, indem Sie sie in Ordner verschieben oder löschen. Des weiteren können Sie Anwendungsdienste recyceln, aktivieren oder deaktivieren und Protokolle für Anwendungsdienste anzeigen.

Sie können alle Anwendungsdienste und den Knoten in einer Domäne überwachen. Des weiteren können Sie Anwendungsdienste recyceln, aktivieren oder deaktivieren und Protokolle für Anwendungsdienste anzeigen.

Sie können alle Anwendungsdienste und den Knoten in einer Domäne überwachen. Des weiteren können Sie Anwendungsdienste recyceln, aktivieren oder deaktivieren und Protokolle für Anwendungsdienste anzeigen.

Sie haben ebenfalls die Möglichkeit, gegenseitige Abhängigkeiten aller Anwendungsdienste und Knoten anzuzeigen. Ein Anwendungsdienst ist abhängig von dem Knoten, auf dem er läuft. Er könnte ebenfalls von einem anderen Anwendungsdienst abhängig sein. So muss der Data Integration Service beispielsweise einem Modellrepository-Dienst zugeordnet sein. Steht der Modellrepository-Dienst nicht zur Verfügung, funktioniert der Data Integration Service nicht.

Zeigen Sie die gegenseitigen Abhängigkeiten der Anwendungsdienste und Knoten an, wenn Sie eine Auswirkungsanalyse durchführen möchten. Anhand der Auswirkungsanalyse können Sie erkennen, welche Auswirkungen bestimmte Domänenaktionen haben, wie das Herunterfahren eines Knotens oder eines Anwendungsdienstes. Beispiel: Sie möchten einen Knoten zwecks Wartungsarbeiten herunterfahren. Bevor Sie den Knoten herunterfahren, müssen Sie alle Anwendungsdienste feststellen, die auf dem Knoten laufen. Ist dies der einzige Knoten, auf dem ein Anwendungsdienst läuft, steht dieser Anwendungsdienst beim Herunterfahren des Knotens nicht zur Verfügung.

Zeigen Sie zur Durchführung einer Auswirkungsanalyse die Abhängigkeiten zwischen den Anwendungsdiensten und dem Knoten an. Anhand der Auswirkungsanalyse können Sie erkennen, welche Auswirkungen bestimmte Domänenaktionen haben, wie das Herunterfahren eines Anwendungsdienstes.

Zeigen Sie zur Durchführung einer Auswirkungsanalyse die Abhängigkeiten zwischen den Anwendungsdiensten und dem Knoten an. Anhand der Auswirkungsanalyse können Sie erkennen, welche Auswirkungen bestimmte Domänenaktionen haben, wie das Herunterfahren eines Anwendungsdienstes.

Verwalten und Überwachen von Anwendungsdiensten und Knoten

KnotenVerwalten und Überwachen von Anwendungsdiensten und Knoten

Sie können Anwendungsdienste und Knoten in einer Domäne verwalten und überwachen. Sie können Anwendungsdienste und einen Knoten in einer Domäne verwalten und überwachen. Sie können Anwendungsdienste und den Knoten in einer Domäne verwalten und überwachen.

1. Klicken Sie im Administrator-Tool auf die Registerkarte **Domäne**.
2. Klicken Sie auf die Ansicht **Dienste und Knoten**.
3. Wählen Sie die Domäne im Navigator aus.
Im Inhaltsbereich werden die in der Domäne definierten Objekte angezeigt.
4. Zum Filtern der im Inhaltsbereich angezeigten Domänenobjekte geben Sie in der Filterleiste Filterkriterien ein.
Der Inhaltsbereich zeigt die Objekte an, die den Filterkriterien entsprechen.
5. Um die Filterkriterien zu entfernen, klicken Sie auf **Zurücksetzen**.
Der Inhaltsbereich zeigt alle in der Domäne definierten Objekte an.
6. Um die Namen der Anwendungsdienste und Knoten Knotendes Knotens im Inhaltsbereich anzuzeigen, klicken Sie auf die Schaltfläche "Details anzeigen".
Im Inhaltsbereich werden die Namen der Anwendungsdienste und Knoten Knotendes Knotens in der Domäne angezeigt.
7. Um die Namen der Anwendungsdienste und Knoten Knotendes Knotens im Inhaltsbereich auszublenden, klicken Sie auf die Schaltfläche "Details ausblenden".
Im Inhaltsbereich werden die Namen der Anwendungsdienste und Knoten Knotendes Knotens in der Domäne ausgeblendet.
8. Um Details zu einem Objekt anzuzeigen, wählen Sie das Objekt im Navigator aus.
Zum Beispiel: Wählen Sie einen Anwendungsdienst im Navigator, um Dienstversion, Dienststatus, Prozessstatus und die letzte Fehlermeldung für den Dienst anzuzeigen.
Die Objektdetails werden angezeigt.
9. Um Eigenschaften für ein Objekt anzuzeigen, wählen Sie das Objekt im Navigator aus.
Der Inhaltsbereich zeigt die Eigenschaften für das Objekt.
10. Zum Recyceln, Aktivieren, Deaktivieren oder Anzeigen von Protokollen für einen Anwendungsdienst doppelklicken Sie im Navigator auf den Anwendungsdienst.
 - Um den Anwendungsdienst zu recyceln, klicken Sie auf die Schaltfläche "Dienst recyceln".
 - Um den Anwendungsdienst zu aktivieren, klicken Sie auf die Schaltfläche "Dienst aktivieren".
 - Um den Anwendungsdienst zu deaktivieren, klicken Sie auf die Schaltfläche "Dienst deaktivieren".
 - Um Protokolle zum Anwendungsdienst anzuzeigen, klicken Sie auf die Schaltfläche "Protokolle für Dienst anzeigen".
11. Zum Recyceln, Aktivieren, Deaktivieren oder Anzeigen von Protokollen für einen Anwendungsdienst doppelklicken Sie im Navigator auf den Anwendungsdienst.
 - Um den Anwendungsdienst zu recyceln, klicken Sie auf die Schaltfläche "Dienst recyceln".
 - Um den Anwendungsdienst zu aktivieren, klicken Sie auf die Schaltfläche "Dienst aktivieren".
 - Um den Anwendungsdienst zu deaktivieren, klicken Sie auf die Schaltfläche "Dienst deaktivieren".
 - Um Protokolle zum Anwendungsdienst anzuzeigen, klicken Sie auf die Schaltfläche "Protokolle für Dienst anzeigen".

12. Um Protokolle zum Anwendungsdienst anzuzeigen, klicken Sie auf die Schaltfläche **Protokolle für Dienst anzeigen**.
13. Um ein Objekt in einen Ordner zu verschieben, führen Sie die folgenden Schritte aus:
 - a. Klicken Sie mit der rechten Maustaste im Navigator auf das Objekt.
 - b. Klicken Sie auf **In Ordner verschieben**.
Das Dialogfeld **Ordner auswählen** wird angezeigt.
 - c. Wählen Sie im Dialogfeld **Ordner auswählen** einen Ordner aus.
Alternativ können Sie einen neuen Ordner erstellen. Klicken Sie dazu auf **Ordner erstellen**.
Das Dialogfeld **Ordner erstellen** wird angezeigt.
Geben Sie den Ordnernamen ein und klicken Sie auf **OK**.
 - d. Klicken Sie auf **OK**.
Das Objekt wird in den angegebenen Ordner verschoben.
14. Um ein Objekt zu löschen, klicken Sie mit der rechten Maustaste im Navigator auf das Objekt.
Klicken Sie auf **Löschen**.

Anzeigen von Abhängigkeiten für Anwendungsdienste, Knoten und Gitter Anzeigen von Abhängigkeiten

In der Ansicht "Dienste und Knoten" auf der Registerkarte "Domäne" können Sie die Abhängigkeiten für Anwendungsdienste, Knoten und Gitter in einer Informatica-Domäne anzeigen. In der Ansicht "Dienste und Knoten" auf der Registerkarte "Domäne" können Sie die Abhängigkeiten für Anwendungsdienste und den Knoten in einer Informatica-Domäne anzeigen.

Zur Anzeige des Fensters **Abhängigkeiten anzeigen** müssen Sie Adobe Flash Player 10.0.0 oder eine spätere Version in Ihrem Browser installiert und aktiviert haben. Wenn Sie den Internet Explorer verwenden, aktivieren Sie die Option **ActiveX-Steuerelement und Plugins ausführen**.

1. Klicken Sie im Administrator-Tool auf die Registerkarte **Domäne**.
2. Klicken Sie auf die Ansicht **Dienste und Knoten**.
3. Wählen Sie die Domäne im Navigator aus.
Im Inhaltsbereich werden die Objekte in der Domäne angezeigt.
4. Klicken Sie im Inhaltsbereich mit der rechten Maustaste auf ein Domänenobjekt und wählen Sie **Abhängigkeiten anzeigen** aus.
Das Fenster **Abhängigkeiten anzeigen** listet die durch blaue und orange Linien verbundenen Domänenobjekte wie folgt auf:
 - Die blauen Linien stellen die Abhängigkeiten von Dienst-zu-Knoten und Dienst-zu-Gitter dar.
 - Die blauen Linien stellen die Abhängigkeiten von Dienst-zu-Knoten dar.
 - Die blauen Linien stellen die Abhängigkeiten von Dienst-zu-Knoten dar.
 - Die orangen Linien stellen die Abhängigkeiten von Dienst-zu-Dienst dar. Um die Abhängigkeiten von Dienst-zu-Dienst anzuzeigen oder auszublenden, aktivieren oder deaktivieren Sie die Option **Serviceabhängigkeiten anzeigen** im Fenster **Abhängigkeiten anzeigen**. Wenn Sie diese Option deaktivieren, verschwinden die orangen Linien, aber die Dienste sind noch sichtbar.

Die nachstehende Tabelle beschreibt, welche Informationen im Fenster **Abhängigkeiten anzeigen** für die verschiedenen Objektarten dargestellt werden:

Objekt	Fenster "Abhängigkeiten anzeigen"
Knoten	<p>Zeigt alle auf diesem Knoten ausgeführten Dienstprozesse sowie den Status jedes einzelnen Prozesses an. Zeigt Gitter dem Knoten zugewiesene Gitter an. Ferner werden auch alle Sekundärabhängigkeiten dargestellt, d.h. Abhängigkeiten, die nicht direkt zu dem Objekt gehören, dessen Abhängigkeiten angezeigt werden sollen.</p> <p>Zum Beispiel: Ein Modellrepository-Dienst, MRS1, wird auf Knoten1 ausgeführt. Ein Data Integration Service, DIS1, und ein Analyst Service, AT1 beziehen zwar Informationen von MRS1, werden aber auf Knoten2 ausgeführt.</p> <p>Das Fenster Abhängigkeiten anzeigen stellt in diesem Fall folgende Informationen dar:</p> <ul style="list-style-type: none"> - Eine Abhängigkeit zwischen Knoten1 und MRS1. - Eine Sekundärabhängigkeit zwischen Knoten1 und den Diensten DIS1 und AT1. Diese Dienste erscheinen ausgegraut, da es sich um Sekundärabhängigkeiten handelt. <p>Wenn Sie Knoten1 herunterfahren, zeigt das Fenster an, dass MRS1 betroffen ist, aber auch DIS1 und AT1, da sie von MRS1 abhängen.</p>
Dienst	<p>Zeigt alle Auf- und Abwärts-Abhängigkeiten sowie den Knoten an, auf dem der Dienst ausgeführt wird. Eine Aufwärtsabhängigkeit ist ein Dienst, von dem der ausgewählte Dienst abhängt. Eine Abwärtsabhängigkeit ist ein Dienst, der von dem ausgewählten Dienst abhängt.</p> <p>Zum Beispiel: Wenn Sie die Abhängigkeiten für einen Data Integration Service anzeigen, sehen Sie die Aufwärtsabhängigkeit in Form des Modellrepository-Diensts, die Abwärtsabhängigkeit in Form des Analyst Service und den Knoten auf dem der Data Integration Service ausgeführt wird.</p>
Gitter	Zeigt die dem Gitter zugewiesenen Knoten und die auf dem Gitter ausgeführten Anwendungsdienste an.

Objekt	Fenster "Abhängigkeiten anzeigen"
Knoten	Zeigt alle auf diesem Knoten ausgeführten Dienstprozesse sowie den Status jedes einzelnen Prozesses an.
Dienst	Zeigt alle Auf- und Abwärts-Abhängigkeiten sowie den Knoten an, auf dem der Dienst ausgeführt wird.

Objekt	Fenster "Abhängigkeiten anzeigen"
Knoten	Zeigt alle auf diesem Knoten ausgeführten Dienstprozesse sowie den Status jedes einzelnen Prozesses an.
Dienst	Zeigt alle Auf- und Abwärts-Abhängigkeiten sowie den Knoten an, auf dem der Dienst ausgeführt wird.

- Im Fenster **Abhängigkeiten anzeigen** können Sie wahlweise folgende Aktionen durchführen:
 - Um zusätzliche Abhängigkeitsinformationen für ein Objekt darzustellen, setzen Sie den Cursor auf das Objekt.
 - Zur Hervorhebung der Abwärtsabhängigkeiten und zur Anzeige weiterer Prozessdetails für einen Dienst, setzen Sie den Cursor auf den Dienst.
 - Um das Fenster **Abhängigkeiten anzeigen** für ein beliebiges Objekt einzublenden, klicken Sie das Objekt mit der rechten Maustaste an und wählen Sie **Abhängigkeiten anzeigen**.
 Das Fenster **Abhängigkeiten anzeigen** wird aktualisiert und zeigt die Abhängigkeiten für das gewählte Objekt.

Herunterfahren einer Domäne

Um administrative Aufgaben auf einer Domäne ausführen zu können, müssen Sie die Domäne eventuell abschalten.

Beispielsweise müssen Sie zum Sichern und Wiederherstellen einer Domänenkonfiguration zunächst die Domäne herunterfahren. Beim Herunterfahren der Domäne stoppt der Dienstmanager auf dem Master-Gateway-Knoten alle Anwendungsdienste und Informatica-Dienste in der Domäne. Nach dem Herunterfahren der Domäne starten Sie die Informatica-Dienste auf jedem Knoten in der Domäne neu. Unter Windows wird der Prozess „Berichterstellungsdienst“ beim Herunterfahren einer Domäne nicht beendet. Sie müssen den Prozess „Berichterstellungsdienst“ beenden, bevor Sie die Knoten in einer Domäne starten können.

Wenn Sie eine Domäne herunterfahren, werden alle Prozesse abgebrochen, die auf Knoten in der Domäne laufen. Stellen Sie vor dem Herunterfahren einer Domäne sicher, dass alle Prozesse, einschließlich Arbeitsabläufe, abgeschlossen sind und keine Benutzer bei Repositorys in der Domäne angemeldet sind.

Wenn Sie eine Domäne herunterfahren, werden alle Prozesse abgebrochen, die auf dem Knoten in der Domäne ausgeführt werden. Stellen Sie vor dem Herunterfahren einer Domäne sicher, dass alle Prozesse, einschließlich Arbeitsabläufen, abgeschlossen sind und keine Benutzer am Modellrepository-Dienst in der Domäne angemeldet sind.

Hinweis: Um einen möglichen Daten- oder Metadaten-Verlust zu vermeiden, und damit die laufenden Prozesse abgeschlossen werden können, können Sie jeden einzelnen Knoten aus dem Administrator-Tool oder dem Betriebssystem heraus herunterfahren.

1. Klicken Sie auf die Registerkarte **Domäne**.
2. Wählen Sie die Domäne im Navigator aus.
3. Klicken Sie auf der Registerkarte **Domäne** auf **Aktionen > Domäne herunterfahren**.
Im Dialogfeld **Herunterfahren** werden die in der Domäne ausgeführten Prozesse aufgelistet.
4. Klicken Sie auf **Ja**.
Das Dialogfeld **Herunterfahren** zeigt eine Warnmeldung an.
5. Klicken Sie auf **Ja**.
Der Dienstmanager auf dem Master-Gateway-Knoten fährt alle Anwendungsdienste und Informatica-Dienste auf jedem Knoten in der Domäne herunter.
6. Um die Domäne neu zu starten, starten Sie die Informatica-Dienste auf den Gateway- und Worker-Knoten in der Domäne neu.
7. Zum Neustart der Domäne starten Sie die Informatica-Dienste neu.

Domäneneigenschaften

Auf der Registerkarte **Domäne** können Sie Domäneneigenschaften einschließlich Datenbankeigenschaften, Gateway-Konfiguration und Dienstebenen konfigurieren.

Klicken Sie auf die Registerkarte **Domäne**, um Eigenschaften anzuzeigen und zu bearbeiten. Wählen Sie im Navigator eine Domäne aus. Dann klicken Sie auf **Eigenschaften**, um die Inhaltsangabe einzublenden. In der Inhaltsübersicht stehen die Domäneneigenschaften.

Sie können die Eigenschaften konfigurieren, wenn Sie die Domäne ändern möchten. So können Sie zum Beispiel die Datenbankeigenschaften, die SMTP-Eigenschaften für Warnmeldungen und die Domänenbelastungs-Eigenschaften ändern.

Außerdem können Sie die Domäne auf höchster Ebene überwachen. In der Ansicht **Dienste und Knoten** können Sie den Status der in der Domäne definierten Anwendungsdienste und Knoten anzeigen.

Außerdem können Sie die Domäne auf höchster Ebene überwachen. In der Ansicht **Dienste und Knoten** können Sie die Statusangaben der Anwendungsdienste und des Knotens in der Domäne anzeigen.

Außerdem können Sie die Domäne auf höchster Ebene überwachen. In der Ansicht **Dienste und Knoten** können Sie die Statusangaben der Anwendungsdienste und des Knotens in der Domäne anzeigen.

Sie können die folgenden Domäneneigenschaften konfigurieren:

- Allgemeine Eigenschaften. Bearbeiten der allgemeinen Eigenschaften wie Dienstbelastbarkeit und Dispatch-Modus.
- Datenbankeigenschaften. Anzeigen der Datenbankeigenschaften wie Datenbankname und Datenbank-Host.
- Datenbankeigenschaften. Anzeigen der Datenbankeigenschaften wie Datenbankname und Datenbank-Host.
- Gateway-Konfiguration. Konfigurieren eines Knotens als Gateway und Angeben des Speicherorts zum Schreiben von Protokollereignissen.
- Gateway-Konfiguration. Konfigurieren eines Knotens als Gateway und Angeben des Speicherorts zum Schreiben von Protokollereignissen.
- Dienstebenenverwaltung. Dienstebenen erstellen und konfigurieren.
- Dienstebenenverwaltung. Dienstebenen erstellen und konfigurieren.
- SMTP-Konfiguration. Bearbeiten der SMTP-Einstellungen für den Ausgangs-Mailserver zum Aktivieren der Warnmeldungen.
- Benutzerdefinierte Eigenschaften. Bearbeiten der für die Informatica-Umgebung einmaligen oder nur in Sonderfällen zutreffenden benutzerdefinierten Eigenschaften. Beim Erstellen einer Domäne hat diese keine benutzerdefinierten Eigenschaften. Benutzerdefinierte Eigenschaften dürfen Sie nur nach Anweisung des globalen Kundensupports von Informatica verwenden.

Allgemeine Eigenschaften

Im Bereich "Allgemeine Eigenschaften" können Sie allgemeine Eigenschaften für die Domäne konfigurieren.

Klicken Sie zum Bearbeiten der allgemeinen Eigenschaften auf **Bearbeiten**.

Die folgende Tabelle beschreibt die Eigenschaften, die im Bereich Allgemeine Eigenschaften bearbeitet werden können:

Eigenschaft	Beschreibung
Name	Schreibgeschützt. Der Name der Domäne.
Resistenz-Timeout	Maximale Anzahl von Sekunden, in denen ein Anwendungsdienst versucht, eine Verbindung oder eine erneute Verbindung zum PowerCenter-Repository-Dienst oder zum PowerCenter-Integrationsdienst herzustellen. Die gültigen Werte liegen im Bereich zwischen 0 und 1000000. Voreingestellt ist 30 Sekunden.
Grenzwert für Resistenz-Timeout	Maximale Anzahl von Sekunden, in denen die Anwendungs-Clients oder Anwendungsdienste versuchen können, eine Verbindung oder eine erneute Verbindung zum PowerCenter-Repository-Dienst oder zum PowerCenter-Integrationsdienst herzustellen. Voreingestellt ist 180 Sekunden.

Eigenschaft	Beschreibung
Neustartzeitraum	Maximale Zeit in Sekunden, in denen die Domäne versucht, einen Anwendungsdienstprozess neu zu starten. Die gültigen Werte liegen im Bereich zwischen 0 und 1000000.
Maximale Anzahl Neustartversuche innerhalb des Neustartzeitraums	Gibt an, wie oft die Domäne versucht, einen Anwendungsdienstprozess neu zu starten. Gültige Werte sind 0 bis 1000. Wenn Sie den Wert auf 0 festlegen, versucht die Domäne nicht, den Dienstprozess neu zu starten.
Sendemodus	<p>Der Modus, den der Load Balancer verwendet, um PowerCenter Integration Service-Aufgaben auf Knoten in einem Gitter zu verteilen. Wählen Sie einen der folgenden Dispatch-Modi aus:</p> <ul style="list-style-type: none"> - MetricBased - RoundRobin - Adaptiv <p>Der Modus, den der Load Balancer verwendet, um Ultra Messaging-Dienstaufgaben auf Knoten in einem Gitter zu verteilen. Wählen Sie einen der folgenden Dispatch-Modi aus:</p> <ul style="list-style-type: none"> - MetricBased - RoundRobin - Adaptiv <p>Diese Eigenschaft gilt nicht für PowerCenter Express.</p>
Sichere Kommunikation aktivieren	<p>Konfiguriert Dienste zur Verwendung des TLS-Protokolls, um Daten sicher innerhalb der Domäne zu übertragen. Durch das Aktivieren sicherer Kommunikation für die Domäne verwenden Dienste sichere Verbindungen zur Kommunikation mit anderen Informatica-Anwendungsdiensten und -Clients.</p> <p>Stellen Sie sicher, dass alle Domänenknoten verfügbar sind, bevor Sie die sichere Kommunikation für die Domäne aktivieren. Wenn ein Knoten nicht verfügbar ist, können Änderungen der sicheren Kommunikation nicht auf den Dienstmanager des Knotens angewendet werden. Um die Änderungen zu übernehmen, müssen Sie die Domäne neu starten. Setzen Sie diese Eigenschaft auf True oder False.</p>
Dienstresistenz-Timeout	Die maximale Anzahl von Sekunden, die Anwendungs-Clients und Anwendungsdienste versuchen können, eine Verbindung zum Datenintegrationsdienst oder dem Modellrepository-Dienst aufzubauen. Der Standardwert ist 180 Sekunden.

Datenbankeigenschaften

Im Bereich Datenbankeigenschaften können Sie die Datenbankeigenschaften für die Domäne anzeigen oder bearbeiten, z.B. den Namen und Host der Datenbank.

Die nachstehende Tabelle beschreibt die Eigenschaften, die sich im Bereich Datenbankeigenschaften bearbeiten lassen:

Eigenschaft	Beschreibung
Datenbanktyp	Datenbanktyp, der die Metadaten der Domänenkonfiguration speichert
Datenbankhost	Name des Computers, der die Datenbank hostet
Datenbankport	Die von der Datenbank verwendete Portnummer
Datenbankname	Der Name der Datenbank

Eigenschaft	Beschreibung
Datenbankbenutzer	Benutzerkonto für die Datenbank, die die Informationen der Domänenkonfiguration enthält
Datenbank-TLS aktiviert	Gibt an, ob es sich bei der Datenbank für das Domänenkonfigurations-Repository um eine sichere Datenbank handelt. TRUE, wenn die Domänenkonfigurations-Repository-Datenbank sicher ist. Sie können ein sicheres Domänenkonfigurations-Repository verwenden, wenn die sichere Kommunikation für die Informatica-Domäne aktiviert ist.

Hinweis: Der Dienstmanager verwendet die DataDirect-Treiber, die in der Installation von Informatica enthalten sind. Informatica bietet keine Unterstützung für die Verwendung von anderen Datenbanktreibern.

Gateway-Konfigurationseigenschaften

Im Bereich für die Gateway-Konfigurationseigenschaften können Sie einen Knoten als Gateway für eine Domäne konfigurieren und das Verzeichnis angeben, in das der Dienstmanager dieses Knotens die Protokollereignisdateien schreibt.

Beim Bearbeiten von Gateway-Konfigurationseigenschaften werden keine früheren Protokolle eingeblendet. Außerdem gelten die geänderten Eigenschaften nur für Neustart- und Failover-Szenarien.

Klicken Sie zum Bearbeiten der Gateway-Konfigurationseigenschaften auf **Bearbeiten**.

Um Gateway-Konfigurationseigenschaften zu sortieren, klicken Sie auf die Spaltenüberschrift, nach der Sie sortieren möchten.

Die folgende Tabelle beschreibt die Eigenschaften, die Sie im Bereich für die Gateway-Konfigurationseigenschaften bearbeiten können:

Eigenschaft	Beschreibung
Knotenname	Schreibgeschützt. Der Name des Knotens
Status	Der Status des Knotens
Gateway	Wählen Sie diese Option, um den Knoten als Gateway zu konfigurieren. Wenn die Domäne eine sichere Domänen-Konfigurationsdatenbank verwendet, müssen Sie die Truststore-Datei und das Passwort für die Datenbank angeben. Um den Knoten als Worker-Knoten zu konfigurieren, löschen Sie diese Option.
Protokollverzeichnispfad	Der Verzeichnispfad für die Protokollereignisdateien. Kann der Protokollmanager nicht in den Verzeichnispfad schreiben, schreibt er Protokollereignisse in die Datei node.log auf dem Master-Gateway-Knoten.

Sicheres Domänenkonfigurations-Repository

Wenn Sie einen Knoten als Gateway-Knoten konfigurieren und die Domäne eine sichere Domänen-Konfigurationsdatenbank verwendet, müssen Sie die Truststore-Datei und das Passwort für die sichere Datenbank angeben.

Wenn Sie mehrere Gateway-Knoten für die Domäne konfigurieren, legen Sie die Datenbank-Truststore-Datei und das Passwort für alle Gateway-Knoten fest.

In der folgenden Tabelle werden die Datenbankeneigenschaften beschrieben:

Eigenschaft	Beschreibung
Datenbank-Truststore-Passwort	Passwort für die Truststore-Datei
Datenbank-Truststore-Speicherort	Pfad und Dateiname der Truststore-Datei für die sichere Datenbank.

Hinweis: Damit Sie eine sichere Domänenkonfigurations-Repository-Datenbank verwenden können, muss die Option „Sichere Kommunikation“ für die Domäne aktiviert sein.

Dienstebenenverwaltung

Im Bereich Dienstebenenverwaltung können Sie Dienstebenen anzeigen, hinzufügen und bearbeiten.

Dienstebenen legen die Priorität unter den Tasks fest, die darauf warten, versendet zu werden. Wenn der Load Balancer mehr Aufgaben zu versenden hat als der der PowerCenter Integration Service gleichzeitig ausführen kann, stellt der Load Balancer diese Aufgaben in die Dispatch-Warteschlange. Wenn mehrere Tasks in der Dispatch-Warteschlange stehen, bestimmt der Load Balancer anhand der Dienstebenen die Reihenfolge, in der die Tasks aus der Warteschlange verteilt werden.

Da es sich bei den Dienstebenen um Domäneneigenschaften handelt, können Sie für all Repositories in einer Domäne die gleichen Dienstebenen verwenden. Sie erstellen und bearbeiten Dienstebenen in den Domäneneigenschaften der Domäne oder mithilfe von `infacmd`.

Sie können die Standard-Dienstebene bearbeiten, aber nicht löschen. Diese Standard-Dienstebene hat eine Dispatch-Priorität von 5 und eine maximale Dispatch-Wartezeit von 1800 Sekunden.

Um eine Dienstebene hinzuzufügen, klicken Sie auf **Hinzufügen**.

Um eine Dienstebene zu bearbeiten, klicken Sie auf den Link für die Dienstebene.

Um eine Dienstebene zu löschen, wählen Sie die Dienstebene aus und klicken auf die Schaltfläche Löschen.

Die folgende Tabelle beschreibt die Eigenschaften, die Sie im Bereich Dienstebenenverwaltung bearbeiten können:

Eigenschaft	Beschreibung
Name	<p>Der Name der Dienstebene. Beim Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden, und er muss in der Domäne eindeutig sein. Er darf nicht länger als 128 Zeichen sein oder mit @ beginnen. Er darf auch keine Leerzeichen oder die folgenden Sonderzeichen enthalten:</p> <p><code>` ~ % ^ * + = { } \ ; : / ? . < > ! ()] [</code></p> <p>Nachdem Sie eine Dienstebene hinzugefügt haben, können Sie ihren Namen nicht mehr ändern.</p>
Dispatch-Priorität	<p>Eine Zahl, die die Dispatch-Priorität für die Dienstebene festlegt. Der Load Balancer versendet zuerst Tasks mit einer hohen Priorität, dann Tasks mit niedriger Priorität. Die Dispatch-Priorität 1 ist die höchste Priorität. Gültige Werte sind 1 bis 10. Der Standard ist 5.</p>
Maximale Dispatch-Wartezeit (Sekunden)	<p>Die Zeit in Sekunden, die der Load Balancer wartet, bevor er die Dispatch-Priorität für eine Task auf die höchsten Priorität ändert. Diese Eigenschaft sorgt dafür, dass keine Task für immer in der Dispatch-Warteschlange wartet. Gültige Werte sind 1 bis 86400. Standard ist 1800.</p>

SMTP-Konfiguration

Mithilfe der SMTP-Konfigurationseigenschaften können Sie SMTP-Einstellungen für die Domäne konfigurieren. Der ausgehende Mailserver verwendet die SMTP-Einstellungen zum Versenden von Alarmen und Scorecard-Benachrichtigungen.

Die nachstehende Tabelle beschreibt die Eigenschaften, die sich im Bereich Datenbankeigenschaften bearbeiten lassen:

Eigenschaft	Beschreibung
Hostname	Hostname für ausgehenden SMTP-Mailserver. Geben Sie zum Beispiel den Microsoft Exchange-Server für Microsoft Outlook ein.
Port	Vom ausgehenden Mailserver verwendeter Port. Die gültigen Werte liegen zwischen 1 und 65535. Standardwert ist 25.
Benutzername	Benutzername für die Authentifizierung beim Senden, wenn dies vom ausgehenden Mailserver gefordert wird.
Passwort	Benutzerpasswort für die Authentifizierung beim Senden, wenn dies vom ausgehenden Mailserver gefordert wird.
E-Mail-Adresse des Absenders	E-Mail-Adresse, die der Dienstmanager im Feld „Von“ beim Senden von Benachrichtigungs-E-Mails verwendet. Wenn Sie dieses Feld leer lassen, verwendet der Dienstmanager Administrator@<Hostname> als Absender.

Benutzerdefinierte Eigenschaften für die Domäne

Konfigurieren Sie benutzerdefinierte Eigenschaften, die für bestimmte Umgebungen eindeutig sind.

In speziellen Fällen ist die Anwendung von benutzerdefinierten Eigenschaften erforderlich. Wenn Sie eine benutzerdefinierte Eigenschaft definieren, geben Sie den Eigenschaftennamen und einen Anfangswert ein. Definieren Sie die benutzerdefinierten Eigenschaften nur auf Anforderung des globalen Kundensupports von Informatica.

KAPITEL 5

Hohe Verfügbarkeit

Dieses Kapitel umfasst die folgenden Themen:

- [Hohe Verfügbarkeit - Übersicht, 87](#)
- [Belastbarkeit, 88](#)
- [Neustart und Failover, 91](#)
- [Wiederherstellung, 92](#)
- [Konfiguration für einen hochverfügbare Domäne, 93](#)
- [Netzwerk, hohe Verfügbarkeit, 97](#)

Hohe Verfügbarkeit - Übersicht

Hohe Verfügbarkeit bedeutet unterbrechungslose Verfügbarkeit der Computersystemressourcen. In einer Informatica-Domäne eliminiert Hochverfügbarkeit einen einzelnen Fehlerpunkt und gewährleistet im Fehlerfall die Minimierung der Dienstunterbrechungen. Wenn Sie hohe Verfügbarkeit für eine Domäne konfigurieren, kann die Domäne auch bei vorübergehendem Netzwerk-, Hardware- oder Dienstaussfall weiter ausgeführt werden.

Durch folgende Hochverfügbarkeitskomponenten werden Dienste in einer Informatica-Domäne hoch verfügbar:

- **Belastbarkeit.** Eine Informatica-Domäne kann temporäre Verbindungsfehler so lange tolerieren, bis entweder das Belastbarkeits-Timeout abläuft oder der Fehler behoben wurde.
- **Neustart und Failover.** Ein Prozess kann auf demselben Knoten oder auf einen Backup-Knoten erneut starten, nachdem der Prozess nicht mehr verfügbar ist.
- **Wiederherstellung.** Operationen können nach einer Dienstunterbrechung abgeschlossen werden. Nach Neustart oder Failover eines Dienstprozesses werden Dienststatus und Operationen wieder hergestellt.

Wenn Sie eine hoch verfügbare Informatica-Umgebung planen, konfigurieren Sie hohe Verfügbarkeit für die internen Informatica-Komponenten und für externe Informatica-Systeme. Interne Komponenten umfassen die Domäne, Anwendungsdienste, Anwendungs-Clients und Befehlszeilenprogramme. Externe Systeme sind Netzwerk, Hardware, Datenbankverwaltungssysteme, FTP-Server, Meldungswarteschlangen und gemeinsame Speicher.

Funktionen für die Hochverfügbarkeit für die Informatica-Umgebung stehen Ihnen basierend auf Ihrer Lizenz zur Verfügung.

Beispiel

Wenn Sie ein Mapping im PowerCenter Designer-Arbeitsbereich öffnen, ist der PowerCenter-Repository-Dienst nicht mehr verfügbar und die Anfrage schlägt fehl. Die Domäne enthält mehrere Knoten für Failover und der PowerCenter Designer ist gegenüber temporären Ausfällen belastbar.

Der PowerCenter Designer versucht, innerhalb des Belastbarkeits-Timeouts eine Verbindung zum PowerCenter-Repository-Dienst herzustellen. Der PowerCenter-Repository-Dienst führt ein Failover zu einem anderen Knoten durch, weil er nicht auf demselben Knoten starten kann.

Der PowerCenter-Repository-Dienst startet innerhalb des Belastbarkeits-Timeout-Zeitraums und der PowerCenter Designer stellt die Verbindung wieder her.

Nachdem der PowerCenter Designer die Verbindung wiederhergestellt hat, erholt sich der PowerCenter-Repository-Dienst von der fehlgeschlagenen Operation und holt das Mapping in den PowerCenter Designer Workspace.

Belastbarkeit

Die Domäne toleriert temporäre Verbindungsfehler zwischen Anwendungs-Clients, Anwendungsdiensten und Knoten.

Ein temporärer Verbindungsfehler kann auftreten, weil ein Anwendungsdienstprozess fehlschlägt oder ein Netzwerkfehler auftritt. Wenn ein temporärer Verbindungsfehler auftritt, versucht der Dienstmanager, die Verbindungen zwischen den Anwendungs-Clients, Anwendungsdiensten und Knoten wiederherzustellen.

Belastbarkeit der Anwendungs-Clients

Die Anwendungs-Clients versuchen, eine erneute Verbindung zu Anwendungsdiensten herzustellen, wenn ein temporärer Verbindungsfehler auftritt.

Basierend auf Ihrer Lizenz sind die folgenden Anwendungs-Clients belastbar in Bezug auf die Dienste, mit denen sie verbunden sind.

PowerCenter Client

Der PowerCenter Client versucht, eine erneute Verbindung zum PowerCenter-Repository-Dienst und zum PowerCenter-Integrationsdienst herzustellen, wenn ein temporärer Netzwerkfehler auftritt.

Wenn Sie eine PowerCenter Client-Aktion durchführen, die eine Verbindung zum Repository benötigt, während der PowerCenter Client versucht, die Verbindung wiederherzustellen, fordert Sie der PowerCenter Client auf, den Vorgang noch einmal zu versuchen, nachdem der PowerCenter Client die Verbindung wieder hergestellt hat. Wenn der PowerCenter Client nicht in der Lage ist, die Verbindung während des Belastbarkeits-Timeout-Zeitraums wieder herzustellen, fordert der PowerCenter Client Sie auf, sich manuell mit dem Repository zu verbinden.

Befehlszeilenprogramme

Befehlszeilenprogramme versuchen, eine erneute Verbindung zur Domäne oder zu einem Anwendungsdienst herzustellen, wenn beim Ausführen eines Befehlszeilenprogramms ein temporärer Netzwerkfehler auftritt.

Beispiel: Belastbarkeit von PowerCenter Clients in Bezug auf Anwendungsdienste

Beim Überwachen eines Arbeitsablaufs durch einen Entwickler tritt zwischen dem PowerCenter-Arbeitsablauf-Monitor und dem PowerCenter-Repository-Dienst ein Netzwerkverbindungsverlust von 120 Sekunden auf. Der PowerCenter Client und der Arbeitsablauf-Monitor haben ein Belastbarkeits-Timeout von 60 Sekunden und der PowerCenter-Repository-Dienst hat ein Belastbarkeits-Timeout von 180 Sekunden.

Der Entwickler bemerkt den Verbindungsverlust von 120 Sekunden nicht. Auf der Registerkarte **Benachrichtigungen** im PowerCenter-Arbeitsablauf-Monitor wird jedoch die folgende Meldung angezeigt:

```
Repository Service notifications are enabled.  
DATE TIME-[REP_55101] Connection to the Repository Service [Repository_Service_Name] is  
broken.  
DATE TIME-[REP_55114] Reconnecting to the Repository Service [Repository_Service_Name].  
The resilience time is 180 seconds.  
DATE TIME-Reconnected to Repository Service [Repository_Service_Name] successfully.
```

Anwendungsdienst-Belastbarkeit

Einige Anwendungsdienste versuchen, eine erneute Verbindung zu Anwendungsdiensten, Anwendungs-Clients und externen Komponenten herzustellen, wenn ein temporärer Verbindungsfehler auftritt.

Basierend auf Ihrer Lizenz sind die folgenden Anwendungsdienste in Bezug auf temporäre Verbindungsfehler ihrer Clients belastbar:

PowerCenter-Integrationsdienst

Der PowerCenter-Integrationsdienst ist in Bezug auf Fehler bei temporären Verbindungen zu anderen Diensten, dem PowerCenter Client und externen Komponenten wie Datenbanken und FTP-Server belastbar.

PowerCenter-Repository-Dienst

Der PowerCenter-Repository-Dienst ist in Bezug auf Fehler bei temporären Verbindungen zu anderen Diensten, wie zum Beispiel dem PowerCenter-Integrationsdienst, belastbar. Er ist auch bei Fehlern bei temporären Verbindungen zur Repository-Datenbank belastbar.

Knoten-Belastbarkeit

Sie können mehrere Knoten in einer Domäne konfigurieren. Jeder Knoten in der Domäne sendet ein Kommunikationssignal zum Master-Gateway-Knoten. Der Master-Gateway-Knoten ist belastbar gegenüber temporären Kommunikationsfehlern aus den Knoten in der Domäne.

Jeder Knoten in der Domäne sendet ein Kommunikationssignal an den Master-Gateway-Knoten in regelmäßigen Abständen von 15 Sekunden. Die Kommunikation enthält eine Liste von Diensten, die auf dem Knoten ausgeführt werden.

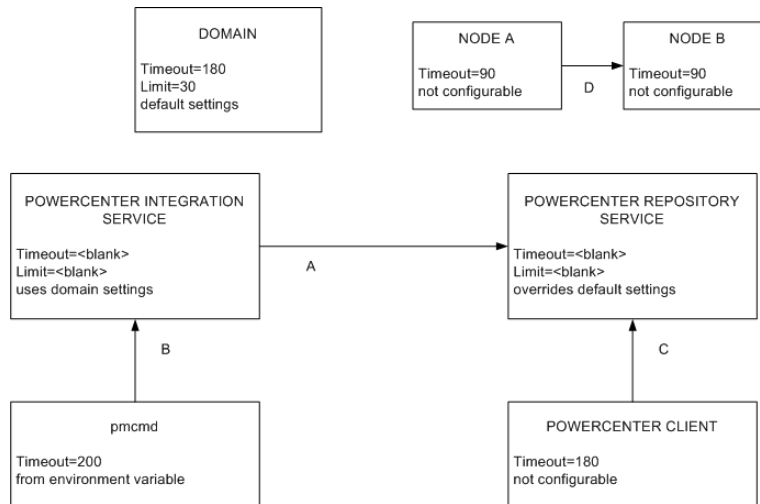
Der Master-Gateway-Knoten weist ein Belastbarkeits-Timeout von 90 Sekunden auf. Wenn die Verbindung von einem Knoten zum Master-Gateway-Knoten innerhalb des Belastbarkeits-Timeouts fehlschlägt, markiert der Master-Gateway-Knoten den Knoten als nicht verfügbar und weist die Dienste einem Backup-Knoten erneut zu. Damit wird gewährleistet, dass Dienste auf einem Knoten unabhängig von Knotenfehlern weiterhin ausgeführt werden.

Beispielkonfiguration für ein Belastbarkeits-Timeout

Bei einigen Belastbarkeits-Timeout-Werten handelt es sich um Standardwerte, andere wiederum können konfiguriert oder überschrieben werden.

Verwenden Sie das für die Domäne für PowerCenter-Anwendungsdienste konfigurierte Belastbarkeits-Timeout und den Grenzwert für das Belastbarkeits-Timeout, wenn Sie diesen nicht den Anwendungsdienst festgelegt haben. Befehlszeilenprogramme verwenden Sie das Dienstbelastbarkeits-Timeout. Ist der Dienstgrenzwert für das Belastbarkeits-Timeout niedriger als das Belastbarkeits-Timeout für den Client, der die Verbindung herstellt, nutzt der Client den Dienstgrenzwert als Belastbarkeits-Timeout.

In der folgenden Abbildung werden einige Beispiele für Verbindungen und Belastbarkeitskonfigurationen in einer Domäne mit PowerCenter-Anwendungsdiensten angezeigt:



Die folgende Tabelle beschreibt das Belastbarkeits-Timeout und die Grenzwerte aus der obigen Abbildung:

	Verbindung von	Verbindung mit	Beschreibung
A	PowerCenter-Integrationsdienst	PowerCenter-Repository-Dienst	Der PowerCenter-Integrationsdienst kann basierend auf dem Belastbarkeits-Timeout der Domäne maximal 30 Sekunden lang versuchen, eine Verbindung zum PowerCenter-Repository-Dienst herzustellen. Er ist nicht an den Grenzwert des PowerCenter-Repository-Diensts für das Belastbarkeits-Timeout von 60 Sekunden gebunden.
B	<i>pmcmd</i>	PowerCenter-Integrationsdienst	<i>pmcmd</i> ist an den Grenzwert des PowerCenter-Integrationsdiensts für das Belastbarkeits-Timeout von 180 Sekunden gebunden und kann das in <i>INFA_CLIENT_RESILIENCE_TIMEOUT</i> konfigurierte Belastbarkeits-Timeout von 200 Sekunden nicht nutzen.
C	PowerCenter Client	PowerCenter-Repository-Dienst	Der PowerCenter Client ist an den Grenzwert des PowerCenter-Repository-Diensts für ein Belastbarkeits-Timeout von 60 Sekunden gebunden. Das voreingestellte Belastbarkeits-Timeout von 180 Sekunden steht ihm nicht zur Verfügung.
D	Knoten A	Knoten B	Knoten A kann maximal 90 Sekunden lang versuchen, eine Verbindung zu Knoten B herzustellen. Der Dienstmanager auf Knoten A und Knoten B verwendet das standardmäßige Knoten Belastbarkeits-Timeout von 90 Sekunden.

Neustart und Failover

Um die Betriebszeit im Fehlerfall zu maximieren, kann die Informatica-Domäne den Neustart oder Failover über einen anderen Knoten ausführen.

Der Dienstmanager auf dem Master-Gateway-Knoten akzeptiert Anfragen des Anwendungsdienstes und verwaltet die Domäne. Wenn kein Master-Gateway-Knoten verfügbar ist, wird die Domäne heruntergefahren. Um die Domäne für den Failover auf einen anderen Knoten zu konfigurieren, müssen Sie mehrere Gateway-Knoten konfigurieren.

Je nach Lizenz können Sie auch Backup-Knoten für Anwendungsdienste konfigurieren. Der Dienstmanager kann im Fehlerfall einen Neustart oder ein Failover für die folgenden Anwendungsdienste ausführen:

- Datenintegrationsdienst
- Modellrepository-Dienst
- PowerCenter-Integrationsdienst
- PowerCenter-Repository-Dienst
- PowerExchange-Listenerdienst
- PowerExchange-Protokollierungsdienst

Domänen-Failover

Der Dienstmanager auf dem Master-Gateway-Knoten nimmt Dienstanfragen entgegen und verwaltet die Domäne und die Dienste in der Domäne. Die Domäne kann ein Failover auf einen anderen Knoten durchführen, wenn die Domäne über mehrere Gateway-Knoten verfügt. Konfigurieren Sie mehrere Gateway-Knoten, um zu verhindern, dass die Domäne heruntergefahren wird, wenn der Master-Gateway-Knoten nicht verfügbar ist.

Der Master-Gateway-Knoten unterhält eine Verbindung zum Repository für die Domänenkonfiguration. Wenn das Domänenkonfigurations-Repository nicht mehr verfügbar ist, versucht der Master-Gateway-Knoten sich erneut zu verbinden, wenn ein Benutzer einen Vorgang durchführt. Wenn der Master-Gateway-Knoten keine Verbindung zum Domänenkonfigurations-Repository aufbauen kann, wird der Master-Gateway-Knoten möglicherweise heruntergefahren.

Wenn die Domäne über mehrere Gateway-Knoten verfügt und der Master-Gateway-Knoten nicht verfügbar ist, wählt der Dienstmanager auf den anderen Gateway-Knoten andere Master-Gateway-Knoten aus, um die Dienstanfragen zu akzeptieren. Die Domäne versucht bei jedem Gateway-Knoten, eine Verbindung zum Domänenkonfigurations-Repository herzustellen. Wenn keiner der Gateway-Knoten eine Verbindung herstellen kann, fährt die Domäne herunter und alle Domänenvorgänge schlagen fehl. Bei Failover des Master-Gateway rufen die Client-Tools Informationen über die alternativen Domänen-Gateways aus der Datei domains.infa ab.

Hinweis: Für Anwendungsdienste, die auf dem Master-Gateway-Knoten ausgeführt werden, findet kein Failover statt, wenn ein anderer Master-Gateway-Knoten ausgewählt ist. Dies trifft nicht zu, wenn für den Anwendungsdienst ein Backup-Knoten konfiguriert ist.

Anwendungsdienst - Neustart und Failover

Wenn ein Anwendungsdienstprozess nicht mehr verfügbar ist, kann der Dienstmanager den Anwendungsdienst neu starten oder ein Failover auf einen Backup-Knoten durchführen. Wenn der

Dienstmanager ein Failover für einen Anwendungsdienst durchführt, startet er den Dienst auf einem anderen Knoten, für den der Dienst zur Ausführung konfiguriert ist.

Die folgenden Situationen beschreiben, wie der Dienstmanager einen Anwendungsdienst neu startet oder wie er für diesen ein Failover durchführt:

- Wenn der primäre Knoten, auf dem der Dienstprozess ausgeführt wird, nicht verfügbar wird, wechselt der Dienst auf einen Backup-Knoten. Der primäre Knoten kann möglicherweise nicht verfügbar sein, wenn er abgeschaltet wird oder die Verbindung zum Knoten nicht mehr verfügbar ist.
- Wenn der primäre Knoten, auf dem der Dienstprozess ausgeführt wird, verfügbar ist, versucht die Domäne, den Prozess gemäß den in den Domäneneigenschaften konfigurierten Neustart-Optionen neu zu starten. Wenn der Prozess nicht neu gestartet wird, kann der Dienstmanager den Prozess als fehlgeschlagen kennzeichnen. Der Dienst wechselt dann auf einen Backup-Knoten und startet einen anderen Prozess. Wenn der Dienstmanager den Prozess als fehlgeschlagen kennzeichnet, muss der Administrator den Prozess nach Behebung möglicher Konfigurationsprobleme aktivieren.

Beim Failover eines Dienstprozesses auf einen Backup-Knoten wechselt er nicht zurück auf den primären Knoten, wenn dieser wieder verfügbar wird. Sie können den Dienstprozess auf dem Backup-Knoten deaktivieren, damit er wieder auf den primären Knoten wechselt.

Wiederherstellung

Bei der Wiederherstellung handelt es sich um den Abschluss von Operationen, nachdem ein unterbrochener Dienst wiederhergestellt wurde. Der Betriebsstatus eines Dienstes enthält Informationen über den Dienstprozess.

Je nach Lizenz können die folgenden Komponenten wiederhergestellt werden, nachdem ein unterbrochener Dienst wieder hergestellt wurde:

Dienstmanager

Der Dienstmanager für jeden Knoten in der Domäne pflegt den Status der auf dem jeweiligen Knoten ausgeführten Dienstprozesse. Wenn das Master-Gateway heruntergefahren wird, erfasst das neu gewählte Master-Gateway die Zustandsinformationen jedes Knotens, um den Zustand der Domäne wiederherzustellen.

PowerCenter-Repository-Dienst

Der PowerCenter-Repository-Dienst pflegt den Betriebsstatus im Repository. Der Betriebsstatus enthält Informationen zu Repository-Sperren, laufenden Anfragen und verbundenen Clients. Nach einem Neustart oder Failover kann der PowerCenter-Repository-Dienst den Betriebsstatus ab dem Zeitpunkt der Unterbrechung wiederherstellen.

PowerCenter-Integrationsdienst

Der PowerCenter-Integrationsdienst pflegt den Betriebsstatus im gemeinsam genutzten Speicher, der für den Dienst konfiguriert ist. Der Betriebsstatus enthält Informationen über geplante, laufende und abgeschlossene Aufgaben für den Dienst.

Der PowerCenter-Integrationsdienst pflegt den Betriebszustand von PowerCenter-Sitzungen und Arbeitsabläufen auf der Basis der Wiederherstellungsstrategie, die Sie für die Sitzung und den Arbeitsablauf konfigurieren. Wenn der PowerCenter-Integrationsdienst neu gestartet wird oder einen Failover für einen Dienstprozess ausführt, werden jene unterbrochenen Arbeitsabläufe automatisch wiederhergestellt, die für eine Wiederherstellung konfiguriert wurden.

Datenintegrationsdienst

Der Datenintegrationsdienst pflegt den Betriebsstatus im Modellrepository. Der Betriebsstatus enthält den Status des Arbeitsablaufs und der Aufgaben im Arbeitsablauf sowie die Werte der Arbeitsablaufvariablen und -parameter während der unterbrochenen Arbeitsablaufinstanz.

Wenn ein Datenintegrationsdienst einen Neustart oder Failover eines Dienstprozesses ausführt, können Sie unterbrochene Arbeitsabläufe, die für die Wiederherstellung des Arbeitsablaufs aktiviert sind, manuell neustarten. Sie können auch die automatische Wiederherstellung von Arbeitsablaufinstanzen konfigurieren, die aufgrund eines unerwarteten Herunterfahrens des Datenintegrationsdienstprozesses abgebrochen wurden.

Konfiguration für einen hochverfügbare Domäne

Um die Systemausfallzeit zu minimieren, konfigurieren Sie Hochverfügbarkeit für die Informatica-Domänenkomponenten.

Sie können die folgenden Informatica-Domänenkomponenten als hoch verfügbar konfigurieren:

Domäne

Ein Knoten in der Domäne fungiert als Gateway für Dienstanforderungen von Clients und leitet sie an den entsprechenden Dienst und Knoten weiter. Um zu verhindern, dass die Domäne herunterfährt, wenn der Master-Gateway-Knoten nicht verfügbar ist, konfigurieren Sie mehr als einen Gateway-Knoten.

Knoten

Informatica-Dienste sind Prozesse, die auf jedem Knoten ausgeführt werden. Konfigurieren Sie Informatica-Dienste so, dass sie automatisch neu gestartet werden, wenn sie unerwartet beendet werden.

Anwendungsdienste

Die Anwendungsdienste werden auf Knoten in der Informatica-Domäne ausgeführt.

Basierend auf Ihrer Lizenz können Sie die folgenden Hochverfügbarkeitsfunktionen für Anwendungsdienste konfigurieren:

- Um die Ausfallzeit von Anwendungsdiensten zu minimieren, konfigurieren Sie Sicherungsknoten für Anwendungsdienste.
- Um den Belastbarkeitszeitraum für Anwendungsdienste anzugeben, überprüfen Sie die Einstellungen und konfigurieren Sie Zeiträume für das Belastbarkeits-Timeout für Anwendungsdienste.
- Um Failover und Wiederherstellung für den PowerCenter-Integrationsdienst sicherzustellen, konfigurieren Sie den PowerCenter-Integrationsdienst zum Speichern der Prozess-Statusinformationen in einem POSIX-kompatiblen gemeinsam genutzten Dateisystem oder in einer Datenbank.

Anwendungs-Clients

Anwendungs-Clients bieten Zugriff auf Informatica-Funktionen und werden auf Benutzercomputern ausgeführt. Anwendungs-Clients senden Anfragen an den Dienstmanager oder an Anwendungsdienste.

Sie können Zeiträume für das Belastbarkeits-Timeout für Befehlszeilenprogramme konfigurieren. Sie können kein Belastbarkeits-Timeout für PowerCenter Clients konfigurieren.

Externe Systeme

Verwenden Sie hoch verfügbare Versionen von externen Systemen, wie zum Beispiel Quell- und Zieldatenbanken, Meldungswarteschlangen und FTP-Server.

Netzwerk

Sorgen Sie für eine hohe Verfügbarkeit des Netzwerkes, indem Sie redundante Komponenten wie Router, Kabel und Netzwerkadapterkarten konfigurieren.

Konfiguration der Belastbarkeit für Anwendungsdienste

Wenn ein temporärer Netzwerkfehler auftritt, versuchen Anwendungsdienste, eine erneute Verbindung zu anderen Anwendungsdiensten für die Dauer des Belastbarkeits-Timeouts herzustellen. Sie können das Belastbarkeits-Timeout für Anwendungsdienste konfigurieren.

Wenn ein Anwendungsdienst eine Verbindung zu einem anderen Anwendungsdienst in der Domäne herstellt, handelt es sich bei dem Dienst, der die Verbindung initiiert, um einen Client eines anderen Diensts.

Sie können Belastbarkeits-Timeouts für Anwendungsdienste für die folgenden Anwendungsdienste konfigurieren:

PowerCenter-Anwendungsdienste

Sie können das Belastbarkeits-Timeout und Beschränkungen für das Belastbarkeits-Timeout in den erweiterten Eigenschaften des PowerCenter-Integrationsdiensts und des PowerCenter-Repository-Diensts konfigurieren. Das Belastbarkeits-Timeout für Anwendungsdienste, das eine Verbindung zu einem PowerCenter-Integrationsdienst oder PowerCenter-Repository-Dienst herstellt, wird durch einen der folgenden Werte bestimmt:

- Die Diensteigenschaft **Belastbarkeits-Timeout**. Das Belastbarkeits-Timeout für den Dienst können Sie in den Diensteigenschaften konfigurieren. Wenn Sie die Belastbarkeit für einen Dienst deaktivieren möchten, setzen Sie das Belastbarkeits-Timeout auf 0.
- Die Domäneneigenschaft **Belastbarkeits-Timeout**. Um das für die Domäne konfigurierte Belastbarkeits-Timeout zu verwenden, nehmen Sie im Feld für das Belastbarkeits-Timeout für den Dienst keine Eingabe vor.
- Die Diensteigenschaft **Grenzwert für Belastbarkeits-Timeout**. Ist der Dienstgrenzwert für das Belastbarkeits-Timeout niedriger als das Belastbarkeits-Timeout für den Client, der die Verbindung herstellt, nutzt der Client den Grenzwert als Belastbarkeits-Timeout. Um den Grenzwert für das für die Domäne konfigurierte Belastbarkeits-Timeout zu benutzen, nehmen Sie im Feld für den Grenzwert für Belastbarkeits-Timeout keine Eingabe vor.
- Die Domäneneigenschaft **Grenzwert des Belastbarkeits-Timeout**. Verwenden Sie das für die Domäne konfigurierte Belastbarkeits-Timeout und nehmen Sie im Feld für das Belastbarkeits-Timeout für den Dienst keine Eingabe vor.

Sie können das Belastbarkeits-Timeout für den SAP BW-Dienst in den allgemeinen Diensteigenschaften konfigurieren. Die Eigenschaft des Belastbarkeits-Timeouts für den SAP BW-Dienst Eigenschaft wird als **Wiederholungsperiode** bezeichnet.

Hinweis: Wenn Sie den Dienst im Administrator-Tool deaktivieren, kann der Client keine Belastbarkeit für Dienstunterbrechungen aufweisen. Wenn Sie den Dienstprozess deaktivieren, ist der Client in Bezug auf Dienstunterbrechung belastbar.

Failover-Konfiguration für einen Anwendungsdienst

Basierend auf Ihrer Lizenz können Sie Backup-Knoten so konfigurieren, dass Anwendungsdienste ein Failover zu einem anderen Knoten durchführen können, wenn der primäre Knoten fehlschlägt. Konfigurieren Sie Backup-Knoten beim Erstellen oder Aktualisieren eines Anwendungsdiensts.

Wenn Sie einen Backup-Knoten konfigurieren, stellen Sie sicher, dass der Knoten Zugriff auf Laufzeitdateien hat, die jeder Anwendungsdienst benötigt, um Datenintegrationsaufgaben wie Arbeitsabläufe und Mappings

durchzuführen. Ein Arbeitsablauf benötigt möglicherweise Parameterdateien, Eingabedateien oder Ausgabedateien.

Konfiguration für Failover und Wiederherstellung des PowerCenter-Integrationsdienstes

Während Failover und Wiederherstellung muss der PowerCenter-Integrationsdienst auf Vorgangstatusdateien zugreifen und Statusinformationen verarbeiten können.

In den Vorgangstatusdateien wird der Status aller Arbeitsablauf- und Sitzungsvorgänge gespeichert. Der PowerCenter-Integrationsdienst speichert den Status aller Arbeitsablauf- und Sitzungsvorgänge in Dateien im Verzeichnis \$PMStorageDir des PowerCenter-Integrationsdienstprozesses.

In den Informationen zum Prozessstatus wird angegeben, welcher Knoten den PowerCenter-Hauptintegrationsdienst und welcher Knoten die jeweilige Sitzung ausgeführt hat. Sie können den PowerCenter-Integrationsdienst konfigurieren, um Informationen zum Prozessstatus in einem Cluster-Dateisystem oder in der PowerCenter-Repository-Datenbank zu speichern.

Speichern von Hochverfügbarkeits-Persistenz in einem Cluster-Dateisystem

Standardmäßig speichert der PowerCenter-Integrationsdienst Informationen zum Prozessstatus mit den Vorgangstatusdateien im Verzeichnis \$PMStorageDir des Integrationsdienstprozesses. Sie müssen das Verzeichnis \$PMStorageDir für jeden PowerCenter-Integrationsdienstprozess zur Verwendung desselben Verzeichnisses in einem Cluster-Dateisystem konfigurieren.

Knoten, auf denen der PowerCenter-Integrationsdienst ausgeführt wird, müssen sich im selben Cluster-Dateisystem befinden, um Ressourcen gemeinsam nutzen zu können. Darüber hinaus müssen Knoten innerhalb eines Clusters im Heartbeat-Netz des Cluster-Dateisystems liegen. Verwenden Sie ein Cluster-Dateisystem mit hoher Verfügbarkeit, das für I/O-Fencing konfiguriert ist. Die Hardwareanforderungen und Konfiguration einer I/O-Fencing-Lösung sind für jedes Dateisystem unterschiedlich.

Die folgenden Cluster-Dateisysteme sind von Informatica für den Einsatz bei PowerCenter-Integrationsdienst-Failover und -Sitzungswiederherstellung zertifiziert:

Storage Array Network

- Veritas Cluster Files System (VxFS)

- IBM General Parallel File System (GPFS)

Network Attached Storage mit NFS v3-Protokoll

- EMC UxFS, auf einem EMV Celerra NAS-Appliance gehostet

- NetApp WAFL auf einem NetApp NAS-Appliance gehostet

Wenden Sie sich direkt an die entsprechenden Anbieter der Dateisysteme, die Ihren Anforderungen entsprechen.

Speichern von Hochverfügbarkeits-Persistenz in einer Datenbank

Sie können den PowerCenter-Integrationsdienst so konfigurieren, dass Informationen zum Prozessstatus in Datenbanktabellen gespeichert werden. Wenn Sie den PowerCenter-Integrationsdienst zum Speichern von Informationen zum Prozessstatus in einer Datenbank konfigurieren, speichert der Dienst weiterhin den Status aller Arbeitsablauf- und Sitzungsvorgänge in Dateien im Verzeichnis \$PMStorageDir. Sie können das Verzeichnis \$PMStorageDir zur Verwendung eines POSIX-konformen freigegebenen Dateisystems konfigurieren. Sie müssen kein Cluster-Dateisystem verwenden.

Konfigurieren Sie den PowerCenter-Integrationsdienst so, dass Informationen zum Prozessstatus in Datenbanktabellen in den erweiterten Eigenschaften gespeichert werden. Der PowerCenter-Integrationsdienst speichert Informationen zum Prozessstatus in persistenten Datenbanktabellen in der zugeordneten PowerCenter-Repository-Datenbank.

Beim Failover wird die automatische Wiederherstellung von Arbeitsabläufen wiederaufgenommen, sobald der Dienstprozess auf die Datenbanktabellen zugreifen kann.

Konfiguration der Belastbarkeit für Befehlszeilenprogramme

Sie können das Belastbarkeits-Timeout konfigurieren, das Befehlszeilenprogramme zum Ausführen von Domänen- und Service-Vorgängen verwenden.

Wenn Sie die Befehlszeilenprogramme `infacmd`, `pmcmd` oder `pmrep` zum Herstellen einer Verbindung zur Domäne oder zu einem Anwendungsdienst verwenden, wird das Belastbarkeits-Timeout durch die Befehlszeilenoption, eine Umgebungsvariable oder das Standardbelastbarkeits-Timeout festgelegt.

Verwenden Sie die folgenden Richtlinien, wenn Sie Befehlszeilenprogramm-Belastbarkeit konfigurieren:

Befehlszeilenoption

Sie können das Belastbarkeits-Timeout für `infacmd` festlegen, indem Sie beim Ausführen eines Befehls immer die Befehlszeilenoption `-ResilienceTimeout` verwenden. Sie können das Belastbarkeits-Timeout für `pmcmd` festlegen, indem Sie beim Ausführen eines Befehls immer die Befehlszeilenoption `-timeout` verwenden. Wenn Sie den `pmrep`-Befehl "Connect" zum Herstellen einer Verbindung zu einem Repository verwenden, können Sie die Befehlszeilenoption `-timeout` verwenden, um das Belastbarkeits-Timeout für `pmrep`-Befehle festzulegen, die die Verbindung verwenden.

Umgebungsvariable.

Wenn Sie die Timeout-Option nicht in der Befehlszeilensyntax `infacmd` und `pmcmd` festlegen, verwenden die Befehlszeilenprogramme `infacmd` und `pmcmd` den Wert der auf dem Client-Computer konfigurierten Umgebungsvariable `INFA_CLIENT_RESILIENCE_TIMEOUT`. Sollten Sie die Timeout-Option nicht festlegen, wenn Sie den `pmrep`-Befehl "Connect" zum Herstellen einer Verbindung zum Repository verwenden, verwenden `pmrep`-Befehle den Wert der auf dem Client-Computer konfigurierten Umgebungsvariable `INFA_CLIENT_RESILIENCE_TIMEOUT`.

Standardwert

Wenn Sie nicht die Befehlszeilenoption bzw. die Umgebungsvariable verwenden, verwenden die Befehlszeilenprogramme `pmcmd` und `pmrep` das Standard-Belastbarkeits-Timeout von 180 Sekunden. Wenn Sie nicht die Befehlszeilenoption bzw. die Umgebungsvariable verwenden, verwendet das Befehlszeilenprogramm `infacmd` den Wert der Domäneneigenschaft **Dienstebenen-Timeout** als Standard-Belastbarkeits-Timeout.

Grenzwert für Timeout

Wenn der Grenzwert für den Belastbarkeits-Timeout für den PowerCenter-Integrationsdienst oder den PowerCenter-Repository-Dienst kleiner als das Befehlszeilen-Belastbarkeits-Timeout ist, verwendet das Befehlszeilenprogramm den Grenzwert als Belastbarkeits-Timeout.

Hinweis: PowerCenter bietet keine Belastbarkeit für einen Repository-Client, wenn der PowerCenter-Repository-Dienst im exklusiven Modus ausgeführt wird.

Domänen-Failover-Konfiguration

Sie können mehrere Gateway-Knoten definieren, um zu verhindern, dass die Domäne heruntergefahren wird, wenn der Master-Gateway-Knoten nicht verfügbar ist.

Bei der Erstinstallation von Informatica-Diensten erstellen Sie einen Gateway-Knoten. Nach der Installation von Informatica können Sie weitere Gateway-Knoten definieren. Um einen Gateway-Knoten zu definieren, fügen Sie der Domäne einen Gateway-Knoten hinzu oder konfigurieren Sie einen Worker-Knoten, der als Gateway-Knoten eingesetzt wird.

Konfiguration des Knoten-Neustarts

Die Informatica-Dienste führen den Dienstmanager auf allen Knoten in der Domäne aus. Sie können die Informatica-Dienste so konfigurieren, dass sie beim unerwarteten Beenden und Starten eines Knotens automatisch starten.

Um die Informatica-Dienste bei Neustart eines Knotens neu zu starten, führen Sie die folgenden Schritte durch:

- Erstellen Sie in einer UNIX-Umgebung ein Skript, das die Informatica-Dienste automatisch startet, wenn der Knoten startet.
- Gehen Sie in einer Windows-Umgebung in die Systemsteuerung und konfigurieren Sie die Informatica-Dienste für einen automatischen Neustart.

Sie können den Neustart unabhängig von Knotentyp und Knotenrolle für alle Knoten konfigurieren.

Netzwerk, hohe Verfügbarkeit

Die Lösungen für die folgenden Situationen können Ihnen bei der hohen Verfügbarkeit helfen.

Ich bin mir nicht sicher, wo ich nach Informationen über den Status für Client-Verbindungen zum PowerCenter-Repository suchen kann.

In PowerCenter Client-Anwendungen, wie z. B. dem PowerCenter Designer und dem Workflow Manager, wird eine Fehlermeldung angezeigt, wenn die Verbindung nicht während des Zeitlimits aufgebaut werden kann. Detaillierte Informationen über Verbindungsfehler finden Sie im Ausgabe-Fenster. Wenn Sie *pmrep* verwenden, erscheinen die Informationen zu Verbindungsfehlern in der Befehlszeile. Wenn der PowerCenter Integration Service keine Verbindung zum Repository aufbauen kann, erscheint der Fehler im PowerCenter Integration Service-Log, im Arbeitsablauf-Log und im Sitzungs-Log.

Ich habe den falschen Verbindungsstring für eine Oracle-Datenbank eingegeben. Jetzt kann ich den PowerCenter Repository Service nicht aktivieren, obwohl ich die Eigenschaften des PowerCenter Repository Service bearbeitet habe, sodass der richtige Verbindungsstring verwendet wird.

Sie müssen warten, bis das Datenbank-Resistenz-Timeout abgelaufen ist, bevor Sie den PowerCenter Repository Service mit dem aktualisierten Verbindungsstring aktivieren können.

Ich verfüge über die Option für hohe Verfügbarkeit, aber mein FTP-Server ist bei einem Ausfall der Netzwerkverbindung nicht resistent.

Der FTP-Server ist ein externes System. Um eine hohe Verfügbarkeit für FTP-Übertragungen zu erreichen, müssen Sie einen hoch verfügbaren FTP-Server einsetzen. Zum Beispiel verfügt Microsoft IIS 6.0 nicht über eine native Unterstützung für den Neustart des Datei-Uploads oder Datei-Downloads. Das Neustarten von Dateien muss von dem Client verwaltet werden, der die Verbindung zum IIS-Server herstellt. Wenn die Übertragung einer Datei zum oder vom IIS 6.0-Server unterbrochen und innerhalb der Client-Belastbarkeits-Timeouts dann wiederhergestellt wird, wird die Übertragung nicht unbedingt wie erwartet fortgesetzt. Wenn der Schreibvorgang zu mehr als der Hälfte abgeschlossen ist, kann die Targetdatei abgelehnt werden.

Ich verfüge über die Option für hohe Verfügbarkeit, aber die Informatica-Domäne ist nicht resistent, wenn Computer über ein Netzwerk verbunden sind.

Wenn Sie mit einem Netzwerk-Switch für die Verbindung von Computern in der Domäne nutzen, müssen Sie die Auto-Select-Option für den Switch verwenden.

KAPITEL 6

Verbindungen

Dieses Kapitel umfasst die folgenden Themen:

- [Verbindungen - Übersicht, 99](#)
- [Verbindungsverwaltung, 99](#)
- [Pass-Through-Sicherheit, 103](#)
- [Poolingeigenschaften von Verbindungsobjekten, 105](#)

Verbindungen - Übersicht

Eine Verbindung ist ein Repository-Objekt, das eine Verbindung im Domänenkonfigurations-Repository definiert.

Der Datenintegrationsdienst verwendet Datenbankverbindungen, um Jobs für das Developer-Tool und das Analyst-Tool zu verarbeiten. Jobs beinhalten Mappings, Profile, Scorecards und SQL-Datendienste.

Sie können Verbindungen im Administrator-Tool, im Developer-Tool und im Analyst-Tool erstellen und verwalten.

Welche Aufgaben Sie jeweils in den einzelnen Tools ausführen können, hängt vom jeweiligen Tool ab. Beispiel: Sie können eine SAP NetWeaver-Verbindung im Developer-Tool erstellen und diese im Administrator-Tool verwalten; im Analyst-Tool hingegen können Sie diese Verbindung weder erstellen noch verwalten.

Hinweis: Diese Verbindungen sind unabhängig von den Verbindungen, die Sie im PowerCenter-Arbeitsablauf-Manager erstellen.

Verbindungsverwaltung

Nach dem Erstellen einer Verbindung können Sie die Verbindung anzeigen, die Verbindungseigenschaften konfigurieren und die Verbindung löschen.

Nachdem Sie eine Verbindung erstellt haben, können Sie die folgenden Aktionen ausführen:

Konfigurieren von Verbindungspooling.

Konfigurieren Sie Verbindungspooling, um die Verarbeitung für den Datenintegrationsdienst zu optimieren. Das Verbindungspooling ist ein Framework zu Cache-Verbindungen.

Anzeigen von Verbindungseigenschaften.

Zeigen Sie die Verbindungseigenschaften über die Ansicht **Verbindungen** auf der Registerkarte **Domäne** an.

Bearbeiten der Verbindung.

Sie können den Namen und die Beschreibung für die Verbindung ändern. Sie können auch Verbindungsdetails wie den Benutzernamen, das Passwort und Verbindungszeichenfolgen bearbeiten. Wenn Sie eine Datenbankverbindung aktualisieren, die Verbindungspooling deaktiviert hat, werden alle Updates sofort wirksam.

Der Datenintegrationsdienst identifiziert Verbindungen anhand der Verbindungs-ID und nicht mit dem Namen der Verbindung. Wenn Sie eine Verbindung umbenennen, aktualisieren das Developer-Tool und das Analyst-Tool die Jobs, die die Verbindung verwenden.

Der Datenintegrationsdienst identifiziert Verbindungen anhand der Verbindungs-ID und nicht mit dem Namen der Verbindung. Wenn Sie eine Verbindung umbenennen, aktualisiert das Developer-Tool die Jobs, die die Verbindung verwenden.

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.

Löschen der Verbindung.

Wenn Sie eine Verbindung löschen, sind die Objekte, die diese Verbindung verwenden, nicht mehr gültig. Wenn Sie eine Verbindung versehentlich löschen, können Sie sie neu erstellen, indem Sie eine andere Verbindung mit derselben Verbindungs-ID wie die gelöschte Verbindung erstellen.

Aktualisieren der Verbindungsliste.

Sie können die Verbindungsliste aktualisieren, um eine Liste mit den neuesten Verbindungen für die Domäne anzuzeigen. Aktualisieren Sie die Verbindungsliste, nachdem ein Benutzer eine Verbindung im Developer-Tool oder im Analyst-Tool hinzugefügt, gelöscht oder umbenannt hat.

Sie können die Verbindungsliste aktualisieren, um eine Liste mit den neuesten Verbindungen für die Domäne anzuzeigen. Aktualisieren Sie die Verbindungsliste, wenn ein Benutzer eine Verbindung im Developer-Tool hinzufügt, löscht oder umbenennt.

Erstellen einer Verbindung

Im Administrator Tool können Sie Verbindungen zu relationalen Datenbanken, sozialen Medien und Dateisystemen herstellen.

1. Klicken Sie im Administrator-Tool auf die Registerkarte **Domäne**.
2. Klicken Sie auf die Ansicht **Verbindungen**.
3. Wählen Sie die Domäne im Navigator aus.
4. Klicken Sie im Navigator auf **Aktionen > Neu > Datenbankverbindung**.

Das Dialogfeld **Neue Datenbankverbindung** wird eingeblendet.

5. Wählen Sie im Dialogfeld **Neue Verbindung** den Verbindungstyp aus, und klicken Sie dann auf **OK**.
Die **Neue Verbindung** wird angezeigt.

6. Geben Sie die Verbindungseigenschaften ein.

Die Verbindungseigenschaften, die Sie eingeben, richten sich nach dem Verbindungstyp. Klicken Sie auf **Weiter**, um zur nächsten Seite im Assistenten **Neue Verbindung** zu wechseln.

7. Klicken Sie nach der Eingabe der Verbindungseigenschaften auf **Verbindung testen**, um die Verbindung zu testen.
8. Klicken Sie auf **Fertig stellen**.

Aktualisieren der Verbindungsliste

Aktualisieren Sie die Verbindungsliste, um die neueste Liste der Verbindungen in der Domäne anzuzeigen.

Das Administrator-Tool zeigt die neueste Verbindungsliste beim Starten des Administrator-Tool an. Wenn ein Benutzer eine Verbindung im Developer-Tool oder im Analyst-Tool hinzufügt, löscht oder umbenennt, ist eine Aktualisierung der Verbindungsliste empfehlenswert.

Das Administrator-Tool zeigt die neueste Verbindungsliste beim Starten des Administrator-Tool an. Sie möchten unter Umständen die Verbindungsliste aktualisieren, wenn ein Benutzer eine Verbindung im Developer-Tool hinzufügt, löscht oder umbenennt.

1. Klicken Sie im Administrator-Tool auf die Registerkarte **Domäne**.
2. Klicken Sie auf die Ansicht **Verbindungen**.
Der Navigator zeigt alle Verbindungen in der Domäne an.
3. Wählen Sie die Domäne im Navigator aus.
4. Klicken Sie auf **Aktionen > Aktualisieren**.

Anzeigen einer Verbindung

Mit den folgenden Schritten zeigen Sie Verbindungen im Administrator Tool an.

1. Klicken Sie im Administrator-Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie auf die Ansicht **Verbindungen**.
Der Navigator zeigt alle Verbindungen in der Domäne an.
3. Wählen Sie im Navigator die Domäne.
Der Inhaltsbereich zeigt alle Verbindungen der Domäne an.
4. Zum Filtern der im Inhaltsbereich angezeigten Verbindungen, geben Sie ein Filterkriterium ein und klicken auf die Schaltfläche Filter.
Der Inhaltsbereich zeigt die Verbindungen an, die dem Filterkriterium entsprechen.
5. Um das Filterkriterium zu entfernen, klicken Sie auf die Schaltfläche "Filter zurücksetzen".
Der Inhaltsbereich zeigt alle Verbindungen der Domäne an.
6. Sortieren Sie die Verbindungen, indem Sie in die Spaltenüberschrift klicken, anhand derer die Verbindungen sortiert werden sollen.
Standardmäßig sind die Verbindungen anhand des Namens sortiert.
7. Um Spalten aus dem Inhaltsbereich zu entfernen oder neue hinzuzufügen, klicken Sie die Spaltenüberschrift mit der rechten Maustaste an.
Wenn Sie eine Leseberechtigung für die Verbindung haben, können Sie die Daten in der Spalte **Erstellt durch** sehen. Andernfalls ist diese Spalte leer.
8. Um die Verbindungsdetails anzuzeigen, wählen Sie eine Verbindung im Navigator aus.
Der Inhaltsbereich zeigt die Verbindungsdetails an.

Konfigurieren des Pooling für eine Verbindung

Das Pooling für eine Verbindung wird im Administrator Tool konfiguriert.

1. Klicken Sie im Administrator-Tool auf die Registerkarte **Domäne**.
2. Klicken Sie auf die Ansicht **Verbindungen**.
3. Wählen Sie im Navigator eine Verbindung aus.
Der Inhaltsbereich zeigt die Verbindungseigenschaften an.
4. Klicken Sie im Inhaltsbereich auf die Ansicht **Pooling**
5. Klicken Sie im Bereich **Pooling-Eigenschaften** auf **Bearbeiten**.
Das Dialogfeld **Pooling-Eigenschaften bearbeiten** wird angezeigt.
6. Bearbeiten Sie die Pooling-Eigenschaften und klicken Sie auf **OK**.

Bearbeiten und Testen einer Verbindung

Im Administrator-Tool können Sie Verbindungen bearbeiten, die Sie im Administrator-Tool, im Analyst-Tool, im Developer-Tool oder mit dem infacmd isp CreateConnection-Befehl erstellt haben. Sie können relationale Datenbankverbindungen testen. Im Administrator-Tool können Sie Verbindungen bearbeiten, die Sie im Administrator- und im Developer-Tool erstellt haben.

1. Klicken Sie im Administrator-Tool auf die Registerkarte **Domäne**.
2. Klicken Sie auf die Ansicht **Verbindungen**.
Der Navigator zeigt alle Verbindungen in der Domäne an.
3. Wählen Sie im Navigator eine Verbindung aus.
Der Inhaltsbereich zeigt die Verbindungseigenschaften.
4. Wählen Sie im Inhaltsbereich die Ansicht **Eigenschaften** oder **Pooling** aus.
5. Um Eigenschaften in einem Abschnitt zu bearbeiten, klicken Sie auf **Bearbeiten**.
Bearbeiten Sie die Eigenschaften und klicken Sie auf **OK**.
Hinweis: Wenn Sie einen Verbindungsnamen ändern, müssen Sie alle Anwendungen, die die Verbindung verwenden, erneut bereitstellen. Außerdem müssen Sie alle Parameterdateien aktualisieren, die den Verbindungsparameter verwenden.
6. Um eine Datenbankverbindung zu überprüfen, wählen Sie die Verbindung im Navigator aus.
Klicken Sie auf **Aktionen > Verbindung testen** auf der Registerkarte **Domäne**.
Das Testergebnis wird in einem Meldungsfenster angezeigt.

Löschen einer Verbindung

Sie können eine Datenbankverbindung im Administrator-Tool löschen.

Wenn Sie eine Datenbankverbindung im Administrator-Tool löschen, entfernen Sie diese auch aus dem Developer-Tool und dem Analyst-Tool.

Wenn Sie im Administrator-Tool eine Verbindung löschen, wird diese im Developer-Tool ebenfalls gelöscht.

1. Klicken Sie im Administrator-Tool auf die Registerkarte **Domäne**.
2. Klicken Sie auf die Ansicht **Verbindungen**.
Der Navigator zeigt alle Verbindungen in der Domäne an.
3. Wählen Sie im Navigator eine Verbindung aus.

4. Klicken Sie im Navigator auf **Aktionen > Löschen**.

Pass-Through-Sicherheit

Pass-Through-Sicherheit ist die Möglichkeit der Verbindung mit einem SQL-Datendienst oder einer externen Quelle unter Verwendung der Client-Anmeldeinformationen anstelle der Anmeldeinformationen eines Verbindungsobjekts.

Abhängig von ihrer Aufgabe im Unternehmen können Benutzer Zugriff auf verschiedene Gruppen von Daten haben. Client-Systeme beschränken den Zugriff auf Datenbanken anhand von Benutzernamen und Passwort. Wenn Sie einen SQL-Datendienst erstellen, können Sie Daten aus verschiedenen Systemen kombinieren und so eine einzige Ansicht der Daten erstellen. Wenn Sie jedoch die Verbindung zum SQL-Datendienst definieren, hat die Verbindung einen Benutzernamen und ein Passwort.

Wenn Sie die Pass-Through-Sicherheit konfigurieren, können Sie Benutzer bei einigen der Daten in einem SQL-Datendienst auf der Basis ihres Benutzernamens einschränken. Wenn sich ein Benutzer mit dem SQL-Datendienst verbindet, ignoriert der Data Integration Service den Benutzernamen und das Passwort im Verbindungsobjekt. Der Benutzer stellt die Verbindung mit dem Client-Benutzernamen oder dem LDAP-Benutzernamen her.

Das Mapping von Web-Dienstoperationen muss möglicherweise ein Verbindungsobjekt für den Zugriff auf Daten verwenden. Wenn Sie Pass-Through-Sicherheit konfigurieren und der Web-Dienst WS-Security nutzt, stellt das Mapping der Web-Dienstoperation eine Verbindung zu einer Quelle mit dem Benutzernamen und dem Passwort her, die in der SOAP-Anfrage des Web-Dienstes bereitgestellt wurden.

Konfigurieren Sie die Pass-Through-Sicherheit für eine Verbindung in den Verbindungseigenschaften des Administratortools oder mit infacmd die UpdateServiceOptions. Sie können die Pass-Through-Sicherheit für Verbindungen zu bereitgestellten Anwendungen festlegen. Sie können die Pass-Through-Sicherheit nicht im Developer-Tool festlegen. Nur SQL-Datendienste und Webdienste erkennen die Pass-Through-Sicherheitskonfiguration.

Weitere Informationen zum Konfigurieren der Sicherheit für SQL-Datendienste finden Sie im Artikel „Sicherheitskonfiguration für SQL-Datendienste“ der Informatica-Produktverwendung:
https://kb.informatica.com/h2l/HowTo%20Library/1/0266_ConfiguringSecurityForSQLDataServices.pdf.

Beispiel

Eine Organisation vereint Mitarbeiterdaten von mehreren Datenbanken, um eine einzelne Ansicht der Mitarbeiterdaten in einem SQL-Datendienst darzustellen. Der SQL-Datendienst enthält Daten aus den Datenbanken "Mitarbeiter" und "Vergütung". Die Datenbank "Mitarbeiter" enthält Informationen zu Namen, Adresse und Abteilung. Die Datenbank "Vergütung" enthält Informationen zu Gehalt und Aktienoptionen.

Ein Benutzer kann beispielsweise Zugriff auf die Mitarbeiterdatenbank, jedoch nicht auf die Vergütungsdatenbank haben. Wenn der Benutzer eine Abfrage auf den SQL-Datendienst ausführt, ersetzt der Data Integration Service die Anmeldeinformationen bei jeder Datenbankverbindung durch den Benutzernamen und das Benutzerpasswort. Die Abfrage schlägt fehl, wenn der Benutzer Gehaltsinformationen aus der Verbindung mit aufnimmt.

Pass-Through-Sicherheit mit Datenobjekt-Zwischenspeicherung

Für den Einsatz des Datenobjekt-Cache mit Pass-Through-Sicherheit müssen Sie Cache in den Pass-Through-Sicherheitseigenschaften für den Data Integration Service aktivieren.

Wenn Sie einen SQL-Datendienst oder einen Web-Dienst bereitstellen, können Sie wählen, ob Sie die logischen Datenobjekte in einer Datenbank zwischenspeichern möchten. Sie müssen die Datenbank zum Speichern des Datenobjekt-Cache angeben. Der Data Integration Service validiert die Benutzer-Anmeldedaten für den Zugriff auf die Cache-Datenbank. Ein Benutzer, der sich mit der Cache-Datenbank verbinden kann, hat Zugriff auf alle Tabellen im Cache-Speicher. Ist Cache aktiviert, führt der Data Integration Service keine Validierung der Benutzer-Anmeldedaten gegen die Quelldatenbanken durch.

Beispiel: Sie konfigurieren Cache für den EmployeeSQLDS SQL Datendienst und aktivieren Pass-Through-Sicherheit für Verbindungen. Der Data Integration Service speichert im Cache Tabellen aus den Kompensations- und Mitarbeiterdatenbanken. Unter Umständen hat ein Benutzer keinen Zugriff auf die Kompensations-Datenbank. Hat der Benutzer jedoch Zugriff auf die Cache-Datenbank, kann er in einer SQL-Anfrage Kompensationsdaten auswählen.

Wenn Sie Pass-Through-Sicherheit konfigurieren, wird Datenobjekt-Cache per Standard nicht für die von Pass-Through-Verbindungen abhängigen Datenobjekte zugelassen. Aktivieren Sie Datenobjekt-Cache mit Pass-Through-Sicherheit, müssen Sie überprüfen, dass Sie keinen unbefugten Benutzern Zugriff auf einige der Daten im Cache gewähren. Falls Sie Cache für Verbindungen mit Pass-Through-Sicherheit aktivieren, ist Datenobjekt-Cache für alle Verbindungen mit Pass-Through-Sicherheit aktiviert.

Pass-Through-Sicherheit hinzufügen

Aktivieren Sie Pass-Through-Sicherheit für eine Verbindung in die Verbindungseigenschaften. Aktivieren Sie Datenobjekt-Caching für Pass-Through-Sicherheitsverbindungen in den Pass-Through-Sicherheitseigenschaften des Data Integration Service.

1. Wählen Sie eine Verbindung aus.
2. Klicken Sie auf die Ansicht **Eigenschaften**.
3. Bearbeiten Sie die Verbindungseigenschaften.
Das Dialogfeld **Verbindungseigenschaften bearbeiten** wird angezeigt.
4. Um Pass-Through-Sicherheit für die Verbindung auszuwählen, wählen Sie die Option **Pass-Through-Sicherheit aktivieren** aus.
5. Wählen Sie optional den Data Integration Service aus, für den Sie Datenobjekt-Caching für Pass-Through-Sicherheit aktivieren möchten.
6. Klicken Sie auf die Ansicht **Eigenschaften**.
7. Bearbeiten Sie die Pass-Through-Sicherheitsoptionen.
Das Dialogfeld **Pass-Through-Sicherheitsoptionen bearbeiten** wird angezeigt.
8. Wählen Sie **Caching zulassen** aus, um Datenobjekt-Caching für den SQL-Datendienst oder Web-Dienst zuzulassen. Dies gilt für alle Verbindungen.
9. Klicken Sie auf **OK**.

Sie müssen den Data Integration Service recyceln, damit Sie die Verbindungen zwischenspeichern können.

Poolingeigenschaften von Verbindungsobjekten

Sie können Poolingeigenschaften von Verbindungen in der Ansicht **Pooling** für eine Datenbankverbindung bearbeiten.

Wenn der Datenintegrationsdienst Jobs in verschiedenen Betriebssystemprozessen ausführt, hängt die Anzahl der Bibliotheken im Verbindungspool von der Anzahl der laufenden DTM-Prozesse ab. Jeder DTM-Prozess führt seine eigene Verbindungspool-Bibliothek. Die Werte der Poolingeigenschaften sind für jede Verbindungspool-Bibliothek. Wenn Sie beispielsweise die maximale Anzahl von Verbindungen auf 15 einstellen, kann jede Verbindungspoolbibliothek maximal 15 inaktive Verbindungen im Pool haben. Wenn bei Ihnen drei DTM-Prozesse laufen, können Sie maximal 45 inaktive Verbindungsinstanzen haben.

Um die Gesamtanzahl inaktiver Verbindungsinstanzen zu verringern, legen Sie die Mindestanzahl an Verbindungen auf 0 fest und verringern Sie die maximal erlaubte inaktive Zeit für jede Datenbankverbindung.

Die folgende Liste beschreibt die Poolingeigenschaften der Datenbankverbindung, die Sie in der Ansicht **Pooling** für Datenbankverbindungen bearbeiten können:

Verbindungspooling aktivieren

Aktiviert das Verbindungspooling. Wenn Sie das Verbindungspooling aktivieren, behält jeder Verbindungspool inaktive Verbindungsinstanzen im Speicher. Um inaktive Verbindungen in den Pools zu löschen, müssen Sie den Datenintegrationsdienst neu starten.

Wenn das Verbindungspooling deaktiviert ist, stoppt der DTM-Prozess oder der Datenintegrationsdienst alle Poolingaktivitäten. Der DTM-Prozess oder der Datenintegrationsdienstprozess erstellt bei jeder Verarbeitung eines Jobs eine Verbindungsinstanz. Er löscht die Instanz, wenn er die Verarbeitung der Jobs beendet.

Standardwert ist aktiviert für DB2 für i5/OS-, DB2 für z/OS-, IBM DB2-, Microsoft SQL Server-, Oracle- und ODBC-Verbindungen. Die Standardeinstellung ist für Adabas-, IMS-, sequenzielle und VSAM-Verbindungen deaktiviert.

Gemäß Voreinstellung ist diese Option für Microsoft SQL Server-, IBM DB2-, Oracle- und ODBC-Verbindungen aktiviert.

Mindestanzahl an Verbindungen

Die Mindestanzahl inaktiver Verbindungsinstanzen, die ein Pool für eine Datenbankverbindung aufrechterhält, nachdem die maximal erlaubte inaktive Zeit erreicht ist. Setzen Sie diesen Wert maximal auf die maximale Anzahl inaktiver Verbindungsinstanzen. Standardwert ist 0.

Maximale Anzahl an Verbindungen

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.

Maximale Leerlaufzeit

Die Anzahl der Sekunden, die eine Verbindungsinstanz, welche die Mindestanzahl von Verbindungsinstanzen überschritten hat, inaktiv bleiben kann, bevor sie vom Verbindungspool gelöscht wird. Der Verbindungspool ignoriert die inaktive Zeit, wenn die Verbindungsinstanz die Mindestanzahl von inaktiven Verbindungsinstanzen nicht überschreitet. Standardwert ist 120.

KAPITEL 7

Verbindungseigenschaften

Dieses Kapitel enthält Verbindungseigenschaften für jede der Verbindungen, die Sie über Informatica-Clients erstellen und verwalten können.

Adabas-Verbindungseigenschaften

Verwenden Sie eine Adabas-Verbindung, um auf eine Adabas-Datenbank zuzugreifen. Die Adabas-Verbindung ist ein Mainframe-Datenbank-Verbindungstyp. Sie erstellen eine Adabas-Verbindung im Developer-Tool. Sie können eine Adabas-Verbindung im Administrator-Tool oder im Developer-Tool verwalten.

In der folgenden Tabelle werden die Eigenschaften von Adabas-Verbindungen erläutert:

Option	Beschreibung
Speicherort	Knotenname für den Speicherort des PowerExchange-Listenerdiensts, der eine Verbindung zu Adabas herstellt. Der Knotenname ist im ersten Parameter der NODE-Anweisung in der PowerExchange-Konfigurationsdatei „dbmover.cfg“ definiert.
Benutzername	Benutzername für die Datenbank Wenn Sie für eine Datenbank auf einem unterstützten Linux- oder UNIX-System die LDAP-Benutzer-Authentifizierung für PowerExchange aktiviert haben, ist der Benutzername der Benutzername des Unternehmens. Weitere Informationen finden Sie im <i>PowerExchange-Referenzhandbuch</i> .

Option	Beschreibung
Passwort	<p>Passwort für den Datenbankbenutzernamen oder eine gültige PowerExchange-Passphrase. Eine PowerExchange-Passphrase kann 9 bis 128 Zeichen lang sein und die folgenden Zeichen enthalten:</p> <ul style="list-style-type: none"> - Groß- und Kleinbuchstaben - Die Zahlen 0 bis 9 - Leerzeichen - Die folgenden Sonderzeichen: ' - ; # \ , . / ! % & * () _ + { } : @ < > ? <p>Hinweis: Das erste Zeichen ist ein Apostroph.</p> <p>Passphrasen dürfen keine einfachen Anführungszeichen ('), doppelten Anführungszeichen (") oder Währungssymbole enthalten.</p> <p>Stellen Sie vor der Verwendung von Passphrasen sicher, dass der PowerExchange-Listenerdienst im DBMOVER-Mitglied mit der Sicherheitseinstellung SECURITY=(1,N) oder höher ausgeführt wird. Weitere Informationen finden Sie unter „SECURITY-Anweisung“ im <i>PowerExchange-Referenzhandbuch</i>.</p> <p>Die zulässigen Zeichen beim Beenden von IBM IRRPHREX haben keine Auswirkungen auf die zulässigen Zeichen in PowerExchange-Passphrasen.</p> <p>Hinweis: Eine gültige RACF-Passphrase kann bis zu 100 Zeichen enthalten. PowerExchange schneidet Passphrases mit mehr als 100 Zeichen ab, wenn diese zur Validierung an RACF übergeben werden.</p>
Codepage	<p>Erforderlich. Name der Codepage für das Lesen aus oder Schreiben in die Datenquelle. Normalerweise ist dieser Wert ein ISO-Codepage-Name, z. B. ISO-8859-6.</p>
Pass-Through-Sicherheit aktiviert	<p>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.</p>
Verschlüsselungstyp	<p>Der Verschlüsselungstyp, den der Datenintegrationsdienst verwendet. Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> - Keine - RC2 - DES <p>Standardwert ist „Keine“.</p> <p>Hinweise:</p> <ul style="list-style-type: none"> - Informatica empfiehlt die Verwendung der SSL (Secure Sockets Layer)-Authentifizierung, anstatt den Verschlüsselungstyp und die Level-Verbindungseigenschaften oder die ENCRYPT- und ENCRYPTLEVEL-Anweisungen in der DBMOVER-Konfigurationsdatei zu konfigurieren. Die SSL-Authentifizierung bietet eine strikere Sicherheit und wird von diversen Informatica-Produkten verwendet. <p>Weitere Informationen zum Implementieren der SSL-Authentifizierung in einem PowerExchange-Netzwerk finden Sie im <i>PowerExchange-Referenzhandbuch</i>.</p> <ul style="list-style-type: none"> - Die Werte, die Sie für die Verbindungsattribute Verschlüsselungstyp und Level auswählen, setzen die Werte in den ENCRYPT- und ENCRYPTLEVEL-Anweisungen außer Kraft, wenn sie in der DBMOVER-Konfigurationsdatei auf dem Integrationsdienst-Rechner definiert wurden. Zum Aktivieren der Verschlüsselung für ein Mapping müssen Sie die geeigneten Verbindungsattribute auswählen.

Option	Beschreibung
[Encryption]-Ebene	<p>Wählen Sie bei Auswahl von RC2 oder DES für Verschlüsselungstyp eine der folgenden Optionen aus, um die Verschlüsselungsebene anzugeben, die der Datenintegrationsdienst verwendet:</p> <ul style="list-style-type: none"> - 1. Verwenden Sie einen 56-Bit-Verschlüsselungsschlüssel für DES und RC2. - 2. Verwenden Sie einen dreifachen 168-Bit-Verschlüsselungsschlüssel für DES und einen 64-Bit-Verschlüsselungsschlüssel für RC2. - 3. Verwenden Sie einen dreifachen 168-Bit-Verschlüsselungsschlüssel für DES und einen 128-Bit-Verschlüsselungsschlüssel für RC2. <p>Diese Option wird ignoriert, wenn Sie keinen Verschlüsselungstyp auswählen. Standard ist 1.</p>
Pacing-Größe	<p>Optional. Menge der Daten, die das Quellsystem an den PowerExchange-Listenerdienst übergeben kann. Legen Sie die Pacing-Größe fest, wenn eine externe Anwendung, eine Datenbank oder der Knoten mit dem Datenintegrationsdienst einen Engpass darstellt. Verwenden Sie niedrigere Werte für schnellere Leistung.</p> <p>Der Mindest- und Standardwert ist 0. Mit dem Wert 0 wird die beste Leistung erzielt.</p>
Als Zeilen interpretieren	<p>Optional. Wählen Sie diese Option, um die Pacing-Größe als Anzahl von Zeilen anzugeben. Löschen Sie diese Option, um die Pacing-Größe in Kilobyte anzugeben. Diese Option ist standardmäßig nicht ausgewählt und die Pacing-Größe wird in Kilobyte angegeben.</p>
Komprimierung	<p>Optional. Wählen Sie diese Option zum Aktivieren der Quelldatenkomprimierung aus. Durch die Komprimierung von Daten können Sie die Menge der Daten verringern, die Informatica-Anwendungen über das Netzwerk senden. Standardmäßig ist diese Option nicht ausgewählt und die Komprimierung ist deaktiviert.</p>
Offload-Verarbeitung	<p>Optional. Steuert, ob für die Verarbeitung von Stapeldaten vom Quellcomputer zum Datenintegrationsdienst-Computer Offload-Verarbeitung verwendet werden soll. Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> - AUTO. Der Datenintegrationsdienst bestimmt, ob Offload-Verarbeitung verwendet werden soll. - Ja. Offload-Verarbeitung wird verwendet. - Nein. Offload-Verarbeitung wird nicht verwendet. <p>Der Standardwert ist AUTO.</p>
Worker-Threads	<p>Optional. Anzahl der vom Datenintegrationsdienst verwendeten Threads, um Stapeldaten bei aktivierter Offload-Verarbeitung zu verarbeiten. Um eine optimale Leistung zu erzielen, darf 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 deaktiviert.</p>

Option	Beschreibung
Array-Größe	Optional. Die Anzahl der Datensätze im Speicher-Array für die Worker-Threads. Diese Option kann verwendet werden, wenn Sie die Option Worker-Threads auf einen Wert größer als 0 festlegen. Gültige Werte sind 1 bis 100.000. Standardwert ist 25.
Schreibmodus	<p>Optional. Modus, in dem der Datenintegrationsdienst Daten zum PowerExchange-Listenerdienst sendet. Wählen Sie einen der folgenden Schreibmodi aus:</p> <ul style="list-style-type: none"> - CONFIRMWRITEON. Sendet Daten an den PowerExchange-Listenerdienst und wartet auf eine Antwort, bevor weitere Daten gesendet werden. Wählen Sie diese Option aus, wenn die Fehlerbehebung Priorität hat. Diese Option kann jedoch zu Leistungseinbußen führen. - CONFIRMWRITEOFF. Sendet Daten an den PowerExchange-Listenerdienst, ohne auf eine Antwort zu warten. Verwenden Sie diese Option, wenn Sie die Zieltabelle im Fall eines Fehlers erneut laden können. - ASYNCHRONOUSWITHFAULTTOLERANCE. Sendet Daten an den PowerExchange-Listenerdienst, ohne auf eine Antwort zu warten. Diese Option aktiviert außerdem die Fehlererkennung. Diese Option kombiniert die Geschwindigkeit von CONFIRMWRITEOFF und die Datenintegrität von CONFIRMWRITEON. <p>Der Standardwert ist CONFIRMWRITEON.</p>

DataSift-Verbindungseigenschaften

Verwenden Sie eine DataSift-Verbindung zum Extrahieren von Daten aus DataSift-Streams. Eine DataSift-Verbindung ist eine Verbindung zu einem sozialen Medium. Sie können eine DataSift-Verbindung im Administrator-Tool oder im Developer-Tool verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Eigenschaften von DataSift-Verbindungen erläutert:

Eigenschaft	Beschreibung
Name	Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. 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 765 Zeichen enthalten.
Speicherort	Die Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Der Verbindungstyp. Wählen Sie DataSift.
Benutzername	Benutzername für das DataSift-Konto.
API-Schlüssel	API-Schlüssel. Der Developer-API-Schlüssel wird auf der Seite „Dashboard“ oder „Einstellungen“ im DataSift-Konto angezeigt.

Facebook-Verbindungseigenschaften

Verwenden Sie eine Facebook-Verbindung, um Daten aus einer Facebook-Webseite zu extrahieren. Eine Facebook-Verbindung ist eine Verbindung zu einem sozialen Medium. Sie können eine Facebook-Verbindung im Administrator-Tool oder im Developer-Tool verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Eigenschaften von Facebook-Verbindungen erläutert:

Eigenschaft	Beschreibung
Name	Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. 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 765 Zeichen enthalten.
Speicherort	Die Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Der Verbindungstyp. Wählen Sie Facebook aus.
Haben Sie OAuth-Details?	Zeigt an, ob Sie OAuth konfigurieren möchten. Wählen Sie einen der folgenden Werte aus: <ul style="list-style-type: none">- Ja. Gibt an, dass Sie über den Zugriffstoken verfügen.- Nein. Startet das OAuth-Dienstprogramm.
Verbraucherschlüssel	Die Anwendungs-ID, die Sie beim Erstellen der Anwendung in Facebook erhalten. Facebook verwendet den Schlüssel zur Identifizierung der Anwendung.
Verbrauchergeheimwort	Das Anwendungsgeheimwort, das Sie beim Erstellen der Anwendung in Facebook erhalten. Facebook verwendet das Geheimwort für das Eigentum am Verbraucherschlüssel.
Zugriffstoken	Zugriffstoken, den das OAuth-Dienstprogramm zurückgibt. Facebook verwendet diesen Token anstelle der Benutzeranmeldedaten für den Zugriff auf geschützte Ressourcen.
Zugriffsgeheimwort	Das Zugriffsgeheimwort ist für eine Facebook-Verbindung nicht erforderlich.
Bereich	Berechtigungen für die Anwendung. Geben Sie die Berechtigungen ein, die Sie zum Konfigurieren von OAuth verwendet haben.

Greenplum-Verbindungseigenschaften

Verwenden Sie eine Greenplum-Verbindung zum Herstellen einer Verbindung zur Greenplum-Datenbank. Die Greenplum-Verbindung ist ein relationaler Verbindungstyp. Sie können eine Greenplum-Verbindung im Administrator-Tool oder im Developer-Tool verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

Beim Erstellen einer Greenplum-Verbindung geben Sie Informationen für Metadaten und Datenzugriff ein.

In der folgenden Tabelle werden die Eigenschaften von Greenplum-Verbindungen erläutert:

Eigenschaft	Beschreibung
Name	Name der relationalen Greenplum-Verbindung.
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 765 Zeichen enthalten.
Speicherort	Domäne, auf der die Verbindung erstellt werden soll.
Typ	Typ der Verbindung.

Benutzername, Passwort, Treibername und Verbindungszeichenfolge sind für das Importieren der Metadaten erforderlich. Die folgende Tabelle beschreibt die Eigenschaften für den Metadatenzugriff:

Eigenschaft	Beschreibung
Benutzername	Benutzername mit Berechtigungen für den Zugriff auf die Greenplum-Datenbank.
Passwort	Passwort für die Verbindung zur Greenplum-Datenbank.
Treibername	Der Name des Greenplum JDBC-Treibers. Beispiel: <code>com.pivotal.jdbc.GreenplumDriver</code> Weitere Informationen über den Treiber finden Sie in der Greenplum-Dokumentation.
Verbindungszeichenfolge	Verwenden Sie die folgende Verbindungs-URL: <code>jdbc:pivotal:greenplum:// <hostname>:<port>;DatabaseName=<database_name></code> Weitere Informationen über den Verbindungs-URL finden Sie in der Greenplum-Dokumentation.

PowerExchange for Greenplum verwendet den Hostnamen, die Portnummer und den Datenbanknamen zum Erstellen einer Steuerdatei, in der Ladespezifikationen für das Greenplum-Bulk-Ladeprogramm `gpload` angegeben werden. Die Option zum Aktivieren von SSL und der Zertifikatspfad werden zum Einrichten sicherer Kommunikation mit dem Greenplum-Server über SSL verwendet.

In der folgenden Tabelle werden die Verbindungseigenschaften für den Datenzugriff beschrieben:

Eigenschaft	Beschreibung
Hostname	Hostname oder IP-Adresse des Greenplum-Servers.
Portnummer	Greenplum-Serverportnummer. Wenn Sie „0“ eingeben, liest das Dienstprogramm „gpload“ von der Umgebungsvariable \$PGPORT. Standardwert ist „5432“.
Datenbankname	Name der Datenbank
SSL aktivieren	Wählen Sie diese Option aus, um sichere Kommunikation zwischen dem Dienstprogramm gpload und dem Greenplum-Server über SSL einzurichten.
Zertifikatspfad	Pfad, in dem die SSL-Zertifikate für den Greenplum-Server gespeichert werden. Informationen zu den Dateien, die im Zertifikatspfad enthalten sein müssen, finden Sie in der gpload-Dokumentation.

HBase Connection Properties

Use an HBase connection to access HBase. The HBase connection is a NoSQL connection. You can create and manage an HBase connection in the Administrator tool or the Developer tool. HBase connection properties are case sensitive unless otherwise noted.

The following table describes HBase connection properties:

Property	Description
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: ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
ID	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.
Description	The description of the connection. The description cannot exceed 4,000 characters.
Location	The domain where you want to create the connection.
Type	The connection type. Select HBase.
ZooKeeper Host(s)	Name of the machine that hosts the ZooKeeper server. When the ZooKeeper runs in the replicated mode, specify a comma-separated list of servers in the ZooKeeper quorum servers. If the TCP connection to the server breaks, the client connects to a different server in the quorum.

Property	Description
ZooKeeper Port	Port number of the machine that hosts the ZooKeeper server. If the Hadoop cluster uses MapR, use the value specified for <code>hbase.zookeeper.property.clientPort</code> in <code>hbase-site.xml</code> . You can find <code>hbase-site.xml</code> on the NameNode machine in the following directory: <code>/opt/mapr/hbase/hbase-0.98.7/conf</code> .
Enable Kerberos Connection	Enables the Informatica domain to communicate with the HBase master server or region server that uses Kerberos authentication.
HBase Master Principal	Service Principal Name (SPN) of the HBase master server. Enables the ZooKeeper server to communicate with an HBase master server that uses Kerberos authentication. Enter a string in the following format: <code>hbase/<domain.name>@<YOUR-REALM></code> Where: <ul style="list-style-type: none"> - <code>domain.name</code> is the domain name of the machine that hosts the HBase master server. - <code>YOUR-REALM</code> is the Kerberos realm.
HBase Region Server Principal	Service Principal Name (SPN) of the HBase region server. Enables the ZooKeeper server to communicate with an HBase region server that uses Kerberos authentication. Enter a string in the following format: <code>hbase_rs/<domain.name>@<YOUR-REALM></code> Where: <ul style="list-style-type: none"> - <code>domain.name</code> is the domain name of the machine that hosts the HBase master server. - <code>YOUR-REALM</code> is the Kerberos realm.

HDFS Connection Properties

Use a Hadoop File System (HDFS) connection to access data in the Hadoop cluster. The HDFS connection is a file system type connection. You can create and manage an HDFS connection in the Administrator tool, Analyst tool, or the Developer tool. HDFS connection properties are case sensitive unless otherwise noted.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

The following table describes HDFS connection properties:

Property	Description
Name	Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. 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.
Description	The description of the connection. The description cannot exceed 765 characters.
Location	The domain where you want to create the connection. Not valid for the Analyst tool.
Type	The connection type. Default is Hadoop File System.
User Name	User name to access HDFS.
NameNode URI	The URI to access HDFS. Use the following format to specify the NameNode URI in Cloudera and Hortonworks distributions: hdfs://<namenode>:<port> Where - <namenode> is the host name or IP address of the NameNode. - <port> is the port that the NameNode listens for remote procedure calls (RPC). Use the following for the NameNode URI for MapR clusters: - maprfs:///

Hive-Verbindungseigenschaften

Verwenden Sie die Hive-Verbindung, um auf Hive-Daten zuzugreifen. Eine Hive-Verbindung ist ein Datenbank-Verbindungstyp. Sie können eine Hive-Verbindung im Administrator Tool, im Analyst Tool oder im Developer Tool erstellen und verwalten. Hive-Verbindungseigenschaften unterscheiden zwischen Groß- und Kleinschreibung, sofern nicht anders angegeben.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Eigenschaften von Hive-Verbindungseigenschaften erläutert:

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 4000 Zeichen enthalten.
Speicherort	Die Domäne, in der Sie die Verbindung erstellen möchten. Nicht gültig für das Analyst Tool.
Typ	Der Verbindungstyp. Wählen Sie „Hive“ aus.
Verbindungsmodi	Hive-Verbindungsmodus. Wählen Sie eine der folgenden Optionen aus: <ul style="list-style-type: none"> - Zum Ausführen von Zuordnungen auf HiveServer2 zugreifen Wählen Sie diese Option, wenn Sie die Verbindung verwenden möchten, um auf das Hive Data Warehouse zuzugreifen. Wenn Sie Hive als Ziel verwenden möchten, müssen Sie die gleiche Verbindung oder eine andere Hive-Verbindung zum Ausführen von Mappings im Hadoop-Cluster aktivieren. - Zum Ausführen von Zuordnungen auf Hive CLI zugreifen Wählen Sie diese Option aus, wenn Sie die Hive CLI zum Ausführen von Zuordnungen im Hadoop-Cluster verwenden möchten.

Eigenschaft	Beschreibung
Benutzername	<p>Benutzername des Benutzers, den der Datenintegrationsdienst zum Ausführen von Mappings im Hadoop-Cluster verwendet. Der Benutzername richtet sich nach der JDBC-Verbindungszeichenfolge, die Sie in der Metadaten- oder Datenzugriffs-Verbindungszeichenfolge für die native Umgebung angegeben haben.</p> <p>Wenn der Hadoop-Cluster MapR verwendet, verwenden Sie einen Betriebssystem-Benutzernamen, der in allen Knoten im Hadoop-Cluster vorhanden ist.</p> <p>Wenn der Hadoop-Cluster Hortonworks HDP verwendet, müssen Sie einen Benutzernamen bereitstellen. Sie können das Benutzerkonto für den Datenintegrationsdienst oder ein Identitätswechsel-Benutzerkonto verwenden.</p> <p>Wenn der Hadoop-Cluster Kerberos-Authentifizierung verwendet, müssen der Prinzipalname der JDBC-Verbindungszeichenfolge und der Benutzername übereinstimmen. Ansonsten hängt der Benutzername vom Verhalten des JDBC-Treibers ab.</p> <p>Wenn der Hadoop-Cluster keine Kerberos-Authentifizierung verwendet, hängt der Benutzername vom Verhalten des JDBC-Treibers ab.</p> <p>Wenn Sie keinen Benutzernamen eingeben, authentifiziert der Hadoop-Cluster Jobs basierend auf den folgenden Kriterien:</p> <ul style="list-style-type: none"> - Der Hadoop-Cluster verwendet keine Kerberos-Authentifizierung. Er authentifiziert Jobs basierend auf dem Benutzernamen des Betriebssystemprofils des Computers, auf dem der Datenintegrationsdienst ausgeführt wird. - Der Hadoop-Cluster verwendet Kerberos-Authentifizierung. Er authentifiziert Jobs basierend auf dem SPN des Datenintegrationsdiensts.
Gemeinsame Attribute in beiden Modi: Umgebungs-SQL	<p>SQL-Befehle zum Einrichten der Hadoop-Umgebung. Im nativen Umgebungstyp führt der Datenintegrationsdienst die Umgebungs-SQL jedes Mal aus, wenn er eine Verbindung zum Hive-Metastore herstellt. Wenn die Hive-Verbindung zum Ausführen von Mappings im Hadoop-Cluster verwendet wird, führt der Datenintegrationsdienst die Umgebungs-SQL am Anfang jeder Hive-Sitzung aus.</p> <p>Die folgenden Regeln und Richtlinien gelten für die Verwendung von Umgebungs-SQL in beiden Verbindungsmodi:</p> <ul style="list-style-type: none"> - 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 <code>hive.aux.jars.path</code> mit allen Einträgen in <code>infapdo.aux.jars.path</code> 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. <p>Wenn die Hive-Verbindung zum Ausführen von Mappings im Hadoop-Cluster verwendet wird, wird nur die Umgebungs-SQL der Hive-Verbindung ausgeführt. Die verschiedenen Umgebungs-SQL-Befehle für die Verbindungen von Hive-Quelle oder -Ziel werden nicht ausgeführt, selbst wenn sich Hive-Quellen und -Ziele in verschiedenen Clustern befinden.</p>

Eigenschaften für den Zugriff auf Hive als Quelle oder Ziel

Die folgende Tabelle beschreibt die Verbindungseigenschaften, die Sie konfigurieren, um auf Hive als Quelle oder Ziel zuzugreifen:

Eigenschaft	Beschreibung
Metadaten-Verbindungszeichenfolge	<p>Die JDBC-Verbindungs-URI für den Zugriff auf die Metadaten des Hadoop-Servers. Diese Eigenschaft ist für HiveServer2 erforderlich.</p> <p>Sie können PowerExchange for Hive zum Kommunizieren mit einem HiveServer-Dienst oder mit einem HiveServer2-Dienst verwenden.</p> <p>Zum Herstellen einer Verbindung zu HiveServer geben Sie den Verbindungsstring im folgenden Format ein:</p> <pre>jdbc:hive://<hostname>:<port>/<db></pre> <p>Wobei</p> <ul style="list-style-type: none">- <code>hostname</code> ist der Name oder die IP-Adresse des Computers, auf dem HiveServer oder HiveServer2 ausgeführt wird.- <code>port</code> ist die Portnummer, auf der HiveServer oder HiveServer2 überwacht.- <code>db</code> der Datenbankname ist, zu der Sie eine Verbindung herstellen möchten. Wenn Sie den Datenbanknamen nicht zur Verfügung stellen, verwendet der Datenintegrationsdienst die standardmäßigen Datenbank-Details. <p>Zum Herstellen einer Verbindung zu HiveServer 2 verwenden Sie das Verbindungsstringformat, das Apache Hive für diese bestimmte Hadoop-Verteilung implementiert. Weitere Informationen über Apache Hive-Verbindungsstringformate finden Sie in der Apache Hive-Dokumentation.</p>
Hive-JDBC-Server umgehen	<p>JDBC-Treibermodus. Aktivieren Sie das Kontrollkästchen zur Verwendung des eingebetteten JDBC-Treibers (eingebetteter Modus).</p> <p>Zur Verwendung des eingebetteten JDBC-Modus führen Sie folgende Aufgaben durch:</p> <ul style="list-style-type: none">- Stellen Sie sicher, dass Hive-Client und Informatica-Dienste auf demselben Rechner installiert sind.- Konfigurieren Sie die Hive-Verbindungseigenschaften zum Ausführen von Mappings im Hadoop-Cluster. <p>Wenn Sie den nicht eingebetteten Modus wählen, müssen Sie den Verbindungszeichenfolge für Datenzugriff konfigurieren.</p> <p>Der eingebettete JDBC-Modus wird dem nicht eingebetteten Modus vorgezogen.</p>
Verbindungszeichenfolge für Datenzugriff	<p>Der Verbindungsstring, der zum Zugriff auf Daten aus dem Hadoop-Datenspeicher verwendet wird.</p> <p>Zum Herstellen einer Verbindung zu HiveServer geben Sie den Verbindungsstring des nicht eingebetteten JDBC-Modus im folgenden Format ein:</p> <pre>jdbc:hive://<hostname>:<port>/<db></pre> <p>Wobei</p> <ul style="list-style-type: none">- <code>hostname</code> ist der Name oder die IP-Adresse des Computers, auf dem HiveServer oder HiveServer2 ausgeführt wird.- <code>port</code> ist die Portnummer, die HiveServer oder HiveServer2 zur Überwachung verwendet.- <code>db</code> die Datenbank ist, zu der Sie eine Verbindung herstellen möchten. Wenn Sie den Datenbanknamen nicht zur Verfügung stellen, verwendet der Datenintegrationsdienst die standardmäßigen Datenbank-Details. <p>Zum Herstellen einer Verbindung zu HiveServer 2 verwenden Sie das Verbindungsstringformat, das Apache Hive für diese bestimmte Hadoop-Verteilung implementiert. Weitere Informationen über Apache Hive-Verbindungsstringformate finden Sie in der Apache Hive-Dokumentation.</p>

Eigenschaften zum Ausführen von Mappings im Hadoop-Cluster

Die folgende Tabelle beschreibt die Hive-Verbindungseigenschaften, die Sie konfigurieren, wenn Sie Hive-Verbindungen verwenden möchten, um Informatica-Mappings im Hadoop-Cluster auszuführen:

Eigenschaft	Beschreibung
Datenbankname	Namespace für Tabellen. Verwenden Sie den Namen <code>default</code> für Tabellen, bei denen kein Datenbankname angegeben wurde. Diese Eigenschaft ist für HiveServer2 erforderlich.
Standard-FS-URI	<p>Die URI für den Zugriff auf das verteilte Standard-Hadoop-Dateisystem. Diese Eigenschaft ist für HiveServer2 erforderlich.</p> <p>Verwenden Sie den folgenden Verbindungs-URI: <code>hdfs://<node name>:<port></code></p> <p>Wobei</p> <ul style="list-style-type: none"> - <code>node name</code> der Hostname oder die IP-Adresse des NameNode ist. - <code>port</code> der Port ist, den NameNode auf Remoteprozeduraufrufe (RPC) abhört. <p>Wenn der Hadoop-Cluster MapR verwendet, verwenden Sie für den Zugriff auf das MapR-Dateisystem die folgende URI: <code>maprfs:///</code></p>
JobTracker/Yarn-Ressourcenmanager-URI	<p>Der Dienst innerhalb von Hadoop, der die MapReduce-Aufgaben an bestimmte Knoten im Cluster sendet.</p> <p>Verwenden Sie das folgende Format: <code><hostname>:<port></code></p> <p>Wobei</p> <ul style="list-style-type: none"> - <code>hostname</code> ist der Hostname oder die IP-Adresse des JobTracker oder des Yarn-Ressourcenmanagers. - <code>port</code> ist der Port, auf dem JobTracker oder der Yarn-Ressourcenmanager auf Remoteprozeduraufrufe (RPC) überwacht. <p>Wenn der Cluster MaPR mit YARN verwendet, verwenden Sie den von <code>yarn.resourcemanager.address</code> in <code>yarn-site.xml</code> angegebenen Wert. Sie können <code>yarn-site.xml</code> im folgenden Verzeichnis auf dem NameNode des Clusters finden: <code>/opt/mapr/hadoop/hadoop-2.5.1/etc/hadoop</code>.</p> <p>MapR mit MapReduce 1 unterstützt einen hochverfügbaren JobTracker. Wenn Sie die MapR-Verteilung mit MapReduce 1 verwenden, definieren Sie den JobTracker-URI im folgenden Format: <code>maprfs:///</code></p>
Hive-Warehouse-Verzeichnis auf HDFS	<p>Der absolute HDFS-Dateipfad der Standarddatenbank für das lokale Cluster-Warehouse. Diese Eigenschaft ist für HiveServer2 erforderlich.</p> <p>Der folgende Dateipfad gibt zum Beispiel ein lokales Warehouse an: <code>/user/hive/warehouse</code></p> <p>Wenn der Metastore-Ausführungsmodus für Cloudera CDH remote ausgeführt wird, muss der Dateipfad dem vom Hive-Metastore-Dienst im Hadoop-Cluster festgelegten Dateipfad entsprechen.</p> <p>Verwenden Sie für MapR den für die Eigenschaft <code>hive.metastore.warehouse.dir</code> angegebenen Wert in <code>hive-site.xml</code>. Sie können <code>hive-site.xml</code> im folgenden Verzeichnis auf dem Knoten finden, der HiveServer2 ausführt: <code>/opt/mapr/hive/hive-0.13/conf</code>.</p>

Eigenschaft	Beschreibung
Erweiterte Hive-/Hadoop-Eigenschaften	<p>Konfiguriert oder überschreibt Hive- oder Hadoop-Cluster-Eigenschaften in hive-site.xml auf dem Computer, auf dem der Datenintegrationsdienst ausgeführt wird. Sie können mehrere Eigenschaften angeben.</p> <p>Verwenden Sie das folgende Format:</p> <pre><property>=<value></pre> <p>Wobei</p> <ul style="list-style-type: none"> - <code>property1</code> ist eine Hive- oder Hadoop-Eigenschaft in hive-site.xml. - <code>value</code> ist der Wert der Hive- oder Hadoop-Eigenschaft. <p>Um mehrere Eigenschaften anzugeben, verwenden Sie <code>&</code> als Trennzeichen für die Eigenschaften.</p> <p>Die maximale Länge für das Format ist 1 MB.</p> <p>Wenn Sie eine erforderliche Eigenschaft für eine Hive-Verbindung eingeben, überschreibt diese die Eigenschaft, die Sie in den erweiterten Hive- bzw. Hadoop-Eigenschaften konfigurieren.</p> <p>Der Datenintegrationsdienst fügt diese Eigenschaften für jeden map-reduce-Job hinzu bzw. legt diese fest. Sie können diese Eigenschaften in der JobConf jedes mapper- oder reducer-Jobs überprüfen. Greifen Sie auf die JobConf jedes Jobs über die Jobtracker-URL unter jedem map-reduce-Job zu.</p> <p>Der Datenintegrationsdienst schreibt Meldungen für diese Eigenschaften in die Datenintegrationsdienst-Protokolle. Die Protokoll-Tracingebene im Datenintegrationsdienst muss so eingestellt sein, dass jede Zeile protokolliert wird. Alternativ dazu kann Verbose-Initialisierungstracing als Protokoll-Tracingebene eingestellt sein.</p> <p>Geben Sie zum Beispiel die folgenden Eigenschaften an, um die Anzahl der reducer-Jobs zur Ausführung eines mapping-Jobs zu begrenzen:</p> <pre>mapred.reduce.tasks=2&hive.exec.reducers.max=10</pre>
Temporärer Tabellen-Komprimierungs-Codec	Hadoop-Komprimierungsbibliothek für einen Komprimierungs-Codec-Klassennamen.
Codec-Klassenname	Codec-Klassenname, der die Datenkomprimierung aktiviert und die Leistung in temporären Staging-Tabellen verbessert.
Metastore-Ausführungsmodus	Steuert, ob eine Verbindung zu einem Remote-Metastore oder einem lokalen Metastore hergestellt wird. Standardmäßig ist „lokal“ ausgewählt. Für einen lokalen Metastore müssen Sie die Metastore-Datenbank-URI, den Treiber, den Benutzernamen und das Passwort angeben. Für einen Remote-Metastore müssen Sie nur die Remote-Metastore-URI angeben.

Eigenschaft	Beschreibung
Metastore-Datenbank-URI	<p>Die JDBC-Verbindungs-URI zum Zugriff auf den Datenspeicher in einer lokalen Metastore-Einrichtung. Verwenden Sie den folgenden Verbindungs-URI:</p> <pre>jdbc:<datastore type>://<node name>:<port>/<database name></pre> <p>wobei</p> <ul style="list-style-type: none"> - <code>node name</code> der Hostname oder die IP-Adresse des Datenspeichers ist. - <code>data store type</code> der Typ des Datenspeichers ist. - <code>port</code> der Port ist, von dem aus der Datenspeicher auf Remoteprozeduraufrufe (RPC) abhört. - <code>database name</code> der Name der Datenbank ist. <p>Die folgende URI gibt zum Beispiel einen lokalen Metastore an, der MySQL als Datenspeicher verwendet:</p> <pre>jdbc:mysql://hostname23:3306/metastore</pre> <p>Verwenden Sie für MapR den für die Eigenschaft <code>javax.jdo.option.ConnectionURL</code> in <code>hive-site.xml</code> angegebenen Wert. <code>hive-site.xml</code> befindet sich im folgenden Verzeichnis auf dem Knoten, auf dem HiveServer 2 ausgeführt wird: <code>/opt/mapr/hive/hive-0.13/conf</code>.</p>
Metastore-Datenbanktreiber	<p>Treiberklassenname für den JDBC-Datenspeicher. Der folgende Klassenname gibt zum Beispiel einen MySQL-Treiber an:</p> <pre>com.mysql.jdbc.Driver</pre> <p>Verwenden Sie für MapR den für die Eigenschaft <code>javax.jdo.option.ConnectionDriverName</code> in <code>hive-site.xml</code> angegebenen Wert. <code>hive-site.xml</code> befindet sich im folgenden Verzeichnis auf dem Knoten, auf dem HiveServer 2 ausgeführt wird: <code>/opt/mapr/hive/hive-0.13/conf</code>.</p>
Metastore-Datenbankbenutzername	<p>Der Benutzername der Metastore-Datenbank.</p> <p>Verwenden Sie für MapR den für die Eigenschaft <code>javax.jdo.option.ConnectionUserName</code> in <code>hive-site.xml</code> angegebenen Wert. <code>hive-site.xml</code> befindet sich im folgenden Verzeichnis auf dem Knoten, auf dem HiveServer 2 ausgeführt wird: <code>/opt/mapr/hive/hive-0.13/conf</code>.</p>
Metastore-Datenbankpasswort	<p>Das Passwort für den Metastore-Benutzernamen.</p> <p>Verwenden Sie für MapR den für die Eigenschaft <code>javax.jdo.option.ConnectionPassword</code> in <code>hive-site.xml</code> angegebenen Wert. <code>hive-site.xml</code> befindet sich im folgenden Verzeichnis auf dem Knoten, auf dem HiveServer 2 ausgeführt wird: <code>/opt/mapr/hive/hive-0.13/conf</code>.</p>
Remote-Metastore-URI	<p>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.</p> <p>Verwenden Sie den folgenden Verbindungs-URI:</p> <pre>thrift://<hostname>:<port></pre> <p>Wobei</p> <ul style="list-style-type: none"> - <code>hostname</code> der Name oder die IP-Adresse des Thrift-Metastore-Servers ist. - <code>port</code> der Port ist, auf dem der Thrift-Server abhört. <p>Verwenden Sie für MapR den für die Eigenschaft <code>hive.metastore.uris</code> in <code>hive-site.xml</code> angegebenen Wert. <code>hive-site.xml</code> befindet sich im folgenden Verzeichnis auf dem Knoten, auf dem HiveServer 2 ausgeführt wird: <code>/opt/mapr/hive/hive-0.13/conf</code>.</p>

HTTP-Verbindungseigenschaften

Verwenden Sie eine HTTP-Verbindung, um eine Verbindung von einer REST-Webdienst-Verbraucher-Umwandlung zu einem Webdienst herzustellen. Die HTTP-Verbindung ist ein Web-Verbindungstyp. Sie erstellen eine HTTP-Verbindung im Developer-Tool. Sie können eine HTTP-Verbindung im Administrator-Tool oder im Developer-Tool verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Eigenschaften von HTTP-Verbindungen erläutert:

Eigenschaft	Beschreibung
Name	Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. 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.
Benutzername	Benutzername, der mit dem Web-Dienst verbunden werden soll. Geben Sie einen Benutzernamen ein, wenn Sie die HTTP-Authentifizierung oder die WS-Security aktiviert haben. Wenn die Web-Dienst-Verbraucher-Umwandlung WS-Security-Ports enthält, erhält die Umwandlung einen dynamischen Benutzernamen durch einen Eingangsport. Der Data Integration Service überschreibt den Benutzernamen, der in der Verbindung definiert ist.
Passwort	Passwort für den Benutzernamen. Geben Sie ein Passwort ein, wenn Sie die HTTP-Authentifizierung oder die WS-Security aktiviert haben. Wenn die Web-Dienst-Verbraucher-Umwandlung WS-Security-Ports enthält, erhält die Umwandlung ein dynamisches Passwort durch einen Eingangsport. Der Data Integration Service überschreibt das Passwort, das in der Verbindung definiert ist.
Endpunkt-URL	URL für den Web-Dienst, auf den zugegriffen werden soll. Der Data Integration Service überschreibt die URL, die in der WSDL-Datei definiert ist. Wenn die Web-Dienst-Verbraucher-Umwandlung einen Endpunkt-URL-Port enthält, erhält die Umwandlung die URL durch einen Eingangsport. Der Data Integration Service überschreibt die URL, die in der Verbindung definiert ist.
Timeout	Anzahl von Sekunden, in der der Data Integration Service auf eine Antwort vom Web-Dienst-Provider wartet, ehe er die Verbindung schließt.

Eigenschaft	Beschreibung
HTTP-Authentifizierungstyp	<p>Art der Benutzer-Authentifizierung via HTTP. Wählen Sie einen der folgenden Werte aus:</p> <ul style="list-style-type: none"> - Keine. Keine Authentifizierung. - Automatisch. Der Data Integration Service wählt den Authentifizierungstyp, den der Web-Dienst-Provider verwendet. - Basis Sie müssen der Domäne des Web-Dienst-Providers einen Benutzernamen und ein Passwort bereitstellen. Der Data Integration Service sendet den Benutzernamen und das Passwort zur Authentifizierung an den Web-Dienst-Provider. - zusammengefasst Sie müssen der Domäne des Web-Dienst-Providers einen Benutzernamen und ein Passwort bereitstellen. Der Data Integration Service generiert eine verschlüsselte Meldungszusammenfassung aus dem Benutzernamen und dem Passwort und sendet diese an den Web-Dienst-Provider. Der Provider generiert einen temporären Wert für den Benutzernamen und das Passwort und speichert diesen in seinem Active Directory auf dem Domänen-Controller. Er vergleicht den Wert mit der Meldungszusammenfassung. Wenn beide übereinstimmen, authentifiziert Sie der Web-Dienst-Provider. - NTLM Sie müssen einen Domänennamen, einen Servernamen oder einen Standardbenutzernamen und ein Passwort bereitstellen. Der Web-Dienst-Provider authentifiziert Sie anhand der Domäne, mit der Sie verbunden sind. Er erhält den Benutzernamen und das Passwort vom Windows Domain Controller und vergleicht sie mit dem Benutzernamen und Passwort, das Sie bereitgestellt haben. Wenn beide übereinstimmen, authentifiziert Sie der Web-Dienst-Provider. Bei der NTLM-Authentifizierung werden keine verschlüsselten Passwörter im Active Directory des Domain Controllers gespeichert.
Trust-Zertifikatsdatei	<p>Die Datei enthält ein Bundle aus vertrauenswürdigen Zertifikaten, die der Data Integration Service verwendet, wenn er das SSL-Zertifikat des Web-Dienstes authentifiziert. Geben Sie den Dateinamen und den kompletten Verzeichnispfad ein.</p> <p>Voreinstellung ist <Informatica-Installationsverzeichnis>/services/shared/bin/ca-bundle.crt.</p>
Clientzertifikat - Dateiname	Clientzertifikat, das der Web-Dienst verwendet, um einen Client zu authentifizieren. Geben Sie die Clientzertifikatsdatei an, wenn der Web-Dienst den Data Integration Service authentifizieren muss.
Clientzertifikat - Passwort	Passwort des Clientzertifikats Geben Sie das Passwort des Clientzertifikats an, wenn der Web-Dienst den Data Integration Service authentifizieren muss.
Clientzertifikat - Typ	<p>Format der Clientzertifikatsdatei. Wählen Sie einen der folgenden Werte aus:</p> <ul style="list-style-type: none"> - PEM. Dateien mit der Dateiendung .pem. - DER. Dateien mit der Dateiendung .cer oder .der <p>Geben Sie den Clientzertifikatstyp an, wenn der Webdienst den Datenintegrationsdienst authentifizieren muss.</p>
Dateiname für privaten Schlüssel	Der private Schlüssel für das Clientzertifikat. Geben Sie den Dateinamen des privaten Schlüssels an, wenn der Web-Dienst den Data Integration Service authentifizieren muss.
Passwort für privaten Schlüssel	Passwort für den privaten Schlüssel des Clientzertifikats. Geben Sie das Passwort des privaten Schlüssels an, wenn der Web-Dienst den Data Integration Service authentifizieren muss.
Privater Schlüsseltyp	Typ des privaten Schlüssels. Der unterstützte Typ ist PEM.

Eigenschaften von IBM DB2-Verbindungen

Verwenden Sie eine IBM DB2-Verbindung für den Zugriff auf IBM DB2. Eine IBM DB2-Verbindung ist eine relationale Datenbankverbindung. Sie können eine IBM DB2-Verbindung im Administrator tool, Developer tool oder Analyst Tool erstellen und verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die DB2-Verbindungseigenschaften beschrieben:

Eigenschaft	Beschreibung
Datenbanktyp	Der Datenbanktyp.
Name	Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. 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 765 Zeichen enthalten.
Benutzername	Der Datenbankbenutzername.
Passwort	Das Passwort für den Datenbankbenutzernamen.
Pass-Through-Sicherheit aktiviert	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 bei der entsprechenden Datenbank anzumelden.
Verbindungszeichenfolge für den Datenzugriff	DB2-Verbindungs-URL für den Zugriff auf Metadaten in der Datenbank. dbname Wobei <code>dbname</code> der im DB2-Client konfigurierte Alias ist.

Eigenschaft	Beschreibung
Eigenschaften für den Metadaten-Zugriff: Verbindungszeichenfolge	<p>Verwenden Sie die folgende URL für die Verbindungszeichenfolge für Metadaten:</p> <pre>jdbc:informatica:db2:// <Hostname>:<Port>;DatabaseName=<Datenbankname></pre> <p>Beim Importieren einer Tabelle werden standardmäßig alle Tabellennamen unterhalb des Namens des Standardschemas angezeigt. Um Tabellen unterhalb eines bestimmten Schemas anstelle des Standardschemas anzuzeigen, können Sie den Namen des Schemas angeben, aus dem Sie die Tabelle importieren möchten. Schließen Sie den Parameter „ischemaName“ in die URL ein, um den Schemanamen anzugeben. Beispiel: Mit der folgenden Syntax wird eine Tabelle aus einem bestimmten Schema importiert:</p> <pre>jdbc:informatica:db2:// <Hostname>:<Port>;DatabaseName=<Datenbankname>;ischemaName=<Schema_Name></pre> <p>Um eine Tabelle in mehreren Schemas zu suchen und zu importieren, können Sie die Namen mehrerer Schemas im Parameter „ischemaName“ festlegen. Beim Namen eines Schemas wird die Groß-/Kleinschreibung beachtet. Trennen Sie Schemanamen durch senkrechte Striche () voneinander. Beispiel: Mit der folgenden Syntax können Sie eine Tabelle in drei Schemas suchen und importieren:</p> <pre>jdbc:informatica:db2:// <Hostname>:<Port>;DatabaseName=<Datenbankname>;ischemaName=<schema_name1> <schema_name2> <schema_name3></pre> <p>Wenn Sie mehrere Schemanamen angeben, müssen Sie die Option Nur Standardschema anzeigen deaktivieren, um die Tabellen unter dem angegebenen Schemanamen anzuzeigen.</p>
AdvancedJDBCSecurityOptions	<p>Datenbankparameter für Metadata-Zugriff auf eine sichere Datenbank. Informatica behandelt den Wert des AdvancedJDBCSecurityOptions-Felds als vertrauliche Daten und speichert die Parameterzeichenfolge als Verschlüsselung.</p> <p>Um eine Verbindung zu einer sicheren Datenbank herzustellen, beziehen Sie die folgenden Parameter mit ein:</p> <ul style="list-style-type: none"> - 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. <p>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.</p> <p>Wenn dieser Parameter auf "false" festgelegt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat nicht. Informatica ignoriert alle Truststore-Informationen, die Sie angeben.</p> <ul style="list-style-type: none"> - 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. <p>Hinweis: Informatica hängt die sichere JDBC-Parameter an die Verbindungszeichenfolge an. Wenn Sie die sicheren JDBC-Parameter direkt in der Verbindungszeichenfolge einschließen, geben Sie keinen Parameter in das Feld AdvancedJDBCSecurityOptions ein.</p>

Eigenschaft	Beschreibung
Eigenschaften für den Datenzugriff: Verbindungszeichenfolge	Die Verbindungszeichenfolge für den Zugriff auf Daten in der Datenbank. Für IBM DB2 ist dies <Datenbankname>
Codepage	Die Codepage, die zum Lesen aus einer Quelldatenbank oder zum Schreiben in eine Zieldatenbank oder Zieldatei verwendet wird.
Umgebungs-SQL	SQL-Befehle zum Einrichten der Datenbankumgebung beim Herstellen einer Verbindung zur Datenbank. Der Datenintegrationsdienst führt die Verbindungsumgebungs-SQL bei jeder Verbindung mit der Datenbank aus.
Transaktions-SQL	SQL-Befehle zum Einrichten der Datenbankumgebung beim Herstellen einer Verbindung zur Datenbank. Der Datenintegrationsdienst führt die Verbindungsumgebungs-SQL zu Beginn jeder Transaktion aus.
Wiederholungsperiode	Diese Eigenschaft ist für die zukünftige Verwendung reserviert.
Tablespace	Der Tablespace-Name der Datenbank.
SQL-Bezeichnerzeichen	Der Zeichentyp, der zur Kennzeichnung von Sonderzeichen und reservierten SQL-Schlüsselwörtern, wie WHERE, verwendet wird. Der Datenintegrationsdienst schließt mit dem ausgewählten Zeichen Sonderzeichen und reservierte SQL-Schlüsselwörter ein. Außerdem nutzt der Datenintegrationsdienst dieses Zeichen für die Eigenschaft „Bezeichner mit gemischter Groß-/Kleinschreibung unterstützen“. Wählen Sie das Zeichen basierend auf der Datenbank in der Verbindung aus.
Bezeichner mit gemischter Groß-/Kleinschreibung unterstützen	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. Diese Option ist standardmäßig deaktiviert.
ODBC-Provider	ODBC. Der Datenbanktyp, zu dem ODBC eine Verbindung herstellt. Geben Sie zur Pushdown-Optimierung den Datenbanktyp an, damit der Datenintegrationsdienst die native Datenbank-SQL generieren kann. Mögliche Werte: - Andere - Sybase - Microsoft_SQL_Server Standardwert ist „Andere“.

Eigenschaften von IBM DB2 für i5/OS-Verbindungen

Verwenden Sie eine IBM DB2 für i5/OS -Verbindung für den Zugriff auf Tabellen in IBM DB2 für i5/OS. Eine IBM DB2 für i5/OS-Verbindung ist ein relationaler Datenbank-Verbindungstyp. Sie können eine IBM DB2 für i5/OS-Verbindung im Administrator-Tool oder im Developer-Tool erstellen und verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Eigenschaften von DB2 für i5/OS-Verbindungen erläutert:

Eigenschaft	Beschreibung
Name	Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. 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 255 Zeichen enthalten.
Verbindungstyp	Der Verbindungstyp (DB2I).
Benutzername	Ein Datenbankbenutzername.
Passwort	Ein Passwort für den angegebenen Benutzernamen oder eine gültige PowerExchange-Passphrase. Eine PowerExchange-Passphrase darf eine Länge von 9 bis 31 Zeichen haben und kann die folgenden Zeichen enthalten: <ul style="list-style-type: none"> - Groß- und Kleinbuchstaben - Die Ziffern 0 bis 9 - Leerzeichen - Die folgenden Sonderzeichen: ' - ; # \ , . / ! % & * () _ + { } : @ < > ? <p>Hinweis: Das erste Zeichen ist ein Apostroph.</p> <p>Passphrasen dürfen keine einfachen Anführungszeichen ('), doppelten Anführungszeichen (") oder Währungssymbole enthalten.</p> <p>Stellen Sie vor der Verwendung von Passphrasen sicher, dass der PowerExchange-Listenerdienst im DBMOVER-Mitglied mit der Sicherheitseinstellung SECURITY=(1,N) oder höher ausgeführt wird. Weitere Informationen finden Sie im Abschnitt zur SECURITY-Anweisung im <i>PowerExchange-Referenzhandbuch</i>.</p>
Pass-Through-Sicherheit aktiviert	Aktiviert Pass-Through-Sicherheit für die Verbindung.
Datenbankname	Der Name der Datenbankinstanz.
Speicherort	Knotenname des Speicherorts des PowerExchange-Listenerdiensts, der mit DB2 verbunden ist. Der Knotenname ist im ersten Parameter der NODE-Anweisung in der PowerExchange-Konfigurationsdatei „dbmover.cfg“ definiert.
Umgebungs-SQL	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.

Eigenschaft	Beschreibung
Datenbankdateiüberschreibungen	<p>Gibt die i5/OS-Datenbankdateiüberschreibung im folgenden Format an:</p> <pre>from_file/to_library/to_file/to_member</pre> <p>wobei</p> <ul style="list-style-type: none"> - <i>from_file</i> ist die zu überschreibende Datei. - <i>to_library</i> ist die zu verwendende neue Bibliothek. - <i>to_file</i> ist die zu verwendende Datei in der neuen Bibliothek. - <i>to_member</i> optional ist und das zu verwendende Elemente in der neuen Bibliothek und Datei darstellt. *FIRST wird verwendet, wenn keine Angabe gemacht wird. <p>Sie können bis zu acht eindeutige Dateiüberschreibungen für eine einzelne Verbindung angeben. Eine einfache Überschreibung gilt für eine einzelne Datei oder ein einzelnes Ziel. Wenn Sie mehr als eine Dateiüberschreibung angeben möchten, umschließen Sie die Zeichenfolge der Dateiüberschreibungen mit doppelten Anführungszeichen (") und nehmen Sie ein Leerzeichen zwischen den Dateiüberschreibungen auf.</p> <p>Hinweis: Wenn Sie sowohl das Bibliotheksverzeichnis als auch Datenbankdateiüberschreibungen angeben und beide eine Tabelle enthalten, hat der Wert der Datenbankdateiüberschreibungen Priorität.</p>
Bibliotheksverzeichnis	<p>Liste der Bibliotheken, die PowerExchange sucht, um den Tabellennamen für Auswählen-, Einfügen-, Löschen- oder Aktualisieren-Anweisungen zu bestimmen. PowerExchange sucht die Liste, wenn der Tabellename nicht angegeben ist.</p> <p>Bibliotheken müssen durch Semikolon getrennt sein.</p> <p>Hinweis: Wenn Sie sowohl das Bibliotheksverzeichnis als auch Datenbankdateiüberschreibungen angeben und beide eine Tabelle enthalten, hat der Wert der Datenbankdateiüberschreibungen Priorität.</p>
Codepage	Die Codepage, die zum Lesen aus einer Quelldatenbank oder zum Schreiben in eine Zieldatenbank oder Zieldatei verwendet wird.
Zu verwendendes SQL-Kennungszeichen	Der Zeichentyp, der verwendet wird, um Sonderzeichen und reservierte SQL-Schlüsselwörter wie WHERE zu kennzeichnen. Der Datenintegrationsdienst schließt mit dem Identifizierzeichen Sonderzeichen und reservierte SQL-Schlüsselwörter ein. Außerdem nutzt der Datenintegrationsdienst dieses Zeichen zur Unterstützung der Eigenschaft für IDs mit gemischter Groß- und Kleinschreibung .
Unterstützte IDs mit gemischter Groß-/Kleinschreibung	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. Diese Option ist standardmäßig deaktiviert.
Isolationsebene	<p>Commit-Bereich der Transaktion. Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> - Keine - CS. Cursorstabilität. - RR. Repeatable Read. - CHG. Ändern. - ALL <p>Der Standardwert ist CS.</p>

Eigenschaft	Beschreibung
Verschlüsselungstyp	<p>Optional. Der Verschlüsselungstyp, den der Datenintegrationsdienst verwendet. Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> - Keine - RC2 - DES <p>Der Standardwert ist „Keine“.</p> <p>Hinweise:</p> <ul style="list-style-type: none"> - Informatica empfiehlt die Verwendung der SSL (Secure Sockets Layer)-Authentifizierung, anstatt den Verschlüsselungstyp und die Level-Verbindungseigenschaften oder die ENCRYPT- und ENCRYPTLEVEL-Anweisungen in der DBMOVER-Konfigurationsdatei zu konfigurieren. Die SSL-Authentifizierung bietet eine striktere Sicherheit und wird von diversen Informatica-Produkten verwendet. <p>Weitere Informationen zum Implementieren der SSL-Authentifizierung in einem PowerExchange-Netzwerk finden Sie im <i>PowerExchange-Referenzhandbuch</i>.</p> <ul style="list-style-type: none"> - Die Werte, die Sie für die Verbindungsattribute Verschlüsselungstyp und Level auswählen, setzen die Werte in den ENCRYPT- und ENCRYPTLEVEL-Anweisungen außer Kraft, wenn sie in der DBMOVER-Konfigurationsdatei auf dem Integrationsdienst-Rechner definiert wurden. Zum Aktivieren der Verschlüsselung für ein Mapping müssen Sie die geeigneten Verbindungsattribute auswählen.
Verschlüsselungsebene	<p>Wenn Sie RC2 oder DES als Verschlüsselungstyp ausgewählt haben, wählen Sie eine der folgenden Optionen, um die Verschlüsselungsebene anzugeben, die der Datenintegrationsdienst verwendet:</p> <ul style="list-style-type: none"> - 1. Verwenden Sie einen 56-Bit-Verschlüsselungsschlüssel für DES und RC2. - 2. Verwenden Sie einen dreifachen 168-Bit-Verschlüsselungsschlüssel für DES und einen 64-Bit-Verschlüsselungsschlüssel für RC2. - 3. Verwenden Sie einen dreifachen 168-Bit-Verschlüsselungsschlüssel für DES und einen 128-Bit-Verschlüsselungsschlüssel für RC2. <p>Diese Option wird ignoriert, wenn Sie keinen Verschlüsselungstyp auswählen.</p> <p>Der Standardwert ist 1.</p>
Pacing-Größe	<p>Optional. Menge der Daten, die das Quellsystem an den PowerExchange-Listenerdienst übergeben kann. Legen Sie die Pacing-Größe fest, wenn eine externe Anwendung, eine Datenbank oder der Knoten mit dem Datenintegrationsdienst einen Engpass darstellt. Verwenden Sie niedrigere Werte für schnellere Leistung.</p> <p>Der Mindest- und Standardwert ist 0. Ein Wert 0 bietet die beste Leistung.</p>
Als Zeilen interpretieren	<p>Optional. Wählen Sie diese Option, um die Pacing-Größe als Anzahl von Zeilen anzugeben. Löschen Sie diese Option, um die Pacing-Größe in Kilobyte anzugeben. Diese Option ist standardmäßig nicht ausgewählt und die Pacing-Größe wird in Kilobyte angegeben.</p>
Komprimierung	<p>Optional. Wählen Sie diese Option zum Aktivieren der Quelldatenkomprimierung aus. Durch die Komprimierung von Daten können Sie die Menge der Daten verringern, die Informatica-Anwendungen über das Netzwerk senden. Standardmäßig ist diese Option nicht ausgewählt und die Komprimierung ist deaktiviert.</p>
Array-Größe	<p>Optional. Die Anzahl der Datensätze im Speicher-Array für die Worker-Threads. Diese Option kann angewendet werden, wenn Sie die Option Worker-Threads auf einen Wert größer als 0 setzen. Gültige Werte sind 25 bis 100.000. Der Standardwert ist 25.</p>

Eigenschaft	Beschreibung
Schreibmodus	<p>Optional. Modus, in dem der Datenintegrationsdienst Daten zum PowerExchange-Listenerdienst sendet. Wählen Sie einen der folgenden Schreibmodi aus:</p> <ul style="list-style-type: none"> - CONFIRMWRITEON. Sendet Daten an den PowerExchange-Listenerdienst und wartet auf eine Antwort, bevor weitere Daten gesendet werden. Wählen Sie diese Option aus, wenn die Fehlerbehebung Priorität hat. Diese Option kann jedoch zu Leistungseinbußen führen. - CONFIRMWRITEOFF. Sendet Daten an den PowerExchange-Listenerdienst, ohne auf eine Antwort zu warten. Verwenden Sie diese Option, wenn Sie die Zieltabelle im Fall eines Fehlers erneut laden können. - ASYNCHRONOUSWITHFAULTTOLERANCE. Sendet Daten an den PowerExchange-Listenerdienst, ohne auf eine Antwort zu warten. Diese Option aktiviert außerdem die Fehlererkennung. Diese Option kombiniert die Geschwindigkeit von CONFIRMWRITEOFF und die Datenintegrität von CONFIRMWRITEON. <p>Der Standardwert ist CONFIRMWRITEON.</p>
Ablehnungsdatei	<p>Überschreibt das Standard-Präfix von PWXR für die verworfene Datei. PowerExchange erstellt die Ablehnungsdatei auf dem Zielcomputer, wenn der Schreibmodus auf ASYNCHRONOUSWITHFAULTTOLERANCE gesetzt ist. Geben Sie PWXDISABLE ein, um die Erstellung der Ablehnungsdateien zu verhindern.</p>

Eigenschaften von IBM DB2 für z/OS-Verbindungen

Verwenden Sie eine IBM DB2 für z/OS-Verbindung für den Zugriff auf Tabellen in IBM DB2 für z/OS. Eine IBM DB2 für z/OS-Verbindung ist ein relationaler Datenbank-Verbindungstyp. Sie können eine IBM DB2 für z/OS-Verbindung im Administrator-Tool oder im Developer-Tool erstellen und verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Eigenschaften von DB2 für z/OS-Verbindungen erläutert:

Eigenschaft	Beschreibung
Name	<p>Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten:</p> <p>~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /</p>
ID	<p>Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.</p>
Beschreibung	<p>Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 255 Zeichen enthalten.</p>
Verbindungstyp	<p>Verbindungstyp (DB2Z)</p>

Eigenschaft	Beschreibung
Benutzername	Datenbankbenutzername.
Passwort	<p>Passwort für den angegebenen Benutzernamen oder eine gültige PowerExchange-Passphrase.</p> <p>Eine PowerExchange-Passphrase kann 9 bis 128 Zeichen lang sein und die folgenden Zeichen enthalten:</p> <ul style="list-style-type: none"> - Groß- und Kleinbuchstaben - Die Ziffern 0 bis 9 - Leerzeichen - Die folgenden Sonderzeichen: ' - ; # \ , . / ! % & * () _ + { } : @ < > ? <p>Hinweis: Das erste Zeichen ist ein Apostroph.</p> <p>Passphrasen dürfen keine einfachen Anführungszeichen (') , doppelten Anführungszeichen (") oder Währungssymbole enthalten.</p> <p>Stellen Sie vor der Verwendung von Passphrasen sicher, dass der PowerExchange-Listenerdienst im DBMOVER-Mitglied mit der Sicherheitseinstellung SECURITY=(1,N) oder höher ausgeführt wird. Weitere Informationen finden Sie im Abschnitt zur SECURITY-Anweisung im <i>PowerExchange-Referenzhandbuch</i>.</p> <p>Die zulässigen Zeichen beim Beenden von IBM IRRPHREX haben keine Auswirkungen auf die zulässigen Zeichen in PowerExchange-Passphrasen.</p> <p>Hinweis: Eine gültige RACF-Passphrase kann bis zu 100 Zeichen lang sein. PowerExchange schneidet Passphrasen mit mehr als 100 Zeichen ab, wenn diese zur Validierung an RACF übergeben werden.</p>
Pass-Through-Sicherheit aktiviert	Aktiviert Pass-Through-Sicherheit für die Verbindung.
DB2-Subsystem-ID	Name des DB2-Subsystems.
Speicherort	Knotenname des Speicherorts des PowerExchange-Listenerdiensts, der mit DB2 verbunden ist. Der Knotenname ist im ersten Parameter der NODE-Anweisung in der PowerExchange-Konfigurationsdatei „dbmover.cfg“ definiert.
Umgebungs-SQL	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.
Korrelations-ID	Mit dem Präfix PWX zu verknüpfender Wert für die Bildung der DB2-Korrelations-ID bei DB2-Anfragen.
Codepage	Codepage, die zum Lesen aus einer Quell-Datenbank oder zum Schreiben auf eine Target-Datenbank oder -Datei verwendet wird.
Zu verwendendes SQL-Kennungszeichen	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. Außerdem nutzt der Datenintegrationsdienst dieses Zeichen zur Unterstützung der Eigenschaft für IDs mit gemischter Groß- und Kleinschreibung .
Unterstützte IDs mit gemischter Groß-/Kleinschreibung	Wählen Sie diese Option, wenn der Datenintegrationsdienst Tabellen-, Ansichts-, Schema-, Synonym- und Spaltennamen beim Generieren und Ausführen von SQL gegen diese Objekte in der Verbindung mit Kennungszeichen umgeben soll. Wählen Sie diese Option aus, wenn für die Objektnamen gemischte Groß-/Kleinschreibung oder Kleinschreibung gilt. Diese Option ist standardmäßig deaktiviert.

Eigenschaft	Beschreibung
Verschlüsselungstyp	<p>Optional. Der Verschlüsselungstyp, den der Datenintegrationsdienst verwendet. Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> - Keine - RC2 - DES <p>Der Standardwert ist „Keine“.</p> <p>Hinweise:</p> <ul style="list-style-type: none"> - Informatica empfiehlt die Verwendung der SSL (Secure Sockets Layer)-Authentifizierung, anstatt den Verschlüsselungstyp und die Level-Verbindungseigenschaften oder die ENCRYPT- und ENCRYPTLEVEL-Anweisungen in der DBMOVER-Konfigurationsdatei zu konfigurieren. Die SSL-Authentifizierung bietet eine striktere Sicherheit und wird von diversen Informatica-Produkten verwendet. <p>Weitere Informationen zum Implementieren der SSL-Authentifizierung in einem PowerExchange-Netzwerk finden Sie im <i>PowerExchange-Referenzhandbuch</i>.</p> <ul style="list-style-type: none"> - Die Werte, die Sie für die Verbindungsattribute Verschlüsselungstyp und Level auswählen, setzen die Werte in den ENCRYPT- und ENCRYPTLEVEL-Anweisungen außer Kraft, wenn sie in der DBMOVER-Konfigurationsdatei auf dem Integrationsdienst-Rechner definiert wurden. Zum Aktivieren der Verschlüsselung für ein Mapping müssen Sie die geeigneten Verbindungsattribute auswählen.
Verschlüsselungsebene	<p>Wenn Sie RC2 oder DES als Verschlüsselungstyp ausgewählt haben, wählen Sie eine der folgenden Optionen, um die Verschlüsselungsebene anzugeben, die der Datenintegrationsdienst verwendet:</p> <ul style="list-style-type: none"> - 1. Verwenden Sie einen 56-Bit-Verschlüsselungsschlüssel für DES und RC2. - 2. Verwenden Sie einen dreifachen 168-Bit-Verschlüsselungsschlüssel für DES und einen 64-Bit-Verschlüsselungsschlüssel für RC2. - 3. Verwenden Sie einen dreifachen 168-Bit-Verschlüsselungsschlüssel für DES und einen 128-Bit-Verschlüsselungsschlüssel für RC2. <p>Diese Option wird ignoriert, wenn Sie keinen Verschlüsselungstyp auswählen.</p> <p>Der Standardwert ist 1.</p>
Pacing-Größe	<p>Optional. Menge der Daten, die das Quellsystem an den PowerExchange-Listenerdienst übergeben kann. Legen Sie die Pacing-Größe fest, wenn eine externe Anwendung, eine Datenbank oder der Knoten mit dem Datenintegrationsdienst einen Engpass darstellt. Verwenden Sie niedrigere Werte für schnellere Leistung.</p> <p>Der Mindest- und Standardwert ist 0. Ein Wert 0 bietet die beste Leistung.</p>
Als Zeilen interpretieren	<p>Optional. Wählen Sie diese Option, um die Pacing-Größe als Anzahl von Zeilen anzugeben. Löschen Sie diese Option, um die Pacing-Größe in Kilobyte anzugeben. Diese Option ist standardmäßig nicht ausgewählt und die Pacing-Größe wird in Kilobyte angegeben.</p>
Komprimierung	<p>Optional. Wählen Sie diese Option zum Aktivieren der Quelldatenkomprimierung aus. Durch die Komprimierung von Daten können Sie die Menge der Daten verringern, die Informatica-Anwendungen über das Netzwerk senden. Standardmäßig ist diese Option nicht ausgewählt und die Komprimierung ist deaktiviert.</p>
Offload-Verarbeitung	<p>Optional. Steuert, ob für die Verarbeitung von Stapeldaten vom Quellcomputer zum Datenintegrationsdienst-Computer Offload-Verarbeitung verwendet werden soll. Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> - AUTO. Der Datenintegrationsdienst bestimmt, ob Offload-Verarbeitung verwendet werden soll. - Ja. Offload-Verarbeitung wird verwendet. - Nein. Offload-Verarbeitung wird nicht verwendet. <p>Der Standardwert ist Nein.</p>

Eigenschaft	Beschreibung
Worker-Threads	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.
Array-Größe	Optional. Die Anzahl der Datensätze im Speicher-Array für die Worker-Threads. Diese Option kann angewendet werden, wenn Sie die Option Worker-Threads auf einen Wert größer als 0 setzen. Gültige Werte sind 1 bis 100.000. Der Standardwert ist 25.
Schreibmodus	<p>Modus, in dem der Datenintegrationsdienst Daten zum PowerExchange-Listenerdienst sendet. Konfigurieren Sie einen der folgenden Schreibmodi:</p> <ul style="list-style-type: none"> - CONFIRMWRITEON. Sendet Daten an den PowerExchange-Listenerdienst und wartet auf eine Antwort, bevor weitere Daten gesendet werden. Wählen Sie diese Option, wenn die Fehlerbehebung Priorität hat. Diese Option kann die Leistung verringern. - CONFIRMWRITEOFF. Sendet Daten an den PowerExchange-Listenerdienst, ohne auf eine Antwort zu warten. Verwenden Sie diese Option, wenn Sie die Zieltabelle im Fall eines Fehlers erneut laden können. - ASYNCHRONOUSWITHFAULTTOLERANCE. Sendet Daten an den PowerExchange-Listenerdienst, ohne auf eine Antwort zu warten. Diese Option bietet auch die Möglichkeit zur Fehlererkennung. Hiermit wird die Geschwindigkeit von Confirm Write Off mit der Datenintegrität von Confirm Write On kombiniert. <p>Der Standardwert ist CONFIRMWRITEON.</p>
Ablehnungsdatei	Überschreibt das Standard-Präfix von PWXR für die verworfene Datei. PowerExchange erstellt die Ablehnungsdatei auf dem Zielcomputer, wenn der Schreibmodus auf ASYNCHRONOUSWITHFAULTTOLERANCE gesetzt ist. Geben Sie PWXDISABLE ein, um eine Erstellung von Ablehnungsdateien zu verhindern.

IMS-Verbindungseigenschaften

Verwenden Sie eine IMS-Verbindung, um auf eine IMS-Datenbank zuzugreifen. Die IMS-Verbindung ist eine nicht-relationaler Mainframe-Datenbank-Verbindungstyp. Der Datenintegrationsdienst stellt über PowerExchange eine Verbindung mit IMS her. Sie erstellen eine IMS-Verbindung im Developer-Tool. Sie können eine IMS-Verbindung im Administrator-Tool oder im Developer-Tool verwalten.

In der folgenden Tabelle werden die Eigenschaften von IMS-Verbindungen erläutert:

Option	Beschreibung
Speicherort	Knotenname für den Speicherort des PowerExchange-Listenerdiensts, der eine Verbindung zu IMS herstellt. Der Knotenname ist im ersten Parameter der NODE-Anweisung in der PowerExchange-Konfigurationsdatei „dbmover.cfg“ definiert.
Benutzername	Benutzername für die Datenbank

Option	Beschreibung
Passwort	<p>Passwort für den angegebenen Datenbankbenutzernamen oder eine gültige PowerExchange-Passphrase.</p> <p>Eine PowerExchange-Passphrase kann 9 bis 128 Zeichen lang sein und die folgenden Zeichen enthalten:</p> <ul style="list-style-type: none"> - Groß- und Kleinbuchstaben - Die Zahlen 0 bis 9 - Leerzeichen - Die folgenden Sonderzeichen: ' - ; # \ , . / ! % & * () _ + { } : @ < > ? <p>Hinweis: Das erste Zeichen ist ein Apostroph.</p> <p>Passphrasen dürfen keine einfachen Anführungszeichen ('), doppelten Anführungszeichen (") oder Währungssymbole enthalten.</p> <p>Die zulässigen Zeichen beim Beenden von IBM IRRPHREX haben keine Auswirkungen auf die zulässigen Zeichen in PowerExchange-Passphrasen.</p> <p>Hinweis: Eine gültige RACF-Passphrase kann bis zu 100 Zeichen enthalten. PowerExchange schneidet Passphrases mit mehr als 100 Zeichen ab, wenn diese zur Validierung an RACF übergeben werden.</p> <p>Um Passphrases für IMS-Verbindungen zu verwenden, stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind:</p> <ul style="list-style-type: none"> - Der PowerExchange-Listenedienst muss mit der Sicherheitseinstellung SECURITY=(1,N) oder höher im DBMOVER-Mitglied ausgeführt werden. Weitere Informationen finden Sie unter „SECURITY-Anweisung“ im <i>PowerExchange-Referenzhandbuch</i>. - Sie müssen ODBA-Zugriff auf IMS wie im <i>PowerExchange-Navigator-Benutzerhandbuch</i> 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.
Codepage	<p>Erforderlich. Name der Codepage für das Lesen aus oder Schreiben in die Datenquelle. Normalerweise ist dieser Wert ein ISO-Codepage-Name, z. B. ISO-8859-6.</p>
Pass-Through-Sicherheit aktiviert	<p>Aktiviert Pass-Through-Sicherheit für die Verbindung.</p>

Option	Beschreibung
Verschlüsselungstyp	<p>Der Verschlüsselungstyp, den der Datenintegrationsdienst verwendet. Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> - Keine - RC2 - DES <p>Standardwert ist „Keine“.</p> <p>Hinweise:</p> <ul style="list-style-type: none"> - Informatica empfiehlt die Verwendung der SSL (Secure Sockets Layer)-Authentifizierung, anstatt den Verschlüsselungstyp und die Level-Verbindungseigenschaften oder die ENCRYPT- und ENCRYPTLEVEL-Anweisungen in der DBMOVER-Konfigurationsdatei zu konfigurieren. Die SSL-Authentifizierung bietet eine striktere Sicherheit und wird von diversen Informatica-Produkten verwendet. <p>Weitere Informationen zum Implementieren der SSL-Authentifizierung in einem PowerExchange-Netzwerk finden Sie im <i>PowerExchange-Referenzhandbuch</i>.</p> <ul style="list-style-type: none"> - Die Werte, die Sie für die Verbindungsattribute Verschlüsselungstyp und Level auswählen, setzen die Werte in den ENCRYPT- und ENCRYPTLEVEL-Anweisungen außer Kraft, wenn sie in der DBMOVER-Konfigurationsdatei auf dem Integrationsdienst-Rechner definiert wurden. Zum Aktivieren der Verschlüsselung für ein Mapping müssen Sie die geeigneten Verbindungsattribute auswählen.
[Encryption]-Ebene	<p>Wählen Sie bei Auswahl von RC2 oder DES für Verschlüsselungstyp eine der folgenden Optionen aus, um die Verschlüsselungsebene anzugeben, die der Datenintegrationsdienst verwendet:</p> <ul style="list-style-type: none"> - 1. Verwenden Sie einen 56-Bit-Verschlüsselungsschlüssel für DES und RC2. - 2. Verwenden Sie einen dreifachen 168-Bit-Verschlüsselungsschlüssel für DES und einen 64-Bit-Verschlüsselungsschlüssel für RC2. - 3. Verwenden Sie einen dreifachen 168-Bit-Verschlüsselungsschlüssel für DES und einen 128-Bit-Verschlüsselungsschlüssel für RC2. <p>Diese Option wird ignoriert, wenn Sie keinen Verschlüsselungstyp auswählen.</p> <p>Standard ist 1.</p>
Pacing-Größe	<p>Optional. Menge der Daten, die das Quellsystem an den PowerExchange-Listenerdienst übergeben kann. Legen Sie die Pacing-Größe fest, wenn eine externe Anwendung, eine Datenbank oder der Knoten mit dem Datenintegrationsdienst einen Engpass darstellt. Verwenden Sie niedrigere Werte für schnellere Leistung.</p> <p>Der Mindest- und Standardwert ist 0. Der Wert 0 bietet die beste Leistung.</p>
Als Zeilen interpretieren	<p>Optional. Wählen Sie diese Option, um die Pacing-Größe als Anzahl von Zeilen anzugeben. Löschen Sie diese Option, um die Pacing-Größe in Kilobyte anzugeben. Diese Option ist standardmäßig nicht ausgewählt und die Pacing-Größe wird in Kilobyte angegeben.</p>
Komprimierung	<p>Optional. Wählen Sie diese Option zum Aktivieren der Quelldatenkomprimierung aus. Durch die Komprimierung von Daten können Sie die Menge der Daten verringern, die Informatica-Anwendungen über das Netzwerk senden. Standardmäßig ist diese Option nicht ausgewählt und die Komprimierung ist deaktiviert.</p>
Offload-Verarbeitung	<p>Optional. Steuert, ob für die Verarbeitung von Stapeldaten vom Quellcomputer zum Datenintegrationsdienst-Computer Offload-Verarbeitung verwendet werden soll. Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> - AUTO. Der Datenintegrationsdienst bestimmt, ob Offload-Verarbeitung verwendet werden soll. - Ja. Offload-Verarbeitung wird verwendet. - Nein. Offload-Verarbeitung wird nicht verwendet. <p>Der Standardwert ist AUTO.</p>

Option	Beschreibung
Worker-Threads	Optional. Anzahl der vom Datenintegrationsdienst verwendeten Threads, um Stapeldaten bei aktivierter Offload-Verarbeitung zu verarbeiten. Um eine optimale Leistung zu erzielen, darf 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 deaktiviert.
Array-Größe	Optional. Die Anzahl der Datensätze im Speicher-Array für die Worker-Threads. Diese Option kann verwendet werden, wenn Sie die Option Worker-Threads auf einen Wert größer als 0 festlegen. Gültige Werte sind 1 bis 100.000. Standardwert ist 25.
Schreibmodus	Optional. Modus, in dem der Datenintegrationsdienst Daten zum PowerExchange-Listenerdienst sendet. Wählen Sie einen der folgenden Schreibmodi aus: <ul style="list-style-type: none"> - CONFIRMWRITEON. Sendet Daten an den PowerExchange-Listenerdienst und wartet auf eine Antwort, bevor weitere Daten gesendet werden. Wählen Sie diese Option aus, wenn die Fehlerbehebung Priorität hat. Diese Option kann jedoch zu Leistungseinbußen führen. - CONFIRMWRITEOFF. Sendet Daten an den PowerExchange-Listenerdienst, ohne auf eine Antwort zu warten. Verwenden Sie diese Option, wenn Sie die Zieltabelle im Fall eines Fehlers erneut laden können. - ASYNCHRONOUSWITHFAULTTOLERANCE. Sendet Daten an den PowerExchange-Listenerdienst, ohne auf eine Antwort zu warten. Diese Option aktiviert außerdem die Fehlererkennung. Diese Option kombiniert die Geschwindigkeit von CONFIRMWRITEOFF und die Datenintegrität von CONFIRMWRITEON. Der Standardwert ist CONFIRMWRITEON.

Propriedades da Conexão do JDBC

É possível usar uma conexão JDBC para acessar tabelas em um banco de dados. É possível criar e gerenciar uma conexão JDBC na ferramenta Administrator, na ferramenta Developer ou na ferramenta Analyst.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

A tabela a seguir descreve as propriedades da conexão do JDBC:

Propriedade	Descrição
Tipo de Banco de Dados	O tipo de banco de dados.
Nome	Nome da conexão. O nome não diferencia maiúsculas de minúsculas e deve ser exclusivo no domínio. O nome não pode exceder 128 caracteres, conter espaços nem conter os seguintes caracteres especiais: ~ ` ! \$ % ^ & * () - + = { [] \ : ; " ' < , > . ? /
ID	String que o Serviço de Integração de Dados usa para identificar a conexão. O ID não diferencia maiúsculas de minúsculas. Ele deve ser de 255 caracteres ou menos e deve ser exclusivo no domínio. Você não pode alterar essa propriedade após criar a conexão. O valor padrão é o nome da conexão.
Descrição	A descrição da conexão. A descrição não pode conter mais de 765 caracteres.
Nome de Usuário	O nome de usuário do banco de dados.

Propriedade	Descrição
Senha	A senha do nome de usuário do banco de dados.
Nome da Classe do Driver JDBC	<p>O nome da classe do driver JDBC.</p> <p>A seguinte lista fornece o nome de classe de driver que você pode inserir para o tipo de banco de dados aplicável:</p> <ul style="list-style-type: none"> - Nome de classe de driver DataDirect JDBC para Oracle: com.informatica.jdbc.oracle.OracleDriver - Nome de classe de driver DataDirect JDBC para IBM DB2: com.informatica.jdbc.db2.DB2Driver - Nome de classe de driver DataDirect JDBC para Microsoft SQL Server: com.informatica.jdbc.sqlserver.SQLServerDriver - Nome de classe de driver DataDirect JDBC para Sybase ASE: com.informatica.jdbc.sybase.SybaseDriver - Nome de classe de driver DataDirect JDBC para Informix: com.informatica.jdbc.informix.InformixDriver - Nome de classe de driver DataDirect JDBC para MySQL: com.informatica.jdbc.mysql.MySQLDriver <p>Para obter mais informações sobre qual classe de driver usar com bancos de dados específicos, consulte a documentação do fornecedor.</p>
Cadeia de Conexão	<p>A cadeia de conexão para se conectar ao banco de dados. Use a seguinte cadeia de conexão:</p> <pre>jdbc:<subprotocol>:<subname></pre>
SQL de Ambiente	Opcional. Insira os comandos SQL para definir o ambiente do banco de dados quando você se conecta ao banco de dados. O Serviço de Integração de Dados executa o SQL de ambiente de conexão ao se conectar ao banco de dados.
Transação SQL	Opcional. Insira os comandos SQL para definir o ambiente do banco de dados quando você se conecta ao banco de dados. O Serviço de Integração de Dados executa o SQL de ambiente de conexão no início de cada transação.
Caractere do Identificador SQL	O tipo de caractere usado para identificar caracteres especiais e palavras-chave SQL reservadas, como WHERE. O Serviço de Integração de Dados coloca o caractere selecionado em torno de caracteres especiais e palavras-chave SQL reservadas. O Serviço de Integração de Dados também usa esse caractere para a propriedade Suporte a identificadores de letras maiúsculas e minúsculas.s.
Suporte a Identificadores com Letras Maiúsculas e Minúsculas	Quando ativado, o Serviço de Integração de Dados coloca o identificador de caracteres em torno de nomes de tabela, exibição, esquema, sinônimo e coluna durante a geração e a execução de SQL em relação a esses objetos na conexão. Use se os objetos tiverem nomes com maiúsculas e minúsculas misturadas ou apenas minúsculas. Por padrão, essa opção não é selecionada.
Segurança de passagem ativada	Ativa a segurança de passagem da conexão. Quando você ativa a segurança de passagem de uma conexão, o domínio usa o nome de usuário e a senha do cliente para fazer logon no banco de dados correspondente, em vez das credenciais definidas no objeto de conexão.

Propriedade	Descrição
Propriedades de Acesso a Metadados: Cadeia de Conexão	<p>A URL de conexão JDBC usada para acessar metadados do banco de dados.</p> <p>A seguinte lista fornece a cadeia de conexão que você pode inserir para o tipo de banco de dados aplicável:</p> <ul style="list-style-type: none"> - Driver DataDirect JDBC para Oracle: jdbc:informatica:oracle://<hostname>:<port>;SID=<sid> - Driver DataDirect JDBC para IBM DB2: jdbc:informatica:db2:// <hostname>:<port>;DatabaseName=<database name> - Driver DataDirect JDBC para Microsoft SQL Server: jdbc:informatica:sqlserver:// <host>:<port>;DatabaseName=<database name> - Driver DataDirect JDBC para Sybase ASE: jdbc:informatica:sybase:// <host>:<port>;DatabaseName=<database name> - Driver DataDirect JDBC para Informix: jdbc:informatica:informix:// <host>:<port>;informixServer=<informix server name>;DatabaseName=<database name> - Driver DataDirect JDBC para MySQL: jdbc:informatica:mysql://<host>:<port>;DatabaseName=<database name> <p>Para obter mais informações sobre a cadeia de conexão a ser usada para bancos de dados específicos, consulte a documentação do fornecedor para sintaxe da URL.</p>
AdvancedJDBCSecurityOptions	<p>Os parâmetros de banco de dados para acesso de metadados a um banco de dados seguro. A Informatica trata o valor do campo AdvancedJDBCSecurityOptions como dados confidenciais e armazena a cadeia do parâmetro criptografada.</p> <p>Para se conectar a um banco de dados seguro, inclua os seguintes parâmetros:</p> <ul style="list-style-type: none"> - EncryptionMethod. Obrigatório. Indica se os dados estão criptografados quando são transmitidos na rede. Esse parâmetro deve ser definido como SSL. - ValidateServerCertificate. Opcional. Indica se a Informatica valida o certificado que é enviado pelo servidor de banco de dados. <p>Se esse parâmetro estiver definido como True, a Informatica validará o certificado enviado pelo servidor de banco de dados. Se você especificar o parâmetro HostNameInCertificate, a Informatica também validará o nome do host no certificado.</p> <p>Se esse parâmetro estiver definido como false, a Informatica não validará o certificado enviado pelo servidor de banco de dados. A Informatica ignora todas as informações de truststore especificadas.</p> <ul style="list-style-type: none"> - HostNameInCertificate. Opcional. O nome do host da máquina que hospeda o banco de dados seguro. Se você especificar um nome do host, o Informatica validará o nome do host incluído na string de conexão em relação ao nome do host no certificado SSL. - TrustStore. Obrigatório. O caminho e o nome do arquivo truststore que contém o certificado SSL do banco de dados. - TrustStorePassword. Obrigatório. A senha do arquivo truststore do banco de dados seguro. <p>Não se aplica ao ODBC.</p> <p>Hinweis: A Informatica anexa os parâmetros JDBC seguros à string de conexão. Se você incluir os parâmetros JDBC seguros diretamente na string de conexão, não insira quaisquer parâmetros no campo AdvancedJDBCSecurityOptions.</p>

Propriedade	Descrição
Página de Código	A página de código usada para leitura de um banco de dados de origem ou para gravação em um banco de dados ou um arquivo de destino.
SQL de Ambiente	Os comandos SQL para definir o ambiente do banco de dados quando você se conecta ao banco de dados. O Serviço de Integração de Dados executa o SQL de ambiente de conexão sempre que se conecta ao banco de dados.
Transação SQL	Os comandos SQL para definir o ambiente do banco de dados quando você se conecta ao banco de dados. O Serviço de Integração de Dados executa o SQL de ambiente de conexão no início de cada transação.
Período de Repetição	Essa propriedade é reservada para uso futuro.
Caractere do Identificador SQL	O tipo de caractere usado para identificar caracteres especiais e palavras-chave SQL reservadas, como WHERE. O Serviço de Integração de Dados coloca o caractere selecionado em torno de caracteres especiais e palavras-chave SQL reservadas. O Serviço de Integração de Dados também usa esse caractere para a propriedade Suporte a identificadores de letras maiúsculas e minúsculas.s. Selecione o caractere com base no banco de dados na conexão.
Suporte a Identificadores com Letras Maiúsculas e Minúsculas	Quando ativado, o Serviço de Integração de Dados coloca o identificador de caracteres em torno de nomes de tabela, exibição, esquema, sinônimo e coluna durante a geração e a execução de SQL em relação a esses objetos na conexão. Use se os objetos tiverem nomes com maiúsculas e minúsculas misturadas ou apenas minúsculas. Por padrão, essa opção não é selecionada.

LinkedIn-Verbindungseigenschaften

Verwenden Sie eine LinkedIn-Verbindung zum Extrahieren von Daten aus der LinkedIn-Website. Eine LinkedIn-Verbindung ist eine Verbindung zu einem sozialen Medium. Sie können eine LinkedIn-Verbindung im Administrator-Tool oder im Developer-Tool verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Eigenschaften von LinkedIn-Verbindungen erläutert:

Eigenschaft	Beschreibung
Name	Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. 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.

Eigenschaft	Beschreibung
Beschreibung	Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Die Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Der Verbindungstyp. Wählen Sie LinkedIn aus.
Haben Sie OAuth-Details?	Zeigt an, ob Sie OAuth konfigurieren möchten. Wählen Sie einen der folgenden Werte aus: <ul style="list-style-type: none"> - Ja. Zeigt an, dass Sie über den Zugriffs-Token und das Geheimwort verfügen. - Nein. Startet das OAuth-Dienstprogramm.
Verbraucherschlüssel	Der API-Schlüssel, den Sie beim Erstellen der Anwendung in LinkedIn erhalten. LinkedIn verwendet den Schlüssel zur Identifizierung der Anwendung.
Verbrauchergeheimwort	Der Geheimschlüssel, den Sie beim Erstellen der Anwendung in LinkedIn erhalten. LinkedIn verwendet das Geheimwort für das Eigentum am Verbraucherschlüssel.
Zugriffstoken	Zugriffstoken, den das OAuth-Dienstprogramm zurückgibt. Die LinkedIn-Anwendung verwendet diesen Token anstelle der Benutzeranmeldedaten für den Zugriff auf geschützte Ressourcen.
Zugriffsgeheimwort	Zugriffsgeheimwort, das das OAuth-Dienstprogramm zurückgibt. Das Geheimwort legt das Eigentum eines Token fest.
Bereich	Optional. Berechtigungen für die Anwendung. Geben Sie die Berechtigungen ein, die Sie zum Konfigurieren von OAuth verwendet haben.

MS SQL Server-Verbindungseigenschaften

Verwenden Sie eine Microsoft SQL Server-Verbindung für den Zugriff auf Microsoft SQL Server. Eine Microsoft SQL Server-Verbindung ist eine Verbindung zu einer relationalen Microsoft SQL Server-Datenbank. Sie können eine Microsoft SQL Server-Verbindung im Administrator-Tool oder im Developer-Tool erstellen und verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die MS SQL Server-Verbindungseigenschaften beschrieben:

Eigenschaft	Beschreibung
Datenbanktyp	Der Datenbanktyp.
Name	Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /

Eigenschaft	Beschreibung
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 765 Zeichen enthalten.
Vertrauenswürdige Verbindung verwenden	Ermöglicht dem Anwendungsdienst, Windows-Authentifizierung für den Zugriff auf die Datenbank zu verwenden. Der Benutzername, der den Anwendungsdienst startet, muss ein gültiger Windows-Benutzer mit Zugriff auf die Datenbank sein. Diese Option ist standardmäßig deaktiviert.
Benutzername	Der Datenbankbenutzername.
Passwort	Das Passwort für den Datenbankbenutzernamen.
Pass-Through-Sicherheit aktiviert	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.
Eigenschaften für den Metadaten-Zugriff: Verbindungszeichenfolge	Verwenden Sie die folgende Verbindungs-URL: <pre>jdbc:informatica:sqlserver://<host name>:<port>;DatabaseName=<database name></pre>
AdvancedJDBCSecurityOptions	<p>Datenbankparameter für Metadata-Zugriff auf eine sichere Datenbank. Informatica behandelt den Wert des AdvancedJDBCSecurityOptions-Felds als vertrauliche Daten und speichert die Parameterzeichenfolge als Verschlüsselung.</p> <p>Um eine Verbindung zu einer sicheren Datenbank herzustellen, beziehen Sie die folgenden Parameter mit ein:</p> <ul style="list-style-type: none"> - EncryptionMethod. Erforderlich. Gibt an, ob Daten bei der Netzwerkübertragung verschlüsselt sind. 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 einen HostNameInCertificate-Parameter eingeben, 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 von Ihnen angegebenen Truststore-Informationen. - 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. <p>Nicht anwendbar auf ODBC. Hinweis: Informatica hängt die sichere JDBC-Parameter an den Verbindungs-String an. Wenn Sie die sicheren JDBC-Parameter direkt im Verbindungs-String einschließen, geben Sie keinen Parameter in das Feld AdvancedJDBCSecurityOptions ein.</p>

Eigenschaft	Beschreibung
Eigenschaften für den Datenzugriff: Verbindungszeichenfolge	<p>Verwenden Sie die folgende Verbindungszeichenfolge:</p> <pre><server name>@<database name></pre> <p>Wenn die Datenbank den Standardport nicht verwendet, verwenden Sie die folgenden Verbindungszeichenfolgen:</p> <pre><server name>:<port>@<dbname> <servername>/<instancename>:<port>@<dbname></pre>
Codepage	Die Codepage, die zum Lesen aus einer Quelldatenbank oder zum Schreiben in eine Zieldatenbank oder Zieldatei verwendet wird.
Domänenname	Der Name der Domäne.
Paketgröße	Die zum Übertragen der Daten verwendete Paketgröße. Dient zur Optimierung der nativen Treiber für Microsoft SQL Server.
Eigentümername	Der Name des Schemaeigentümers.
Schemaname	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 anders lautet als der Benutzername für die Datenbank und Sie den Cache mit einem externen Tool verwalten.
Umgebungs-SQL	SQL-Befehle zum Einrichten der Datenbankumgebung beim Herstellen einer Verbindung zur Datenbank. Der Datenintegrationsdienst führt die Verbindungsumgebungs-SQL bei jeder Verbindung mit der Datenbank aus.
Transaktions-SQL	SQL-Befehle zum Einrichten der Datenbankumgebung beim Herstellen einer Verbindung zur Datenbank. Der Datenintegrationsdienst führt die Verbindungsumgebungs-SQL zu Beginn jeder Transaktion aus.
Wiederholungsperiode	Diese Eigenschaft ist für die zukünftige Verwendung reserviert.
SQL-ID-Zeichen	<p>Der Zeichentyp, der zur Kennzeichnung von Sonderzeichen und reservierten SQL-Schlüsselwörtern, wie WHERE, verwendet wird. Der Datenintegrationsdienst schließt mit dem ausgewählten Zeichen Sonderzeichen und reservierte SQL-Schlüsselwörter ein. Außerdem nutzt der Datenintegrationsdienst dieses Zeichen zur Unterstützung der ID-Eigenschaft für gemischte Groß- und Kleinschreibung.</p> <p>Wählen Sie das Zeichen basierend auf der Datenbank in der Verbindung aus.</p>
Unterstützte IDs für gemischte Groß-/Kleinschreibung	Sofern aktiviert, schließt der Datenintegrationsdienst Tabellen-, Ansichts-, Schema-, Synonym- und Spaltennamen in ID-Zeichen 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. Diese Option ist standardmäßig deaktiviert.
ODBC-Provider	<p>ODBC. Der Datenbanktyp, zu dem ODBC eine Verbindung herstellt. Geben Sie zur Pushdown-Optimierung den Datenbanktyp an, damit der Datenintegrationsdienst die native Datenbank-SQL generieren kann. Mögliche Werte:</p> <ul style="list-style-type: none"> - Andere - Sybase - Microsoft_SQL_Server <p>Standardwert ist „Andere“.</p>

ODBC-Verbindungseigenschaften

Verwenden Sie eine ODBC-Verbindung für den Zugriff auf ODBC-Daten. Eine ODBC-Verbindung ist eine relationale Datenbankverbindung. Sie können eine ODBC-Verbindung im Administrator-Tool, Developer-Tool oder Analyst-Tool erstellen und verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Eigenschaften von ODBC-Verbindungen erläutert:

Eigenschaft	Beschreibung
Datenbanktyp	Der Datenbanktyp.
Name	Name der Verbindung. Der Name unterliegt der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf nicht mehr als 128 Zeichen, keine Leerzeichen oder die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
ID	Zeichenfolge, die vom Datenintegrationsdienst zum Erkennen der Verbindung verwendet wird. 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 fungiert der Name der Verbindung.
Beschreibung	Die Beschreibung der Verbindung. Die Beschreibung darf nicht länger als 765 Zeichen sein.
Benutzername	Der Datenbankbenutzername.
Passwort	Passwort für den Datenbankbenutzernamen.
Pass-Through-Sicherheit aktiviert	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.
Eigenschaften für den Datenzugriff: Verbindungszeichenfolge	ODBC-Verbindungs-URL für den Zugriff auf Metadaten in der Datenbank. <Name der Datenquelle>
Codepage	Die Codepage, die zum Lesen aus einer Quelldatenbank oder zum Schreiben in eine Zieldatenbank oder Zieldatei verwendet wird.
Umgebungs-SQL	SQL-Befehle zum Einrichten der Datenbankumgebung beim Herstellen einer Verbindung zur Datenbank. Der Datenintegrationsdienst führt die Verbindungsumgebungs-SQL bei jeder Verbindung mit der Datenbank aus.
Transaktions-SQL	SQL-Befehle zum Einrichten der Datenbankumgebung beim Herstellen einer Verbindung zur Datenbank. Der Datenintegrationsdienst führt die Verbindungsumgebungs-SQL zu Beginn jeder Transaktion aus.
Wiederholungszeitraum	Diese Eigenschaft ist für die zukünftige Verwendung reserviert.

Eigenschaft	Beschreibung
SQL-ID-Zeichen	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. Außerdem nutzt der Datenintegrationsdienst dieses Zeichen zur Unterstützung der ID-Eigenschaft für gemischte Groß- und Kleinschreibung. Wählen Sie das Zeichen basierend auf der Datenbank in der Verbindung aus.
Unterstützte IDs für gemischte Groß-/Kleinschreibung	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. Diese Option ist standardmäßig deaktiviert.
ODBC-Provider	Der Datenbanktyp, zu dem die ODBC-Verbindung hergestellt wird. Geben Sie zur Pushdown-Optimierung den Datenbanktyp an, damit der Datenintegrationsdienst die native Datenbank-SQL generieren kann. Mögliche Werte: <ul style="list-style-type: none"> - Andere - Sybase - Microsoft_SQL_Server Voreingestellt ist "Andere".

Eigenschaften für Oracle-Verbindungen

Verwenden Sie eine Oracle-Verbindung, um eine Verbindung zu einer Oracle-Datenbank herzustellen. Die Oracle-Verbindung ist eine relationale Verbindung. Sie können eine Oracle-Verbindung im Administrator-Tool, Developer-Tool oder Analyst-Tool erstellen und verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Eigenschaften von Oracle-Verbindungen erläutert:

Eigenschaft	Beschreibung
Datenbanktyp	Der Datenbanktyp.
Name	Name der Verbindung. Der Name unterliegt der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf nicht mehr als 128 Zeichen, keine Leerzeichen oder die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
ID	Zeichenfolge, die vom Datenintegrationsdienst zum Erkennen der Verbindung verwendet wird. 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 fungiert der Name der Verbindung.
Beschreibung	Die Beschreibung der Verbindung. Die Beschreibung darf nicht länger als 765 Zeichen sein.
Benutzername	Der Datenbankbenutzername.

Eigenschaft	Beschreibung
Passwort	Passwort für den Datenbankbenutzernamen.
Pass-Through-Sicherheit aktiviert	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.
Eigenschaften für den Metadaten-Zugriff: Verbindungszeichenfolge	Verwenden Sie die folgende Verbindungs-URL: jdbc:informatica:oracle://<host_name>:<port>;SID=<database name>
AdvancedJDBCSecurityOptions	Datenbankparameter für Metadata-Zugriff auf eine sichere Datenbank. Informatica behandelt den Wert des AdvancedJDBCSecurityOptions-Felds als vertrauliche Daten und speichert die Parameterzeichenfolge als Verschlüsselung. Um eine Verbindung zu einer sicheren Datenbank herzustellen, beziehen Sie die folgenden Parameter mit ein: <ul style="list-style-type: none"> - EncryptionMethod. Erforderlich. Gibt an, ob Daten bei der Netzwerkübertragung verschlüsselt sind. 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 einen HostNameInCertificate-Parameter eingeben, 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 von Ihnen angegebenen Truststore-Informationen. - 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: Informatica hängt die sichere JDBC-Parameter an die Verbindungszeichenfolge an. Wenn Sie die sicheren JDBC-Parameter direkt in die Verbindungszeichenfolge einschließen, geben Sie keinen Parameter in das Feld AdvancedJDBCSecurityOptions ein.
Eigenschaften für den Datenzugriff: Verbindungszeichenfolge	Verwenden Sie die folgende Verbindungszeichenfolge: <database name>.world
Codepage	Die Codepage, die zum Lesen aus einer Quelldatenbank oder zum Schreiben in eine Zieldatenbank oder Zieldatei verwendet wird.
Umgebungs-SQL	SQL-Befehle zum Einrichten der Datenbankumgebung beim Herstellen einer Verbindung zur Datenbank. Der Datenintegrationsdienst führt die Verbindungsumgebungs-SQL bei jeder Verbindung mit der Datenbank aus.
Transaktions-SQL	SQL-Befehle zum Einrichten der Datenbankumgebung beim Herstellen einer Verbindung zur Datenbank. Der Datenintegrationsdienst führt die Verbindungsumgebungs-SQL zu Beginn jeder Transaktion aus.
Wiederholungszeitraum	Diese Eigenschaft ist für die zukünftige Verwendung reserviert.

Eigenschaft	Beschreibung
Parallelmodus aktivieren	Ermöglicht Parallelverarbeitung beim Laden von Daten in eine Tabelle im Bulk-Modus. Diese Option ist gemäß Voreinstellung deaktiviert.
SQL-ID-Zeichen	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. Außerdem nutzt der Datenintegrationsdienst dieses Zeichen zur Unterstützung der ID-Eigenschaft für gemischte Groß- und Kleinschreibung. Wählen Sie das Zeichen basierend auf der Datenbank in der Verbindung aus.
Unterstützte IDs für gemischte Groß-/Kleinschreibung	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. Diese Option ist standardmäßig deaktiviert.

Salesforce-Verbindungseigenschaften

Verwenden Sie eine Salesforce-Verbindung zum Herstellen einer Verbindung zu einem Salesforce-Objekt. Der Salesforce-Verbindung ist ein Anwendungsverbindungstyp. Sie können eine Salesforce-Verbindung im Administrator-Tool oder im Developer-Tool verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Eigenschaften von Salesforce-Verbindungen erläutert:

Eigenschaft	Beschreibung
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: ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
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 765 Zeichen enthalten.
Speicherort	Die Informatica-Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Der Verbindungstyp. Wählen Sie Salesforce.
Benutzername	Salesforce-Benutzername

Eigenschaft	Beschreibung
Benutzerpasswort	<p>Passwort für den Salesforce-Benutzernamen</p> <p>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).</p> <p>Beim Passwort wird zwischen Groß- und Kleinschreibung unterschieden.</p>
Dienst-URL	<p>URL des Salesforce-Dienstes, 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.</p>

SAP-Verbindungseigenschaften

Verwenden Sie eine SAP-Verbindung zum Herstellen einer Verbindung zu einer SAP-Datenquelle. Der SAP-Verbindung ist ein Enterprise-Anwendungsverbindungstyp. Sie erstellen diese Verbindung im Developer-Tool. Sie können eine SAP-Verbindung im Administrator-Tool oder im Developer-Tool verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Eigenschaften von SAP-Verbindungen erläutert:

Eigenschaft	Beschreibung
Benutzername	Benutzername für das SAP-Quellsystem.
Passwort	Passwort für den Benutzernamen.
Ablaufverfolgung	<p>Wählen Sie diese Option zum Verfolgen der vom SAP-System durchgeführten RFC-Aufrufe aus. SAP speichert die Informationen über die RFC-Aufrufe in einer Ablaufverfolgungsdatei.</p> <p>Über die folgenden Verzeichnisse können Sie auf die Ablaufverfolgungsdateien zugreifen:</p> <ul style="list-style-type: none"> - Verzeichnis <code>tomcat/bin</code> auf dem Informatica-Server - Verzeichnis <code>clients/DeveloperClient</code> auf dem Clientcomputer
Verbindungstyp	<p>Wählen Sie Typ A aus, um eine Verbindung zu einem SAP-System herzustellen.</p> <p>Wählen Sie Typ B aus, wenn Sie den SAP-Lastenausgleich verwenden möchten.</p>
Hostname	Hostname oder IP-Adresse des SAP-Servers. Informatica verwendet diesen Eintrag, um eine Verbindung zum SAP-Server herzustellen.
R3-Name	Name des SAP-Systems.
Gruppe	Gruppenname des SAP-Anwendungsservers.

Eigenschaft	Beschreibung
Systemnummer	SAP-Systemnummer.
Clientnummer	SAP-Clientnummer.
Sprache	Die für das Mapping gewünschte Sprache. Muss mit der Codepage des Developer-Tools kompatibel sein. Wenn Sie diese Option leer lassen, verwendet Informatica die Standardsprache des SAP-Systems.
Codepage	Codepage kompatibel mit dem SAP-Server. Muss auch dem Sprachcode entsprechen.
Staging-Verzeichnis	Pfad im SAP-System, in dem die Staging-Datei erstellt wird.
Quellverzeichnis	Der Datenintegrationsdienst-Pfad mit der Quelldatei.
FTP verwenden	Ermöglicht FTP-Zugriff auf SAP.
FTP-Benutzer	Benutzername zum Herstellen einer Verbindung zum FTP-Server.
FTP-Passwort	Passwort für den FTP-Benutzer.
FTP-Host	<p>Hostname oder IP-Adresse des FTP-Servers.</p> <p>Optional können Sie eine Portnummer von 1 bis einschließlich 65535 angeben. Der Standardwert für FTP ist 21. Verwenden Sie folgende Syntax für die Angabe des Hostnamens:</p> <pre>hostname:port_number</pre> <p>oder</p> <pre>IP address:port_number</pre> <p>Wenn Sie eine Portnummer angeben, aktivieren Sie diese Portnummer für FTP auf dem Host.</p> <p>Wenn Sie SFTP aktivieren, geben Sie einen Hostnamen oder eine Portnummer für einen SFTP-Server an. Standardwert für SFTP ist 22.</p>
Wiederholungszeitraum	Anzahl der Sekunden, die der Datenintegrationsdienst eine Neuverbindung mit dem FTP-Host herzustellen versucht, wenn die Verbindung fehlschlägt. Wenn der Datenintegrationsdienst im Wiederholungszeitraum keine erneute Verbindung zum FTP-Host herstellen kann, schlägt die Sitzung fehl. Standardwert ist 0. Dieser Wert zeigt einen unbeschränkten Wiederholungszeitraum an.
SFTP verwenden	Ermöglicht SFTP-Zugriff auf SAP.
Name der öffentlichen Schlüsseldatei	Pfad und Name der öffentlichen Schlüsseldatei Erforderlich, wenn der SFTP-Server öffentliche Schlüssel-Authentifizierung verwendet. Aktiviert für SFTP.
Name der privaten Schlüsseldatei	Pfad und Name der privaten Schlüsseldatei Erforderlich, wenn der SFTP-Server öffentliche Schlüssel-Authentifizierung verwendet. Aktiviert für SFTP.
Passwort für privaten Schlüsseldateinamen	Privates Schlüsseldateipasswort, das für die Entschlüsselung der privaten Schlüsseldatei verwendet wird. Erforderlich, wenn der SFTP-Server öffentliche Schlüssel-Authentifizierung verwendet und der private Schlüssel verschlüsselt ist. Aktiviert für SFTP.

Eigenschaften sequenzieller Verbindungen

Verwenden Sie eine sequenzielle Verbindung für den Zugriff auf eine sequenzielle Datenquelle. Sie erstellen eine sequenzielle Verbindung im Developer-Tool. Sie können eine sequenzielle Verbindung im Administrator-Tool oder im Developer-Tool verwalten.

Eine sequenzielle Datenquelle ist eine Datenquelle, auf die mit PowerExchange über ein Daten-Mapping zugegriffen werden kann, die mittels einer SEQ-Zugriffsmethode definiert wurde. Der Datenintegrationsdienst stellt über PowerExchange eine Verbindung mit der Datenquelle her.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Eigenschaften von sequenziellen Verbindungen erläutert:

Option	Beschreibung
Speicherort	Knotenname für den Speicherort des PowerExchange-Listenerdiensts, der eine Verbindung zum sequenziellen Datensatz herstellt. Der Knotenname ist im ersten Parameter der NODE-Anweisung in der PowerExchange-Konfigurationsdatei „dbmover.cfg“ definiert.
Benutzername	Ein Benutzername, der für den Zugriff auf den sequenziellen Datensatz autorisiert ist.
Passwort	<p>Passwort für den angegebenen Benutzernamen oder eine gültige PowerExchange-Passphrase.</p> <p>Eine PowerExchange-Passphrase kann 9 bis 128 Zeichen lang sein und die folgenden Zeichen enthalten:</p> <ul style="list-style-type: none">- Groß- und Kleinbuchstaben- Die Ziffern 0 bis 9- Leerzeichen- Die folgenden Sonderzeichen: ' - ; # \ , . / ! % & * () _ + { } : @ < > ? <p>Hinweis: Das erste Zeichen ist ein Apostroph.</p> <p>Passphrasen dürfen keine einfachen Anführungszeichen ('), doppelten Anführungszeichen (") oder Währungssymbole enthalten.</p> <p>Stellen Sie vor der Verwendung von Passphrasen sicher, dass der PowerExchange-Listenerdienst im DBMOVER-Mitglied mit der Sicherheitseinstellung SECURITY=(1,N) oder höher ausgeführt wird. Weitere Informationen finden Sie unter „SECURITY-Anweisung“ im <i>PowerExchange-Referenzhandbuch</i>.</p> <p>Die zulässigen Zeichen beim Beenden von IBM IRRPHREX haben keine Auswirkungen auf die zulässigen Zeichen in PowerExchange-Passphrasen.</p> <p>Hinweis: Eine gültige RACF-Passphrase kann bis zu 100 Zeichen lang sein. PowerExchange schneidet Passphrasen mit mehr als 100 Zeichen ab, wenn diese zur Validierung an RACF übergeben werden.</p>
Codepage	Erforderlich. Name der Codepage für das Lesen aus oder Schreiben in den sequenziellen Datensatz. Normalerweise ist dieser Wert ein ISO-Codepage-Name, z. B. ISO-8859-6.
Pass-Through-Sicherheit aktiviert	Aktiviert Pass-Through-Sicherheit für die Verbindung.

Option	Beschreibung
Verschlüsselungstyp	<p>Optional. Der Verschlüsselungstyp, den der Datenintegrationsdienst verwendet. Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> - Keine - RC2 - DES <p>Der Standardwert ist „Keine“.</p> <p>Hinweise:</p> <ul style="list-style-type: none"> - Informatica empfiehlt die Verwendung der SSL (Secure Sockets Layer)-Authentifizierung, anstatt den Verschlüsselungstyp und die Level-Verbindungseigenschaften oder die ENCRYPT- und ENCRYPTLEVEL-Anweisungen in der DBMOVER-Konfigurationsdatei zu konfigurieren. Die SSL-Authentifizierung bietet eine striktere Sicherheit und wird von diversen Informatica-Produkten verwendet. <p>Weitere Informationen zum Implementieren der SSL-Authentifizierung in einem PowerExchange-Netzwerk finden Sie im <i>PowerExchange-Referenzhandbuch</i>.</p> <ul style="list-style-type: none"> - Die Werte, die Sie für die Verbindungsattribute Verschlüsselungstyp und Level auswählen, setzen die Werte in den ENCRYPT- und ENCRYPTLEVEL-Anweisungen außer Kraft, wenn sie in der DBMOVER-Konfigurationsdatei auf dem Integrationsdienst-Rechner definiert wurden. Zum Aktivieren der Verschlüsselung für ein Mapping müssen Sie die geeigneten Verbindungsattribute auswählen.
[Encryption]-Ebene	<p>Wählen Sie bei Auswahl von RC2 oder DES für Verschlüsselungstyp eine der folgenden Optionen aus, um die Verschlüsselungsebene anzugeben, die der Datenintegrationsdienst verwendet:</p> <ul style="list-style-type: none"> - 1. Verwenden Sie einen 56-Bit-Verschlüsselungsschlüssel für DES und RC2. - 2. Verwenden Sie einen dreifachen 168-Bit-Verschlüsselungsschlüssel für DES und einen 64-Bit-Verschlüsselungsschlüssel für RC2. - 3. Verwenden Sie einen dreifachen 168-Bit-Verschlüsselungsschlüssel für DES und einen 128-Bit-Verschlüsselungsschlüssel für RC2. <p>Diese Option wird ignoriert, wenn Sie keinen Verschlüsselungstyp auswählen.</p> <p>Der Standardwert ist 1.</p>
Pacing-Größe	<p>Optional. Menge der Daten, die das Quellsystem an den PowerExchange-Listenerdienst übergeben kann. Legen Sie die Pacing-Größe fest, wenn eine externe Anwendung, eine Datenbank oder der Knoten mit dem Datenintegrationsdienst einen Engpass darstellt. Verwenden Sie niedrigere Werte für schnellere Leistung.</p> <p>Der Mindest- und Standardwert ist 0. Der Wert 0 bietet die beste Leistung.</p>
Als Zeilen interpretieren	<p>Wählen Sie diese Option optional aus, um die Pacing-Größe als eine Anzahl von Zeilen auszudrücken. Löschen Sie diese Option, um die Pacing-Größe in Kilobyte anzugeben. Diese Option ist standardmäßig nicht ausgewählt und die Pacing-Größe wird in Kilobyte angegeben.</p>
Komprimierung	<p>Optional. Wählen Sie diese Option zum Aktivieren der Quelldatenkomprimierung aus. Durch die Komprimierung von Daten können Sie die Menge der Daten verringern, die Informatica-Anwendungen über das Netzwerk senden. Standardmäßig ist diese Option nicht ausgewählt und die Komprimierung ist deaktiviert.</p>
Offload-Verarbeitung	<p>Optional. Steuert, ob für die Verarbeitung von Stapeldaten vom Quellcomputer zum Datenintegrationsdienst-Computer Offload-Verarbeitung verwendet werden soll. Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> - AUTO. Der Datenintegrationsdienst bestimmt, ob Offload-Verarbeitung verwendet werden soll. - Ja. Offload-Verarbeitung wird verwendet. - Nein. Offload-Verarbeitung wird nicht verwendet. <p>Der Standardwert ist AUTO.</p>

Option	Beschreibung
Worker-Threads	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.
Array-Größe	Optional: Die Anzahl der Datensätze im Speicher-Array für die Worker-Threads. Diese Option kann verwendet werden, wenn Sie die Option Worker-Threads auf einen Wert größer als 0 festlegen. Gültige Werte sind 25 bis 100.000. Der Standardwert ist 25.
Schreibmodus	<p>Optional. Modus, in dem der Datenintegrationsdienst Daten zum PowerExchange-Listenerdienst sendet. Wählen Sie einen der folgenden Schreibmodi aus:</p> <ul style="list-style-type: none"> - CONFIRMWRITEON. Sendet Daten an den PowerExchange-Listenerdienst und wartet auf eine Antwort, bevor weitere Daten gesendet werden. Wählen Sie diese Option aus, wenn die Fehlerbehebung Priorität hat. Diese Option kann jedoch zu Leistungseinbußen führen. - CONFIRMWRITEOFF. Sendet Daten an den PowerExchange-Listenerdienst, ohne auf eine Antwort zu warten. Verwenden Sie diese Option, wenn Sie die Zieltabelle im Fall eines Fehlers erneut laden können. - ASYNCHRONOUSWITHFAULTTOLERANCE. Sendet Daten an den PowerExchange-Listenerdienst, ohne auf eine Antwort zu warten. Diese Option aktiviert außerdem die Fehlererkennung. Diese Option kombiniert die Geschwindigkeit von CONFIRMWRITEOFF und die Datenintegrität von CONFIRMWRITEON. <p>Der Standardwert ist CONFIRMWRITEON.</p>

Propriedades de Conexão do Teradata Parallel Transporter

Use uma conexão do Teradata para acessar tabelas do Teradata. A conexão do Teradata é uma conexão do tipo Banco de dados. Você pode criar e gerenciar uma conexão do Teradata na ferramenta Administrator ou Developer.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

A seguinte tabela descreve as Propriedades de conexão do Teradata:

Propriedade	Descrição
Nome	Name der Verbindung. Der Name unterliegt nicht der Groß-/ Kleinschreibung und muss innerhalb der Domäne eindeutig sein. 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.
Descrição	Descrição da conexão. A descrição não pode conter mais de 765 caracteres.
Nome do Usuário	Nome de usuário do banco de dados Teradata com as permissões de gravação adequadas para acessar o banco de dados.
Senha	Senha para o nome de usuário do banco de dados Teradata.
Nome do Driver	Nome da unidade do Teradata JDBC.
String de Conexão	Use a seguinte string de conexão: jdbc:teradata://<hostname>/database=<database name>,tmode=ANSI,charset=UTF8

A tabela a seguir descreve as propriedades para acessar dados:

Propriedade	Descrição
TDPID	Nome ou endereço IP da máquina do banco de dados Teradata.
Nome do Banco de Dados	Nome do banco de dados Teradata. Se você não inserir um nome de banco de dados, a API do Teradata PT usará o nome do banco de dados de logon padrão.
Página de Código de Dados	Página de código associada ao banco de dados. Quando você executar um mapeamento que carrega em um destino do Teradata, a página de código da conexão do Teradata PT deve ser igual à página de código do destino do Teradata. O padrão é UTF-8.
Tenacidade	Número de horas que a API do Teradata PT continua tentando efetuar logon quando o número máximo de operações está em execução no banco de dados Teradata. Deve ser um integer positivo que não seja zero. O padrão é 4.
Máximo de Sessões	Número máximo de sessões que a API do Teradata PT estabelece com o banco de dados Teradata. Deve ser um integer positivo que não seja zero. O padrão é 4.

Propriedade	Descrição
Sessões Mínimas	Número mínimo de sessões da API do Teradata PT exigidas para que o trabalho da API do Teradata PT continue. Deve ser um integer positivo entre 1 e o valor Sessões máximas. O padrão é 1.
Suspender	Quantidade de tempo, em minutos, que a API do Teradata PT fica em pausa antes de tentar efetuar logon quando o número máximo de operações está em execução no banco de dados Teradata. Deve ser um número inteiro positivo que não seja zero. O padrão é 6.
Usar a URL do JDBC de Metadados para o TDCH	Indica que o Teradata Connector for Hadoop (TDCH) deve usar a URL do JDBC que você especificou na string de conexão nas propriedades de acesso a metadados. O padrão é selecionado. Desmarque essa opção para inserir outra URL do JDBC que o TDCH deve usar ao executar o mapeamento.
URL do JDBC para TDCH	Insira a URL do JDBC que o TDCH deve usar ao executar um mapeamento do Teradata. Use o seguinte formato: <code>jdbc:teradata://<hostname>/database=<database name>, tmode=ANSI, charset=UTF8</code> Este campo está disponível somente quando você desmarca a opção Usar a URL do JDBC para TDCH .

Twitter-Verbindungseigenschaften

Verwenden Sie eine Twitter-Verbindung, um Daten aus einer Twitter-Website zu extrahieren. Die Twitter-Verbindung ist eine Verbindung zu sozialen Medien. Sie können eine Twitter-Verbindung im Administrator-Tool oder im Developer-Tool verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Eigenschaften von Twitter-Verbindungen erläutert:

Eigenschaft	Beschreibung
Name	Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. 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 765 Zeichen enthalten.

Eigenschaft	Beschreibung
Speicherort	Die Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Der Verbindungstyp. Wählen Sie Twitter aus.
Haben Sie OAuth-Details?	Zeigt an, ob Sie OAuth konfigurieren möchten. Wählen Sie einen der folgenden Werte aus: - Ja. Zeigt an, dass Sie über den Zugriffs-Token und das Geheimwort verfügen. - Nein. Startet das OAuth-Dienstprogramm.
Verbraucherschlüssel	Der Verbraucherschlüssel, den Sie beim Erstellen der Anwendung in Twitter erhalten. Twitter verwendet die Schlüssel zur Identifizierung der Anwendung.
Verbrauchergeheimwort	Das Verbrauchergeheimwort, das Sie beim Erstellen einer Twitter-Anwendung erhalten. Twitter verwendet das Geheimwort für das Eigentum am Verbraucherschlüssel.
Zugriffstoken	Zugriffstoken, den das OAuth-Dienstprogramm zurückgibt. Twitter verwendet diesen Token anstelle der Benutzeranmeldedaten für den Zugriff auf geschützte Ressourcen.
Zugriffsgeheimwort	Zugriffsgeheimwort, das das OAuth-Dienstprogramm zurückgibt. Das Geheimwort legt das Eigentum eines Token fest.

Streaming-Verbindungseigenschaften für Twitter

Verwenden Sie eine Twitter-Streaming-Verbindung, um auf Nahezu-Echtzeitdaten von der Twitter-Website zuzugreifen. Die Twitter-Streaming-Verbindung ist eine Verbindung zu der Streaming-API des sozialen Medienunternehmens. Sie können eine Twitter-Streaming-Verbindung im Administrator-Tool oder im Developer-Tool erstellen und verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

Die folgende Tabelle beschreibt die Eigenschaften für eine Twitter-Streaming-Verbindung:

Eigenschaft	Beschreibung
Name	Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. 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 765 Zeichen enthalten.
Speicherort	Die Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Der Verbindungstyp. Wählen Sie Twitter-Streaming aus.

Die folgende Tabelle beschreibt die Eigenschaften für den Hose-Typ und die offene Authentifizierung (OAuth):

Eigenschaft	Beschreibung
Hose-Typ	Streaming-API-Methoden. Sie können eine der folgenden Methoden angeben: <ul style="list-style-type: none"> - Filter. Die Twitter <code>statuses/filter</code>-Methode gibt öffentliche Statusangaben zurück, die mit den Suchkriterien übereinstimmen. - Beispiel. Die Twitter <code>statuses/sample</code>-Methode gibt eine zufällige Stichprobe aus allen öffentlichen Statusangaben zurück.
Verbraucherschlüssel	Der Verbraucherschlüssel, den Sie beim Erstellen der Anwendung in Twitter erhalten. Twitter verwendet die Schlüssel zur Identifizierung der Anwendung.
Verbrauchergeheimwort	Das Verbrauchergeheimwort, das Sie beim Erstellen einer Twitter-Anwendung erhalten. Twitter verwendet das Geheimwort für das Eigentum am Verbraucherschlüssel.
Haben Sie OAuth-Details?	Zeigt an, ob Sie OAuth konfigurieren möchten. Wählen Sie einen der folgenden Werte aus: <ul style="list-style-type: none"> - Ja. Zeigt an, dass Sie über den Zugriffs-Token und das Geheimwort verfügen. - Nein. Startet das OAuth-Dienstprogramm.
Zugriffstoken	Zugriffstoken, den das OAuth-Dienstprogramm zurückgibt. Twitter verwendet diesen Token anstelle der Benutzeranmeldedaten für den Zugriff auf geschützte Ressourcen.
Zugriffsgeheimwort	Zugriffsgeheimwort, das das OAuth-Dienstprogramm zurückgibt. Das Geheimwort legt das Eigentum eines Token fest.

VSAM-Verbindungseigenschaften

Verwenden Sie eine VSAM-Verbindung für den Zugriff auf VSAM-Datentabellen. Die VSAM-Verbindung ist ein Einfachdatei-Verbindungstyp. Sie erstellen eine VSAM-Verbindung im Developer-Tool. Sie können eine VSAM-Verbindung im Administrator-Tool oder im Developer-Tool verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Eigenschaften von VSAM-Verbindungen erläutert:

Option	Beschreibung
Speicherort	Knotenname für den Speicherort des PowerExchange-Listenerdiensts, der eine Verbindung zum VSAM-Dataset herstellt. Der Knotenname ist im ersten Parameter der NODE-Anweisung in der PowerExchange-Konfigurationsdatei „dbmover.cfg“ definiert.
Benutzername	Ein Benutzername, der zum Herstellen einer Verbindung zum VSAM-Dataset autorisiert ist.

Option	Beschreibung
Passwort	<p>Passwort für den angegebenen Benutzer oder eine gültige PowerExchange-Passphrase. Eine PowerExchange-Passphrase kann 9 bis 128 Zeichen lang sein und die folgenden Zeichen enthalten:</p> <ul style="list-style-type: none"> - Groß- und Kleinbuchstaben - Die Ziffern 0 bis 9 - Leerzeichen - Die folgenden Sonderzeichen: ' - ; # \ , . / ! % & * () _ + { } : @ < > ? <p>Hinweis: Das erste Zeichen ist ein Apostroph.</p> <p>Passphrasen dürfen keine einfachen Anführungszeichen ('), doppelten Anführungszeichen (") oder Währungssymbole enthalten.</p> <p>Stellen Sie vor der Verwendung von Passphrasen sicher, dass der PowerExchange-Listenerdienst im DBMOVER-Mitglied mit der Sicherheitseinstellung SECURITY=(1,N) oder höher ausgeführt wird. Weitere Informationen finden Sie unter „SECURITY-Anweisung“ im <i>PowerExchange-Referenzhandbuch</i>.</p> <p>Die zulässigen Zeichen beim Beenden von IBM IRRPHREX haben keine Auswirkungen auf die zulässigen Zeichen in PowerExchange-Passphrasen.</p> <p>Hinweis: Eine gültige RACF-Passphrase kann bis zu 100 Zeichen lang sein. PowerExchange schneidet Passphrasen mit mehr als 100 Zeichen ab, wenn diese zur Validierung an RACF übergeben werden.</p>
Codepage	<p>Erforderlich. Name der Codepage für das Lesen aus oder Schreiben in das VSAM-Dataset. Normalerweise ist dieser Wert ein ISO-Codepage-Name, z. B. ISO-8859-6.</p>
Pass-Through-Sicherheit aktiviert	<p>Aktiviert Pass-Through-Sicherheit für die Verbindung.</p>
Verschlüsselungstyp	<p>Optional. Der Verschlüsselungstyp, den der Datenintegrationsdienst verwendet. Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> - Keine - RC2 - DES <p>Der Standardwert ist „Keine“.</p> <p>Hinweise:</p> <ul style="list-style-type: none"> - Informatica empfiehlt die Verwendung der SSL (Secure Sockets Layer)-Authentifizierung, anstatt den Verschlüsselungstyp und die Level-Verbindungseigenschaften oder die ENCRYPT- und ENCRYPTLEVEL-Anweisungen in der DBMOVER-Konfigurationsdatei zu konfigurieren. Die SSL-Authentifizierung bietet eine striktere Sicherheit und wird von diversen Informatica-Produkten verwendet. <p>Weitere Informationen zum Implementieren der SSL-Authentifizierung in einem PowerExchange-Netzwerk finden Sie im <i>PowerExchange-Referenzhandbuch</i>.</p> <ul style="list-style-type: none"> - Die Werte, die Sie für die Verbindungsattribute Verschlüsselungstyp und Level auswählen, setzen die Werte in den ENCRYPT- und ENCRYPTLEVEL-Anweisungen außer Kraft, wenn sie in der DBMOVER-Konfigurationsdatei auf dem Integrationsdienst-Rechner definiert wurden. Zum Aktivieren der Verschlüsselung für ein Mapping müssen Sie die geeigneten Verbindungsattribute auswählen.

Option	Beschreibung
[Encryption]-Ebene	<p>Wählen Sie bei Auswahl von RC2 oder DES für Verschlüsselungstyp eine der folgenden Optionen aus, um die Verschlüsselungsebene anzugeben, die der Datenintegrationsdienst verwendet:</p> <ul style="list-style-type: none"> - 1. Verwenden Sie einen 56-Bit-Verschlüsselungsschlüssel für DES und RC2. - 2. Verwenden Sie einen dreifachen 168-Bit-Verschlüsselungsschlüssel für DES und einen 64-Bit-Verschlüsselungsschlüssel für RC2. - 3. Verwenden Sie einen dreifachen 168-Bit-Verschlüsselungsschlüssel für DES und einen 128-Bit-Verschlüsselungsschlüssel für RC2. <p>Diese Option wird ignoriert, wenn Sie keinen Verschlüsselungstyp auswählen. Der Standardwert ist 1.</p>
Pacing-Größe	<p>Optional. Menge der Daten, die das Quellsystem an den PowerExchange-Listenerdienst übergeben kann. Legen Sie die Pacing-Größe fest, wenn eine externe Anwendung, eine Datenbank oder der Knoten mit dem Datenintegrationsdienst einen Engpass darstellt. Verwenden Sie niedrigere Werte für schnellere Leistung. Der Mindest- und Standardwert ist 0. Der Wert 0 bietet die beste Leistung.</p>
Als Zeilen interpretieren	<p>Optional. Wählen Sie diese Option, um die Pacing-Größe als Anzahl von Zeilen anzugeben. Löschen Sie diese Option, um die Pacing-Größe in Kilobyte anzugeben. Diese Option ist standardmäßig nicht ausgewählt und die Pacing-Größe wird in Kilobyte angegeben.</p>
Komprimierung	<p>Optional. Wählen Sie diese Option zum Aktivieren der Quelldatenkomprimierung aus. Durch die Komprimierung von Daten können Sie die Menge der Daten verringern, die Informatica-Anwendungen über das Netzwerk senden. Standardmäßig ist diese Option nicht ausgewählt und die Komprimierung ist deaktiviert.</p>
Offload-Verarbeitung	<p>Optional. Steuert, ob für die Verarbeitung von Stapeldaten vom Quellcomputer zum Datenintegrationsdienst-Computer Offload-Verarbeitung verwendet werden soll. Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> - AUTO. Der Datenintegrationsdienst bestimmt, ob Offload-Verarbeitung verwendet werden soll. - Ja. Offload-Verarbeitung wird verwendet. - Nein. Offload-Verarbeitung wird nicht verwendet. <p>Der Standardwert ist AUTO.</p>
Worker-Threads	<p>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.</p>

Option	Beschreibung
Array-Größe	Optional. Die Anzahl der Datensätze im Speicher-Array für die Worker-Threads. Diese Option kann verwendet werden, wenn Sie die Option Worker-Threads auf einen Wert größer als 0 festlegen. Gültige Werte sind 25 bis 100.000. Der Standardwert ist 25.
Schreibmodus	Optional. Modus, in dem der Datenintegrationsdienst Daten zum PowerExchange-Listenerdienst sendet. Wählen Sie einen der folgenden Schreibmodi aus: <ul style="list-style-type: none"> - CONFIRMWRITEON. Sendet Daten an den PowerExchange-Listenerdienst und wartet auf eine Antwort, bevor weitere Daten gesendet werden. Wählen Sie diese Option aus, wenn die Fehlerbehebung Priorität hat. Diese Option kann jedoch zu Leistungseinbußen führen. - CONFIRMWRITEOFF. Sendet Daten an den PowerExchange-Listenerdienst, ohne auf eine Antwort zu warten. Verwenden Sie diese Option, wenn Sie die Zieltabelle im Fall eines Fehlers erneut laden können. - ASYNCHRONOUSWITHFAULTTOLERANCE. Sendet Daten an den PowerExchange-Listenerdienst, ohne auf eine Antwort zu warten. Diese Option aktiviert außerdem die Fehlererkennung. Diese Option kombiniert die Geschwindigkeit von CONFIRMWRITEOFF und die Datenintegrität von CONFIRMWRITEON. Der Standardwert ist CONFIRMWRITEON.

Eigenschaften von Web Content-Kapow Katalyst-Verbindungen

Verwenden Sie eine Web Content-Kapow Katalyst-Verbindung, um auf Robots im Kapow Katalyst zuzugreifen. Dies ist eine Verbindung zu einem sozialen Medium. Sie können eine Web Content-Kapow Katalyst-Verbindung im Administrator-Tool oder im Developer-Tool erstellen und verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

Die folgende Tabelle beschreibt die Eigenschaften von Web Content-Kapow Katalyst-Verbindungen:

Eigenschaft	Beschreibung
Name	Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. 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 765 Zeichen enthalten.
Speicherort	Die Informatica-Domäne, in der Sie die Verbindung erstellen möchten.

Eigenschaft	Beschreibung
Typ	Der Verbindungstyp. Wählen Sie den Web Content-Kapow Katalyst aus.
URL der Management-Konsole	URL der Management-Konsole, in der der Robot hochgeladen wurde. Die URL muss mit http oder https beginnen. Zum Beispiel: http://localhost:50080.
RQL-Dienst-Port	Die Portnummer, wobei der Socket-Dienst den RQL-Dienst überwacht. Geben Sie einen Wert zwischen 1 und 65535 ein. Der Standardwert ist 50000.
Benutzername	Benutzername auf der lokalen Management-Konsole erforderlich.
Passwort	Passwort für den Zugriff auf die lokale Management-Konsole.

Verbindungseigenschaften für Web Services

Verwenden Sie eine Web-Dienst-Verbindung, um eine Web-Dienst-Verbraucher-Umwandlung mit einem Web-Dienst zu verbinden.

Die folgende Tabelle beschreibt die konfigurierbaren Eigenschaften von Web-Diensten:

Eigenschaft	Beschreibung
Benutzername	Benutzername, der mit dem Web-Dienst verbunden werden soll. Geben Sie einen Benutzernamen ein, wenn Sie die HTTP-Authentifizierung oder die WS-Security aktiviert haben. Wenn die Web-Dienst-Verbraucher-Umwandlung WS-Security-Ports enthält, erhält die Umwandlung einen dynamischen Benutzernamen durch einen Eingangsport. Der Data Integration Service überschreibt den Benutzernamen, der in der Verbindung definiert ist.
Passwort	Passwort für den Benutzernamen. Geben Sie ein Passwort ein, wenn Sie die HTTP-Authentifizierung oder die WS-Security aktiviert haben. Wenn die Web-Dienst-Verbraucher-Umwandlung WS-Security-Ports enthält, erhält die Umwandlung ein dynamisches Passwort durch einen Eingangsport. Der Data Integration Service überschreibt das Passwort, das in der Verbindung definiert ist.
Endpunkt-URL	URL für den Web-Dienst, auf den zugegriffen werden soll. Der Data Integration Service überschreibt die URL, die in der WSDL-Datei definiert ist. Wenn die Web-Dienst-Verbraucher-Umwandlung einen Endpunkt-URL-Port enthält, erhält die Umwandlung die URL durch einen Eingangsport. Der Data Integration Service überschreibt die URL, die in der Verbindung definiert ist.
Timeout	Anzahl von Sekunden, in der der Data Integration Service auf eine Antwort vom Web-Dienst-Provider wartet, ehe er die Verbindung schließt.

Eigenschaft	Beschreibung
HTTP-Authentifizierungstyp	<p>Art der Benutzer-Authentifizierung via HTTP. Wählen Sie einen der folgenden Werte aus:</p> <ul style="list-style-type: none"> - Keine. Keine Authentifizierung. - Automatisch. Der Data Integration Service wählt den Authentifizierungstyp, den der Web-Dienst-Provider verwendet. - Basis. Sie müssen der Domäne des Web-Dienst-Providers einen Benutzernamen und ein Passwort bereitstellen. Der Data Integration Service sendet den Benutzernamen und das Passwort zur Authentifizierung an den Web-Dienst-Provider. - zusammengefasst. Sie müssen der Domäne des Web-Dienst-Providers einen Benutzernamen und ein Passwort bereitstellen. Der Data Integration Service generiert eine verschlüsselte Meldungszusammenfassung aus dem Benutzernamen und dem Passwort und sendet diese an den Web-Dienst-Provider. Der Provider generiert einen temporären Wert für den Benutzernamen und das Passwort und speichert diesen in seinem Active Directory auf dem Domänen-Controller. Er vergleicht den Wert mit der Meldungszusammenfassung. Wenn beide übereinstimmen, authentifiziert Sie der Web-Dienst-Provider. - NTLM. Sie müssen einen Domänennamen, einen Servernamen oder einen Standardbenutzernamen und ein Passwort bereitstellen. Der Web-Dienst-Provider authentifiziert Sie anhand der Domäne, mit der Sie verbunden sind. Er erhält den Benutzernamen und das Passwort vom Windows Domain Controller und vergleicht sie mit dem Benutzernamen und Passwort, das Sie bereitgestellt haben. Wenn beide übereinstimmen, authentifiziert Sie der Web-Dienst-Provider. Bei der NTLM-Authentifizierung werden keine verschlüsselten Passwörter im Active Directory des Domain Controllers gespeichert.
WS-Security-Typ	<p>Art der WS-Security, die Sie verwenden möchten. Wählen Sie einen der folgenden Werte aus:</p> <ul style="list-style-type: none"> - Keine. Der Data Integration Service fügt keinen Web-Dienst Sicherheits-Header an die generierte SOAP-Anfrage an. - PasswordText. Der Data Integration Service fügt einen Web-Dienst Sicherheits-Header an die generierte SOAP-Anfrage an. Das Passwort wird in reinem Textformat gespeichert. - PasswordDigest. Der Data Integration Service fügt einen Web-Dienst Sicherheits-Header an die generierte SOAP-Anfrage an. Das Passwort wird in zusammengefasster Form gespeichert, was einen effektiven Schutz gegen Antwortangriffe auf das Netzwerk bietet. Der Data Integration Service kombiniert das Passwort mit einem Einmalschlüssel und einem Zeitstempel. Der Data Integration Service weist dem Passwort einen SHA-Hashwert zu, codiert es in base64-Codierung und verwendet das verschlüsselte Passwort im SOAP-Header.
Trust-Zertifikatsdatei	<p>Die Datei enthält ein Bundle aus vertrauenswürdigen Zertifikaten, die der Data Integration Service verwendet, wenn er das SSL-Zertifikat des Web-Dienstes authentifiziert. Geben Sie den Dateinamen und den kompletten Verzeichnispfad ein.</p> <p>Voreinstellung ist <code><Informatica-Installationsverzeichnis>/services/shared/bin/ca-bundle.crt</code>.</p>
Clientzertifikat - Dateiname	<p>Clientzertifikat, das der Web-Dienst verwendet, um einen Client zu authentifizieren. Geben Sie die Clientzertifikatsdatei an, wenn der Web-Dienst den Data Integration Service authentifizieren muss.</p>
Clientzertifikat - Passwort	<p>Passwort des Clientzertifikats. Geben Sie das Passwort des Clientzertifikats an, wenn der Web-Dienst den Data Integration Service authentifizieren muss.</p>
Clientzertifikat - Typ	<p>Format der Clientzertifikatsdatei. Wählen Sie einen der folgenden Werte aus:</p> <ul style="list-style-type: none"> - PEM. Dateien mit der Dateiendung .pem. - DER. Dateien mit der Dateiendung .cer oder .der <p>Geben Sie den Clientzertifikatstyp an, wenn der Web-Dienst den Data Integration Service authentifizieren muss.</p>

Eigenschaft	Beschreibung
Privater Schlüssel - Dateiname	Der private Schlüssel für das Clientzertifikat. Geben Sie den Dateinamen des privaten Schlüssels an, wenn der Web-Dienst den Data Integration Service authentifizieren muss.
Privater Schlüssel - Passwort	Passwort für den privaten Schlüssel des Clientzertifikats. Geben Sie das Passwort des privaten Schlüssels an, wenn der Web-Dienst den Data Integration Service authentifizieren muss.
Privater Schlüssel - Typ	Typ des privaten Schlüssels. Der unterstützte Typ ist PEM.

KAPITEL 8

Exportieren und Importieren von Domänenobjekten

Dieses Kapitel umfasst die folgenden Themen:

- [Export und Import von Domänenobjekten - Übersicht , 161](#)
- [Exportprozess, 162](#)
- [Domänenobjekte anzeigen, 162](#)
- [Importprozess, 169](#)

Export und Import von Domänenobjekten - Übersicht

Mit Hilfe der Befehlszeile können Sie Objekte zwischen unterschiedlichen Domänen derselben Version migrieren.

Beispielsweise können Domänenobjekte aus der Entwicklungsumgebung in eine Test- oder Produktionsumgebung migriert werden.

Verwenden Sie zum Exportieren und Importieren von Domänenobjekten die folgenden infacmd isp Befehle:

ExportDomainObjects

Exportiert native Benutzer, native Gruppen, Rollen und Verbindungen in eine XML-Datei.

ImportDomainObjects

Importiert native Benutzer, native Gruppen, Rollen und Verbindungen in eine Informatica-Domäne.

Mit einer infacmd-Kontrolldatei können Sie beim Exportieren und Importieren die Objekte filtern.

Mit dem Befehl `infacmd xrf generateReadableViewXML` können Sie außerdem eine lesbare XML-Datei aus einer Exportdatei generieren. Prüfen Sie die lesbare XML-Datei, um herauszufinden, ob die importierten Objekte gefiltert werden müssen.

Exportprozess

Sie können die Befehlszeile zum Exportieren von Domänenobjekten aus einer Domäne verwenden.

Führen Sie die folgenden Schritte durch, wenn Sie ein Domänenobjekt exportieren möchten:

1. Bestimmen Sie, welche Domänenobjekte exportiert werden sollen.
2. Wenn Sie nicht alle Domänenobjekte exportieren möchten, erstellen Sie eine Export-Steuerdatei, um die zu exportierenden Objekte herauszufiltern.
3. Führen Sie den Befehl `infacmd isp exportDomainObjects` aus, um die Domänenobjekte zu exportieren.

Der Befehl exportiert die Domänenobjekte in eine Exportdatei. Sie können diese Datei zum Importieren in eine andere Domäne nutzen.

Regeln und Richtlinien für das Exportieren von Domänenobjekten

Lesen Sie die folgenden Regeln und Richtlinien, bevor Sie Domänenobjekte exportieren:

- Wenn Sie einen Benutzer exportieren, wird standardmäßig nicht das Passwort des Benutzers exportiert. Wenn Sie das Passwort nicht exportieren, muss der Administrator das Passwort für den Benutzer zurücksetzen, nachdem der Benutzer in die Domäne importiert wurde. Wenn Sie jedoch den Befehl `infacmd isp exportDomainObjects` ausführen, können Sie wählen, eine verschlüsselte Version des Passworts zu exportieren.
- Wenn Sie einen Benutzer exportieren, werden die zugehörigen Gruppen des Benutzers nicht exportiert. Weisen Sie gegebenenfalls den Benutzer der Gruppe zu, nachdem Sie den Benutzer und die Gruppe importieren haben.
- Wenn Sie eine Gruppe exportieren, werden alle Untergruppen und Benutzer in der Gruppe exportiert.
- Sie können den Administrator-Benutzer, die Administrator-Rolle, die Gruppe "Jeder" und LDAP-Benutzer oder -Gruppen nicht exportieren. Um LDAP-Benutzer und -Gruppen in einer Informatica-Domäne zu ersetzen, exportieren Sie die LDAP-Benutzer und -Gruppen direkt aus dem LDAP-Verzeichnisdienst.
- Um native Benutzer und Gruppen aus Domänen der verschiedenen Versionen zu exportieren, verwenden Sie den Befehl `infacmd isp exportUsersAndGroups`.
- Wenn Sie eine Verbindung exportieren, wird standardmäßig nicht das Verbindungspasswort exportiert. Wenn Sie das Passwort nicht exportieren, muss der Administrator das Passwort für die Verbindung zurücksetzen, nachdem die Verbindung in die Domäne importiert wurde. Wenn Sie jedoch den Befehl `infacmd isp exportDomainObjects` ausführen, können Sie wählen, eine verschlüsselte Version des Passworts zu exportieren.

Domänenobjekte anzeigen

Sie können die Namen und Eigenschaften von Domänenobjekten in der exportierten XML-Datei anzeigen lassen.

Führen Sie den Befehl `infacmd xrf generateReadableViewXML` aus, um aus der Exportdatei eine lesbare XML-Datei zu erstellen.

Der nachfolgende Abschnitt stellt eine lesbare XML-Datei dar:

```
<global:View xmlns:global="http://global" xmlns:connection="http://connection"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="
  http://connection connection.xsd http://global globalSchemaDomain.xsd http://global
```

```

globalSchema.xsd">
<NativeUser isAdmin="false" name="admin" securityDomain="Native" viewId="0">
  <UserInfo email="" fullName="admin" phone="" viewId="1"/>
</NativeUser>
<User isAdmin="false" name="User1" securityDomain="Native" viewId="15">
  <UserInfo email="" fullName="NewUSer" phone="" viewId="16"/>
</User>
<Group name="TestGroup1" securityDomain="Native" viewId="182">
  <UserRef name="User1" securityDomain="Native" viewId="183"/>
  <UserRef name="User6" securityDomain="Native" viewId="188"/>
</Group>
<Role customRole="false" name="Administrator" viewId="242">
  <Description viewId="243">Provides all privilege and permission access to an
Informatica service.</Description>
  <ServicePrivilegeDefinition name="PwxListenerService" viewId="244">
    <Privilege category="" isEnabled="true" name="close" viewId="245"/>
    <Privilege category="" isEnabled="true" name="closeforce" viewId="246"/>
    <Privilege category="" isEnabled="false" name="Management Commands" viewId="249"/>
    <Privilege category="" isEnabled="false" name="Informational Commands"
viewId="250"/>
  </ServicePrivilegeDefinition>
</Role>
<Connection connectionString="inqa85sql25@qa90"
connectionType="SQLServerNativeConnection"
domainName="" environmentsSQL="" name="conn4" ownerName=""
schemaName="" transactionSQL="" userName="dummy" viewId="7512">
  <ConnectionPool maxIdleTime="120" minConnections="0" usePool="true" viewId="7514"/>
</Connection>
</global:View>

```

Darstellbare Domänenobjektnamen

Sie können die folgenden Namen und Eigenschaften von Domänenobjekten in einer lesbaren XML-Datei anzeigen:

Benutzer

In der folgenden Tabelle finden Sie eine Auflistung der Eigenschaften und des Typs:

Eigenschaft	Typ
Name	String
securityDomain	String
Admin	boolean
UserInfo	List<UserInfo>

UserInfo

In der folgenden Tabelle finden Sie eine Auflistung der Eigenschaften und des Typs:

Eigenschaft	Typ
Beschreibung	String
E-Mail	String

fullName	String
Telefon	String

Rolle

In der folgenden Tabelle finden Sie eine Auflistung der Eigenschaften und des Typs:

Eigenschaft	Typ
Name	String
Beschreibung	String
customRole	boolean
servicePrivilege	List<ServicePrivilegeDef>

ServicePrivilegeDef

In der folgenden Tabelle finden Sie eine Auflistung der Eigenschaften und des Typs:

Eigenschaft	Typ
Name	String
Berechtigungen	List<Berechtigung>

Berechtigung

In der folgenden Tabelle finden Sie eine Auflistung der Eigenschaften und des Typs:

Eigenschaft	Typ
Name	String
aktivieren	boolean
Kategorie	String

Gruppe

In der folgenden Tabelle finden Sie eine Auflistung der Eigenschaften und des Typs:

Eigenschaft	Typ
Name	String
securityDomain	String
Beschreibung	String

UserRefs	List<UserRef>
----------	---------------

GroupRef

In der folgenden Tabelle finden Sie eine Auflistung der Eigenschaften und des Typs:

Eigenschaft	Typ
Name	String
securityDomain	String

UserRef

- Name
- securityDomain

ConnectInfo

In der folgenden Tabelle finden Sie eine Auflistung der Eigenschaften und des Typs:

Eigenschaft	Typ
id	String
Name	String
connectionType	String
ConnectionPoolAttributes	List<ConnectionPoolAttributes>

ConnectionPoolAttributes

In der folgenden Tabelle finden Sie eine Auflistung der Eigenschaften und des Typs:

Eigenschaft	Typ
maxIdleTime	int
minConnections	int
poolSize	int
usePool	boolean

Unterstützte Verbindungstypen

- DB2iNativeConnection
- DB2NativeConnection

- DB2zNativeConnection
- JDBCConnection
- ODBCNativeConnection
- OracleNativeConnection
- PWXMetaConnection
- SAPConnection
- SDKConnection
- SQLServerNativeConnection
- SybaseNativeConnection
- TeradataNativeConnection
- URLLocation
- WebServiceConnection
- NRDBMetaConnection
- NRDBNativeConnection
- RelationalBaseSDKConnection

DB2iNativeConnection-Eigenschaften

- connectionType
- connectionString
- username
- environmentSQL
- libraryList
- Speicherort
- databaseFileOverrides

DB2NativeConnection-Eigenschaften

- connectionType
- connectionString
- username
- environmentSQL
- tableSpace
- transactionSQL

DB2zNativeConnection-Eigenschaften

- connectionType
- connectionString
- username
- environmentSQL
- Speicherort

JDBCConnection-Eigenschaften

- connectionType

- connectionString
- username
- dataStoreType

ODBCNativeConnection-Eigenschaften

- connectionType
- connectionString
- username
- environmentSQL
- transactionSQL
- odbcProvider

OracleNativeConnection-Eigenschaften

- connectionType
- connectionString
- username
- environmentSQL
- transactionSQL

PWXMetaConnection-Eigenschaften

- connectionType
- databaseName
- userName
- dataStoreType
- dbType
- hostName
- Speicherort
- Port

SAPConnection-Eigenschaften

- connectionType
- userName
- Beschreibung
- dataStoreType

SDKConnection-Eigenschaften

- connectionType
- SDKConnectionType
- dataSourceType

SQLServerNativeConnection-Eigenschaften

- connectionType
- connectionString
- username

- environmentSQL
- transactionSQL
- domainName
- ownerName
- schemaName

TeradataNativeConnection-Eigenschaften

- connectionType
- username
- environmentSQL
- transactionSQL
- dataSourceName
- databaseName

TeradataNativeConnection-Eigenschaften

- connectionType
- username
- environmentSQL
- transactionSQL
- connectionString

URLLocation-Eigenschaften

- connectionType
- locatorURL

WebServiceConnection-Eigenschaften

- connectionType
- url
- userName
- wsseType
- httpAuthenticationType

NRDBNativeConnection-Eigenschaften

- connectionType
- userName
- Speicherort

NRDBMetaConnection-Eigenschaften

- connectionType
- username
- Speicherort
- dataStoreType
- hostName
- Port

- databaseType
- databaseName
- Erweiterungen

RelationalBaseSDKConnection-Eigenschaften

- connectionType
- databaseName
- connectionString
- domainName
- environmentSQL
- hostName
- Eigentümer
- ispSvcName
- metadataDataStorageType
- metadataConnectionString
- metadataConnectionUserName

Importprozess

Sie können die Befehlszeile zum Importieren von Domänenobjekten aus einer Exportdatei in eine Domäne verwenden.

Führen Sie die folgenden Schritte durch, wenn Sie Domänenobjekte importieren möchten:

1. Führen Sie den Befehl `xrf generateReadableViewXML` aus, um aus der Exportdatei eine lesbare XML-Datei zu erstellen. Sehen Sie die Domänenobjekte in der lesbaren XML-Datei durch und legen Sie fest, welche Objekte importiert werden sollen.
2. Wenn Sie nicht alle Domänenobjekte aus der Exportdatei importieren möchten, erstellen Sie eine Import-Steuerdatei, um die zu importierenden Objekte herauszufiltern.
3. Führen Sie den Befehl `infacmd isp importDomainObjects` aus, um die Domänenobjekte in die angegebene Domäne zu importieren.
4. Nach dem Importieren der Objekte, ist es eventuell erforderlich, andere Domänenobjekte wie Anwendungsdienst und Ordner zu erstellen.

Regeln und Richtlinien für den Import von Domänenobjekten

Beachten Sie die folgenden Regeln und Richtlinien, ehe Sie Domänenobjekte importieren.

- Wenn Sie eine Gruppe importieren, importieren Sie auch alle zugehörigen Untergruppen und Benutzer dieser Gruppe.
- Um native Benutzer und Gruppen von Domänen verschiedener Versionen zu importieren, verwenden Sie den Befehl `infacmd isp importUsersAndGroups`.
- Nach dem Importieren eines Benutzers oder einer Gruppe, können Sie den Benutzer oder diese Gruppe nicht mehr umbenennen.

- Rollen werden unabhängig von Benutzern oder Gruppen importiert. Weisen Sie den Benutzern und Gruppen Rollen zu, nachdem Sie die Rollen, Benutzer und Gruppen importiert haben.
- Sie können die Administrator-Gruppe, den Administrator-Benutzer, die Administrator-Rolle, die Gruppe "Jeder" bzw. LDAP-Benutzer und -Gruppen nicht importieren.

Konfliktlösung

Ein Konflikt tritt immer dann auf, wenn Sie versuchen, ein Objekt mit einem Namen zu importieren, der bereits für ein Objekt in der Zieldomäne vergeben wurde. Durch Konfigurieren der Konfliktlösung können Sie bestimmen, wie bei Konflikten während des Imports verfahren werden soll.

Eine Konfliktlösungsstrategie bestimmen Sie entweder über die Befehlszeile oder die Kontrolldatei beim Importieren der Objekte. Wenn Sie die Konfliktlösung über die Befehlszeile und die Kontrolldatei vorgeben, hat die Kontrolldatei Priorität. Tritt ein Konflikt auf, ohne dass Sie eine Konfliktlösungsstrategie festgelegt haben, schlägt der Import fehl.

Sie können eine der folgenden Konfliktlösungsstrategien konfigurieren:

Erneut verwenden

Wiederverwendung des Objekts in der Target-Domäne

Umbenennen

Umbenennen des Quellobjekts Entweder Sie geben einen Namen in der Kontrolldatei an, oder der Name wird generiert. Ein generierter Name hat am Ende eine angehängte Nummer.

Ersetzen

Das Target-Objekt wird durch das Quellobjekt ersetzt.

Zusammenführen

Führt Quell- und Target-Objekte zu einer Gruppe zusammen. Wenn Sie zum Beispiel Gruppen desselben Namens zusammenführen, werden die Benutzer und Untergruppen beider Gruppen in der Gruppe im Target-Objekt zusammengeführt.

Sie können die Konfliktlösungsstrategie bei einem Zusammenführungskonflikt nicht über die Befehlszeile definieren. Verwenden Sie eine Steuerungsdatei zum Definieren der Lösungsstrategie bei Zusammenführungskonflikten. Sie müssen den Abschnitt des Gruppenobjektyps mit Zusammenführung als Konfliktlösungsrichtlinie mit erneuter Verwendung, Austausch oder Umbenennen für alle in Konflikt stehenden Benutzer in der Steuerungsdatei einbeziehen.

Geben Sie zum Beispiel die Lösungsstrategie bei Zusammenführungskonflikten für die folgenden Gruppen an:

- Gruppe A mit Benutzern a1, a2, b1, b2 in der Quelldomäne
- Gruppe A mit Benutzern a1, a2, a3, b1, b2 in der Zieldomäne

Sie erhalten die folgenden Ergebnisse in der Gruppe nach dem Zusammenführen in der Zieldomäne:

- a1, a2, b1, b2, wenn Sie sich zur Wiederverwendung oder zum Ersatz entscheiden
- a1, a2, a3, b1, b2, wenn Sie sich zum Umbenennen entscheiden

KAPITEL 9

Lizenzverwaltung

Dieses Kapitel umfasst die folgenden Themen:

- [Lizenzverwaltung - Übersicht, 171](#)
- [Arten von Lizenzschlüsseln, 173](#)
- [Ein Lizenzobjekt erstellen, 174](#)
- [Eine Lizenz einem Dienst zuweisen, 175](#)
- [Entfernen eine Lizenz von einem Anwendungsdienst, 176](#)
- [Aktualisieren einer Lizenz, 176](#)
- [Entfernen einer Lizenz, 177](#)
- [Lizenzeigenschaften, 178](#)

Lizenzverwaltung - Übersicht

Der Dienstmanager auf dem Master-Gateway-Knoten verwaltet die Informatica-Lizenzen.

Mit einer Lizenz können Sie die folgenden Aufgaben ausführen:

- Ausführen von Anwendungsdiensten wie der Analyst-Dienst, Datenintegrationsdienst und PowerCenter-Repository-Dienst.
- Verwenden von Add-On-Optionen wie Partitionierung für PowerCenter, Gitter und hohe Verfügbarkeit.
- Zugriff auf bestimmte Typen von Verbindungen wie Oracle, Teradata, Microsoft SQL Server und IBM MQ Series.
- Verwenden von Metadaten Exchange-Optionen wie Metadaten Exchange für Cognos und Metadata Exchange für Rational Rose.

Die verwendete Lizenz bestimmt die Aufgaben, die von Ihnen durchgeführt werden können, wie z. B. das Erstellen von Benutzern. Sie können die Lizenz mit einer neuen Lizenzdatei im Administrator-Tool aktualisieren, um zusätzliche Funktionen in PowerCenter Express zu nutzen.

Die verwendete Lizenz bestimmt die Aufgaben, die von Ihnen durchgeführt werden können, wie z. B. das Erstellen von Benutzern.

Beim Installieren von Informatica erstellt das Installationsprogramm basierend auf dem von Ihnen für die Installation verwendeten Lizenzschlüssel ein Lizenzobjekt in der Domäne.

Sie müssen jedem Anwendungsdienst ein Lizenzobjekt zuordnen, um den Dienst zu aktivieren. So müssen Sie zum Beispiel dem PowerCenter-Integrationsdienst eine Lizenz zuordnen, bevor Sie einen Arbeitsablauf mit dem PowerCenter-Integrationsdienst ausführen können.

Sie können weitere Lizenzobjekte in der Domäne erstellen. Basierend auf Ihren Projektanforderungen benötigen Sie möglicherweise mehrere Lizenzobjekte. Beispielsweise können Sie zwei Lizenzobjekte haben, wobei jedes Lizenzobjekt Ihnen ermöglicht, Dienste auf einem anderen Betriebssystem auszuführen. Sie können auch mehrere Lizenzobjekte verwenden, um mehrere Projekte in derselben Domäne zu verwalten. Ein Projekt benötigt eventuell Zugriff auf bestimmte Datenbanktypen, während dies für das andere Projekt nicht erforderlich ist.

Lizenzvalidierung

Beim Starten der Anwendungsprozesse werden diese vom Service Manager validiert. Der Service Manager validiert für jeden Dienstprozess die folgenden Informationen:

- Produktversion. Stellt sicher, dass Sie die richtige Version der Informatica Services ausführen.
- Plattform. Stellt sicher, dass die Informatica Services auf einem lizenzierten Betriebssystem ausgeführt werden.
- Ablaufdatum. Überprüft das Ablaufdatum der Lizenz. Wenn die Lizenz abläuft, werden Informatica Services nicht gestartet.
- Ablaufdatum. Überprüft das Ablaufdatum der Lizenz. Wenn die Lizenz abläuft, werden Informatica Services nicht gestartet.
- Ablaufdatum. Überprüft, dass die Lizenz nicht erloschen ist. Erlischt die Lizenz, kann kein der Lizenz zugeordneter Anwendungsdienst starten. Sie müssen den Informatica Services eine gültige Lizenz zuordnen, um sie starten zu können.
- PowerCenter-Optionen. Bestimmt die Optionen, die von den Informatica Services verwendet werden können. So prüft beispielsweise der Service Manager, ob der PowerCenter Integration Service die Sitzung mit Gitteroption nutzen kann.
- Konnektivität. Überprüft Verbindungen, die von den Informatica Services verwendet werden können. Zum Beispiel prüft der Service Manager, ob PowerCenter sich mit einer IBM DB2 Datenbank verbinden kann.
- Metadaten austausch-Optionen. Bestimmt die Metadaten austausch-Optionen, die für die Nutzung zur Verfügung stehen. Beispielsweise prüft der Service Manager, dass Sie Zugriff auf den Metadaten austausch für Business-Objekt-Designer haben.

Lizenzierungsprotokollereignisse

Der Service Manager generiert Protokollereignisse und schreibt diese in den Protokoll-Manager. Protokollereignisse werden für folgende Aktionen generiert:

- Erstellen oder Löschen einer Lizenz.
- Zuweisen eines inkrementellen Lizenzschlüssels an eine Lizenz.
- Zuweisen eines Anwendungsdienstes an eine Lizenz.
- Entfernen einer Lizenz von einem Anwendungsdienst.
- Ablauf der Lizenz.
- Der Service Manager trifft auf einen Fehler, zum Beispiel einen Validierungsfehler.

Ein Protokollereignis enthält den Benutzernamen und den Zeitpunkt des Ereignisses.

Sie müssen eine Berechtigung für die Domäne besitzen, um die Protokolle für die Lizenzierungsereignisse anzuzeigen.

Die Lizenzierungsereignisse werden in den Domänenprotokollen angezeigt.

Lizenzverwaltungstasks

Sie können die folgenden Tasks zur Lizenzverwaltung ausführen:

- Lizenz im Administrator Tool erstellen. Zur Erstellung einer Lizenz im Administrator Tool brauchen Sie einen Lizenzschlüssel.
- Zuweisung einer Lizenz zu jedem Anwendungsdienst. Weisen Sie jedem Anwendungsdienst eine Lizenz zu, um den Dienst zu aktivieren.
- Zuweisung einer Lizenz aus einem Anwendungsdienst entfernen. Sie müssen die Zuweisung der Lizenz zum Anwendungsdienst rückgängig machen, wenn Sie den Dienst einstellen oder von einer Entwicklungsumgebung in eine Produktionsumgebung migrieren möchten. Nachdem Sie die Lizenz des Dienstes aufgehoben haben, können Sie den Dienst erst wieder aktivieren, wenn Sie ihm eine neue gültige Lizenz zuweisen.
- Aktualisieren der Lizenz. Wenn Sie der vorhandenen Lizenz PowerCenter-Optionen hinzufügen möchten, müssen Sie die Lizenz aktivieren.
- Entfernen der Lizenz. Lizenzen müssen entfernt werden, wenn sie veraltet sind.
- Konfigurieren von Benutzerberechtigungen für eine Lizenz.
- Anzeigen von Lizenzdetails. Möglicherweise müssen Sie die Lizenz überprüfen, um Details wie das Ablaufdatum und die maximale Anzahl der lizenzierten CPUs festzustellen. Diese Details müssen Sie manchmal nachprüfen, damit gewährleistet ist, dass Sie die Lizenzbedingungen einhalten. Zur Feststellung der Details für jede Lizenz verwenden Sie das Administrator Tool.
- Überwachen der Lizenznutzung und der lizenzierten Optionen. Sie können die Nutzung der logischen CPUs und der PowerCenter Repository Services überwachen. Außerdem können Sie die Anzahl der für eine Lizenz erworbenen Softwareoptionen überwachen und anhand des Lizenzverwaltungsberichts feststellen, wie oft die Nutzungsgrenzen bei einer Lizenz überschritten wurden.

All diese Tasks können Sie mit dem Administrator Tool oder anhand von *infacmd isp*-Befehlen ausführen.

Arten von Lizenzschlüsseln

Informatica bietet Lizenzschlüssel in Lizenzdateien an. Der Lizenzschlüssel ist verschlüsselt. Wenn Sie aus einer Lizenzschlüsseldatei eine Lizenz erstellen, entschlüsselt der Service Manager den Lizenzschlüssel und ermöglicht den Erwerb von Optionen.

Sie erstellen eine Lizenz aus einer Lizenzschlüsseldatei. Sie weisen die Lizenzschlüssel der Lizenz zu, um zusätzliche Optionen zu aktivieren. Informatica verwendet folgende Arten von Lizenzschlüsseln:

- Originalschlüssel Informatica generiert einen Originalschlüssel auf der Basis Ihres Vertrags. Je nach Vertrag kann Informatica auch mehrere Originalschlüssel bereitstellen.
- Inkrementelle Schlüssel Informatica generiert inkrementelle Schlüssel auf der Basis der Updates einer vorhandenen Lizenz, z. B. eine erweiterte Lizenzperiode oder eine zusätzliche Option.

Hinweis: Lizenzen von Informatica ändern sich im Allgemeinen bei jeder Version. Verwenden Sie eine für die aktuelle Version gültige Lizenzschlüsseldatei, um sicherzustellen, dass Ihre Installation alle Funktionen enthält.

Originalschlüssel

Mit einem Originalschlüssel lassen sich der Vertrag, das Produkt und die lizenzierten Funktionen identifizieren. Zu den lizenzierten Funktionen gehört die Informatica-Edition, der Bereitstellungstyp, die

Anzahl der autorisierten CPUs und die autorisierten Informatica-Optionen und -Konnektivität. Sie verwenden die Originalschlüssel, um Informatica zu installieren und Lizenzen für die Dienste zu erstellen. Um Informatica zu installieren, benötigen Sie einen Lizenzschlüssel. Das Installationsprogramm erstellt ein Lizenzobjekt für die Domäne im Administrator Tool. Sie können weitere Originalschlüssel dazu verwenden, zusätzliche Lizenzen in derselben Domäne zu erstellen. Für jedes Lizenzobjekt ist ein anderer Originallizenzschlüssel erforderlich.

Inkrementelle Schlüssel

Inkrementelle Schlüssel dienen der Aktualisierung bereits existierender Lizenzen. Inkrementelle Schlüssel fügen Sie einer existierenden Lizenz hinzu, wenn Sie Optionen wie PowerCenter-Optionen, die Konnektivität und Optionen zum Metadatenaustausch hinzufügen oder entfernen möchten. Wenn zum Beispiel eine existierende Lizenz keine hohe Verfügbarkeit gewährleistet, können Sie zur existierenden Lizenz einen inkrementellen Schlüssel mit der Hochverfügbarkeitsoption hinzufügen.

Der Service Manager aktualisiert das Ablaufdatum der Lizenz, wenn das Ablaufdatum des inkrementellen Schlüssels später als das Ablaufdatum eines Originalschlüssels liegt. Der Service Manager nutzt das späteste Ablaufdatum. Ein Lizenzobjekt kann verschiedene Ablaufdaten für Optionen in der Lizenz haben. So kann die relationale Konnektivitätsoption der IBM DB2 zum Beispiel am 12.01.2006 und die Option für Gittersitzungen am 04.01.06 erlöschen.

Der Service Manager validiert den inkrementellen Schlüssel gegen den für die Lizenzerstellung benutzten Originalschlüssel. Sind die Schlüssel nicht kompatibel, wird eine Fehlermeldung ausgegeben.

Ein Lizenzobjekt erstellen

Sie haben die Möglichkeit, ein Lizenzobjekt in einer Domäne zu erstellen und die Lizenz zu Anwendungsdiensten hinzuzufügen. Die Lizenzerstellung erfolgt im Administrator Tool mittels einer Lizenzschlüsseldatei. Die Lizenzschlüsseldatei enthält einen verschlüsselten Originalschlüssel. Den Originalschlüssel brauchen Sie für die Lizenzerstellung.

Alternativ können Sie auch mit dem Befehl `infacmd isp AddLicense` eine Lizenz zu einer Domäne hinzufügen.

Für die Lizenzerstellung gelten folgende Richtlinien:

- Verwenden Sie eine gültige Lizenzschlüsseldatei. Die Lizenzschlüsseldatei muss einen Originallizenzschlüssel enthalten. Die Lizenzschlüsseldatei darf nicht abgelaufen sein.
- Für mehrere Lizenzen können Sie nicht dieselbe Lizenzschlüsseldatei einsetzen. Jede Lizenz muss einen eindeutigen Originalschlüssel besitzen.
- Geben Sie für jede Lizenz einen eindeutigen Namen ein. Den Namen für die Lizenz müssen Sie bei der Lizenzerstellung angeben. Der Name darf unter allen Objekten in der Domäne nur einmal vorkommen.
- Legen Sie die Lizenzschlüsseldatei an einem Speicherort ab, auf den der Administrator Tool-Computer zugreifen kann. Beim Erstellen des Lizenzobjekts müssen Sie den Speicherort der Lizenzschlüsseldatei angeben.

Nachdem Sie die Lizenz erstellt haben, können Sie die Beschreibung ändern. Um die Beschreibung einer Lizenz zu ändern, wählen Sie die Lizenz im Navigator des Administrator Tools und klicken Sie auf Bearbeiten.

1. Klicken Sie im Administrator Tool auf **Aktionen > Neu > Lizenz**.

Das Fenster **Lizenz erstellen** wird aufgerufen.

2. Geben Sie folgende Optionen ein:

Option	Beschreibung
Name	Name der Lizenz. Beim Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden, und er muss in der Domäne eindeutig sein. Er darf nicht länger als 128 Zeichen sein oder mit @ beginnen. Außerdem darf er keine Leerzeichen oder die folgenden Sonderzeichen enthalten: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () []
Beschreibung	Beschreibung der Lizenz. Die Beschreibung darf nicht länger als 765 Zeichen sein.
Pfad	Pfad der Domäne, in der Sie die Lizenz erstellen. Schreibgeschütztes Feld. Klicken Sie optional auf Durchsuchen und wählen Sie im Fenster Ordner auswählen eine Domäne. Optional klicken Sie auf Ordner erstellen , um einen Ordner für die Domäne zu erstellen.
Lizenzdatei	Die Datei, die den Originalschlüssel enthält. Klicken Sie auf Durchsuchen , um die Datei zu suchen.

Wenn Sie versuchen, eine Lizenz mit einem inkrementellen Schlüssel zu erstellen, wird eine Meldung eingeblendet, die besagt, dass Sie erst einen inkrementellen Schlüssel angeben können, nachdem Sie einen Originalschlüssel hinzugefügt haben.

Zur Erstellung einer Lizenz ist ein Originalschlüssel erforderlich.

3. Klicken Sie auf **Erstellen**.

Eine Lizenz einem Dienst zuweisen

Sie müssen einem Anwendungsdienst eine Lizenz zuweisen, bevor Sie den Dienst aktivieren können. Wenn Sie einem Dienst eine Lizenz zuweisen, aktualisiert der Service Manager die Metadaten der Lizenz. Sie können auch den Befehl *infacmd isp AssignLicense* verwenden, um einer Lizenz einen Dienst zuzuweisen.

1. Wählen Sie die Lizenz im **Domänen-Navigator** des Administrator Tools aus.
2. Klicken Sie auf die Registerkarte **Zugewiesene Dienste**.
3. Auf der Registerkarte **Lizenz**, klicken Sie auf **Aktionen > Zugewiesene Dienste bearbeiten**.
Das Fenster **Lizenz den Diensten zuweisen oder nicht zuweisen** erscheint.
4. Wählen Sie die Dienste unter **Nicht zugewiesene Dienste** aus und klicken Sie auf Hinzufügen.
Mit Strg-Klick wählen Sie mehrere Dienste aus. Mit Umsch-Klick wählen Sie eine zusammenhängende Liste von Diensten aus. Sie können auch auf **Alle hinzufügen** klicken, um die Lizenz allen Diensten zuzuweisen.
5. Klicken Sie auf **OK**.

Regeln und Richtlinien zum Zuweisen von Lizenzen an einen Dienst

Halten Sie sich an die folgenden Regeln und Richtlinien, wenn Sie Lizenzen zuweisen:

- Sie können Lizenzen zuweisen, um Dienste zu deaktivieren.
- Wenn Sie einem Dienst eine Lizenz zuweisen möchten, der bereit seine Lizenz besitzt, müssen Sie die vorhandene Lizenz zunächst von diesem Dienst entfernen.

- Um einen Dienst mit einem Backup-Knoten zu starten, müssen Sie diesem eine Lizenz mit einer höheren Verfügbarkeit zuweisen.
- Um einen Dienst automatisch zu starten, müssen Sie diesem eine Lizenz mit einer höheren Verfügbarkeit zuweisen.

Entfernen eine Lizenz von einem Anwendungsdienst

Möglicherweise müssen Sie die Zuordnung einer Lizenz bei einem Dienst aufheben, wenn der Dienst veraltet ist oder Sie einen Dienst nicht weiter betreiben wollen. Vielleicht möchten Sie einen Dienst nicht fortsetzen, wenn Sie mit mehr CPUs arbeiten als lizenziert sind.

Sie können das Administrator Tool oder den Befehl *infacmd isp UnassignLicense* verwenden, um die Zuordnung einer Lizenz für einen Dienst aufzuheben.

Bevor Sie die Zuordnung einer Lizenz aufheben können, müssen Sie den Dienst deaktivieren. Nachdem Sie eine Lizenz von dem Dienst entfernt haben, können Sie den Dienst nicht aktivieren. Sie müssen eine gültige Lizenz zuweisen, um den Dienst wieder aktivieren zu können.

Sie müssen den Dienst deaktivieren, bevor Sie die Lizenz entfernen können. Wenn Sie versuchen, eine Lizenz von einem aktivierten Dienst zu entfernen, wird eine Meldung angezeigt, die besagt, dass der Dienst nicht entfernt werden kann, weil er ausgeführt wird.

1. Wählen Sie die Lizenz im **Domänen-Navigator** des Administrator Tools aus.
2. Klicken Sie auf die Registerkarte **Zugewiesene Dienste**.
3. Auf der Registerkarte **Lizenz** klicken Sie auf **Aktionen > Zugewiesene Dienste bearbeiten**.
Das Fenster **Diese Lizenz zu Services zuweisen oder Zuordnung aufheben** wird angezeigt.
4. Wählen Sie unter **Zugewiesener Dienst** den Dienst aus, und klicken Sie dann auf **Entfernen**. Klicken Sie optional auf **Alle entfernen**, um alle zugewiesenen Dienste aufzuheben.
5. Klicken Sie auf **OK**.

Aktualisieren einer Lizenz

Sie können die aktuelle Lizenz in der Informatica-Domäne mit einem neuen Lizenzschlüssel einem inkrementellen Lizenzschlüssel aktualisieren.

Wenn Sie einen inkrementellen Schlüssel zu einer Lizenz hinzufügen, fügt der Dienstmanager lizenzierte Optionen hinzu oder entfernt diese, und aktualisiert das Ablaufdatum der Lizenz.

Sie können auch den Befehl *infacmd isp UpdateLicense* benutzen, um einen inkrementellen Schlüssel einer Lizenz hinzuzufügen.

Nach dem Aktualisieren der Lizenz müssen Sie die Informatica-Dienste neustarten, damit die Änderungen wirksam werden.

Verwenden Sie die folgenden Richtlinien, um eine Lizenz zu aktualisieren:

- Überprüfen Sie, ob die Lizenzschlüsseldatei für den Computer mit dem Administrator-Tool zugänglich ist. Wenn Sie das Lizenzobjekt aktualisieren, müssen Sie den Speicherort der Lizenzschlüsseldatei angeben.

- Die inkrementelle Schlüssel muss mit dem Originalschlüssel kompatibel sein. Ein Fehler wird angezeigt, wenn die Schlüssel nicht kompatibel sind.

Der Dienstmanager validiert den inkrementellen Schlüssel gegen den ursprünglichen Schlüssel entsprechend den folgenden Informationen:

- Seriennummer
- Bereitstellungsart
- Händler
- Informatica-Ausgabe
- Informatica Version:

1. Wählen Sie eine **Lizenz** im Navigator.
2. Klicken Sie auf die Registerkarte **Eigenschaften**.
3. Klicken Sie auf der Registerkarte **Lizenz** auf **Aktionen > Lizenz aktualisieren**. **Aktionen > Inkrementellen Schlüssel hinzufügen**.

Das Fenster **Lizenz aktualisieren** wird angezeigt.

4. Klicken Sie auf **Durchsuchen**, um die Lizenzschlüsseldatei auszuwählen. Optional können Sie den Pfad zum Lizenzschlüssel eingeben.
5. Klicken Sie auf **OK**.
6. Im Abschnitt **Lizenzdetails** der Registerkarte **Eigenschaften** klicken Sie auf **Bearbeiten**, um die Beschreibung der Lizenz zu bearbeiten.
7. Klicken Sie auf **OK**.

Entfernen einer Lizenz

Sie können eine Lizenz mit dem Administrator Tool oder dem Befehl `infacmd isp RemoveLicense` aus einer Domäne entfernen.

Deaktivieren Sie vor dem Entfernen einer Lizenz alle Dienste, die der Lizenz zugewiesen sind. Wenn Sie die Dienste nicht deaktivieren, werden alle laufenden Prozesse beim Entfernen der Lizenz abgebrochen. Wenn Sie eine Lizenz zu entfernen, hebt der Service Manager die Lizenz für jeden zugewiesenen Dienst auf und entfernt die Lizenz aus der Domäne. Zur erneuten Aktivierung eines Dienstes weisen Sie ihm eine andere Lizenz zu.

Wenn Sie eine Lizenz entfernen, können Sie noch immer die Lizenznutzungs-Logs im Log Viewer für diese Lizenz anzeigen, aber Sie können keinen Lizenzbericht für diese Lizenz ausführen.

So entfernen Sie eine Lizenz aus der Domäne:

1. Wählen Sie die Lizenz im **Domänen-Navigator** des Administrator Tools aus.
2. Klicken Sie auf **Aktionen > Löschen**.

Lizenzeigenschaften

Sie können Lizenzdetails mithilfe des Administrator-Tools oder des `infacmd isp ShowLicense`-Befehls anzeigen.

Sie können Lizenzdetails mithilfe des Administrator-Tools anzeigen.

Sie können Lizenzdetails mithilfe des Administrator-Tools anzeigen.

Die Lizenzdetails basieren auf allen Lizenzschlüsseln, die der Lizenz zugewiesen wurden. Der Service Manager aktualisiert die vorhandenen Lizenzdetails, wenn Sie einen neuen inkrementellen Schlüssel zur Lizenz hinzufügen.

Sie können die Lizenzdetails überprüfen und Optionen festlegen, die verfügbar sein sollen. Darüber hinaus können Sie die Lizenzdetails und Lizenznutzungsprotokolle auch beim Überwachen der Lizenzen überprüfen.

Zum Beispiel: Sie können die Anzahl der CPUs festlegen, für die Ihr Unternehmen pro Betriebssystem lizenziert ist.

Um die Lizenzdetails anzuzeigen, wählen Sie die Lizenz im **Navigator** aus.

Das Administrator-Tool zeigt die Lizezeigenschaften in den folgenden Abschnitten an:

- **Lizenzdetails:** Auf der Registerkarte **Eigenschaften** werden die Lizenzdetails angezeigt. Hier erscheinen die Attribute zu den Lizenzen, wie Lizenzobjektname, Beschreibung und Ablaufdatum.
- **Unterstützte Plattformen:** Auf der Registerkarte **Eigenschaften** werden die unterstützten Plattformen angezeigt. Hier erscheinen die Betriebssysteme und die Anzahl der unterstützten CPUs pro Betriebssystem.
- **Repositorys:** Auf der Registerkarte **Eigenschaften** werden die lizenzierten Repositorys angezeigt. Hier erscheint die maximale Anzahl der lizenzierten Repositorys.
- **Zugewiesene Dienste:** Zeigen Sie Anwendungsdienste an, die der Lizenz auf der Registerkarte **Zugewiesene Dienste** zugeordnet sind.
- **PowerCenter-Optionen:** Auf der Registerkarte **Optionen** werden die lizenzierten Repositorys angezeigt. Zeigt alle lizenzierten PowerCenter-Optionen an, z. B. Sitzung auf Gitter, hohe Verfügbarkeit und Pushdown-Optimierung.
- **Dienstoptionen:** Zeigen Sie die Dienstoptionen auf der Registerkarte **Optionen** an. Zeigt alle lizenzierten Dienste an, wie z. B. den Data Integration Service und den Modellrepository-Dienst.
- **Dienstoptionen:** Zeigen Sie die Dienstoptionen auf der Registerkarte **Optionen** an. Zeigt alle lizenzierten Dienste wie zum Beispiel den Ultra Messaging-Dienst an.
- **Verbindungen:** Auf der Registerkarte **Optionen** werden die lizenzierten Verbindungen angezeigt. Es erscheinen alle lizenzierten Verbindungen. Die Lizenz ermöglicht es Ihnen, Verbindungen wie DB2 und Oracle-Datenbankverbindungen zu nutzen.
- **Metadaten austausch-Optionen:** Zeigen Sie auf der Registerkarte **Optionen** die Metadaten austausch-Optionen an. Sie können eine Liste aller lizenzierten Metadaten austausch-Optionen anzeigen, wie z. B. Metadaten austausch für den Business-Objekte Designer.

Sie können auch den Lizenzverwaltungsbericht zur Überwachung der Lizenzen abrufen.

Lizenzdetails

Mit den Lizenzdetails können Sie Informationen auf hoher Ebene über die Lizenz abrufen. Anhand dieser Lizenzinformationen können Sie die Lizenznutzung überprüfen.

Die allgemeinen Eigenschaften für die Lizenz finden Sie im Abschnitt **Lizenzdetails** auf der Registerkarte **Eigenschaften**.

Folgende Tabelle beschreibt die allgemeinen Eigenschaften einer Lizenz.

Eigenschaft	Beschreibung
Name	Name der Lizenz.
Beschreibung	Beschreibung der Lizenz.
Speicherort	Pfad zur Lizenz im Navigator.
Edition	PowerCenter Advanced Edition
Lizenzversion	Version der Lizenz.
Herausgegeben von	Vertragshändler des Produkts.
Ausgestellt am	Datum der Lizenzvergabe an den Kunden.
Läuft ab am	Datum, an dem die Lizenz erlischt
Gültigkeitszeitraum	Gültigkeitszeitraum der Lizenz
Seriennummer	Die Seriennummer der Lizenz. Die Seriennummer kennzeichnet den Kunden oder das Projekt. Bei mehreren PowerCenter-Installationen hat jedes Projekt eine separate Seriennummer. Der Original- und der inkrementelle Schlüssel einer Lizenz haben dieselbe Seriennummer.
Bereitstellungsebene	Ebene der Bereitstellung. Die Werte sind "Entwicklung" und "Produktion."

Eigenschaft	Beschreibung
Name	Name der Lizenz.
Beschreibung	Beschreibung der Lizenz.
Speicherort	Pfad zur Lizenz im Navigator.
Edition	Typ des Lizenzschlüssels.
Lizenzversion	Version der Lizenz.
Herausgegeben von	Vertragshändler des Produkts.
Ausgestellt am	Datum, an dem die Lizenz vergeben wurde.
Läuft ab am	Datum, an dem die Lizenz abläuft.
Gültigkeitszeitraum	Gültigkeitszeitraum der Lizenz.
Seriennummer	Die Seriennummer der Lizenz. Die Seriennummer kennzeichnet den Kunden oder das Projekt. Bei mehreren PowerCenter Express-Installationen hat jedes Projekt eine separate Seriennummer. Der Original- und der inkrementelle Schlüssel einer Lizenz haben dieselbe Seriennummer.

Eigenschaft	Beschreibung
Bereitstellungsebene	Ebene der Bereitstellung. Der Wert ist "Produktion".
Anzahl Benutzer	Maximale Anzahl der Benutzer, die Sie für den PowerCenter Express-Lizenzschlüssel hinzufügen können.

Eigenschaft	Beschreibung
Name	Name der Lizenz.
Beschreibung	Beschreibung der Lizenz.
Speicherort	Pfad zur Lizenz im Navigator.
Edition	Typ des Lizenzschlüssels.
Lizenzversion	Version der Lizenz.
Herausgegeben von	Vertragshändler des Produkts.
Ausgestellt am	Datum, an dem die Lizenz vergeben wurde.
Läuft ab am	Datum, an dem die Lizenz abläuft.
Gültigkeitszeitraum	Gültigkeitszeitraum der Lizenz.
Seriennummer	Die Seriennummer der Lizenz. Die Seriennummer kennzeichnet den Kunden oder das Projekt.
Bereitstellungsebene	Ebene der Bereitstellung. Der Wert ist "Produktion".
Anzahl Benutzer	Maximale Anzahl der Benutzer, die Sie für den Lizenzschlüssel hinzufügen können.

Mit den Lizenz-Ereignisprotokollen können Sie unter anderem zusammenfassende Prüfungsberichte anzeigen. Zum Anzeigen der Logs für die Lizenzereignisse benötigen Sie die Domänenberechtigung.

Unterstützte Plattformen

Sie weisen jedem Dienst eine Lizenz zu. Der Dienst kann auf jedem Betriebssystem ausgeführt werden, das die Lizenz unterstützt. Eine Produktlizenz kann mehrere Betriebssystemplattformen unterstützen.

Die unterstützten Plattformen einer Lizenz werden im Abschnitt "Unterstützte Plattformen" der Registerkarte **Eigenschaften** angezeigt.

Die folgende Tabelle beschreibt die Eigenschaften für die unterstützten Plattformen einer Lizenz:

Eigenschaft	Beschreibung
Beschreibung	Name des unterstützten Betriebssystems.
Logische CPUs	Anzahl der CPUs, die im auf dem Betriebssystem ausgeführt werden können.
Ausgestellt am	Datum, an dem die Lizenz ausgegeben wurde.
Läuft ab	Datum, an dem die Lizenz abläuft.

Repositorys

Die maximale Anzahl aktiver Repositorys für die Lizenz erscheinen im Abschnitt Repository der Registerkarte Eigenschaften.

Die folgende Tabelle beschreibt die Repository-Eigenschaften für eine Lizenz:

Eigenschaft	Beschreibung
Beschreibung	Name des Repository
Instanzen	Anzahl der Repository-Instanzen, die auf dem Betriebssystem ausgeführt werden.
Ausgestellt am	Datum, an dem die Lizenz für diese Option ausgestellt wurde.
Läuft ab	Datum, an dem die Lizenz für diese Option abläuft.

Dienstoptionen

Die Lizenz bietet Ihnen die Möglichkeit, die Optionen des Informatica-Dienstes, wie zum Beispiel die Datenbereinigung, Datenföderation und die Pushdown-Optimierung zu nutzen.

Die Optionen für die Lizenz werden im Abschnitt PowerCenter-Optionen auf der Registerkarte **Optionen** angezeigt.

Verbindungen

Die Lizenz ermöglicht es Ihnen, Verbindungen wie DB2 und Oracle-Datenbankverbindungen zu nutzen. Die Lizenz ermöglicht Ihnen auch, Verbindungen für PowerExchange-Adapter (z. B. PowerExchange for Facebook) zu verwenden.

Die Verbindungen für die Lizenz erscheinen im Abschnitt Verbindungen der Registerkarte **Optionen**.

Metadaten austausch-Optionen

Die Lizenz bietet die Möglichkeit, Optionen für den Austausch von Metadaten zu wählen, z. B. den Metadaten austausch für den Business-Objekte Designer und für Mikrostrategien.

Die Optionen für den Austausch von Metadaten für die Lizenz erscheinen im Abschnitt Metadaten austausch-Optionen auf der Registerkarte **Optionen**.

KAPITEL 10

Log-Verwaltung

Dieses Kapitel umfasst die folgenden Themen:

- [Protokollverwaltung - Übersicht, 182](#)
- [Protokoll-Manager-Architektur, 183](#)
- [Protokollspeicherort, 185](#)
- [Log-Verwaltung - Konfiguration, 185](#)
- [Die Registerkarte Logs, 187](#)
- [Protokollereignisse, 192](#)
- [Protokoll-Aggregator, 199](#)

Protokollverwaltung - Übersicht

Der Service Manager liefert akkumulierte Protokollereignisse für Domäne, Anwendungsdienste, Benutzer sowie PowerCenter-Sitzungen und -Arbeitsabläufe. Um die Protokollierungsfunktion durchzuführen, führt der Service Manager einen Protokoll-Manager und einen Log Agent aus.

Der Protokoll-Manager wird auf dem Master-Gateway-Knoten ausgeführt. Er sammelt und verarbeitet Protokollereignisse für Domänenoperationen, Anwendungsdienste und Benutzeraktivitäten des Service Manager. Die Protokollereignisse enthalten Betriebs- und Fehlermeldungen für eine Domäne. Der Service Manager und die Anwendungsdienste senden Protokollereignisse an die Protokollverwaltung. Wenn die Protokollverwaltung Protokollereignisse empfängt, erstellt sie Protokollereignisdateien. Sie können Dienstprotokollereignisse im Administrator-Tool gemäß von Ihnen angegebenen Kriterien anzeigen.

Der Log Agent wird auf allen Knoten der Domäne ausgeführt. Der Log Agent ruft die Protokollereignisse von Sitzungen und Arbeitsabläufen ab, die von PowerCenter Integration Service geschrieben wurden, um sie im Workflow Monitor anzuzeigen. Zu den Arbeitsablaufprotokollereignissen gehören Informationen über die vom PowerCenter Integration Service ausgeführten Aufgaben, Arbeitsablaufverarbeitung und Arbeitsablauffehler. Zu den Sitzungsablaufprotokollereignissen gehören Informationen über die vom PowerCenter Integration Service ausgeführten Aufgaben, Sitzungsverarbeitung, Sitzungsfehler sowie Ladeübersichten und Umwandlungsstatistiken für die Sitzung. Sie können Protokollereignisse für den letzten ausgeführten Arbeitsablauf im Fenster Protokollereignisse im Workflow Monitor anzeigen.

Der Log Agent wird auf den Knoten ausgeführt, um für jeden Data Integration Service Protokollereignisse für Profil-Jobs, Scorecard-Jobs, Vorschau-Jobs, Mapping-Jobs und SQL-Datendienste zu sammeln und zu verarbeiten. Sie können Protokollereignisse für Profil-Jobs, Scorecard-Jobs, Vorschau-Jobs, Mapping-Jobs und SQL-Datendienste auf der Registerkarte "Überwachen" anzeigen.

Der Log Agent wird auf dem Knoten ausgeführt, um Protokollereignisse für Profil-Jobs, Vorschau-Jobs und Mapping-Jobs zu sammeln und zu verarbeiten. Sie können Protokollereignisse auf der Registerkarte "Überwachen" anzeigen.

Der Log Agent wird auf dem Knoten ausgeführt, um Protokollereignisse für Profil-Jobs, Vorschau-Jobs und Mapping-Jobs zu sammeln und zu verarbeiten. Sie können Protokollereignisse auf der Registerkarte "Überwachen" anzeigen.

Protokollereignisdateien sind Binärdateien, die vom Log Viewer des Administrator-Tools zur Anzeige von Protokollereignissen verwendet werden. Wenn Sie Protokollereignisse im Administrator-Tool anzeigen, nutzt die Protokollverwaltung die Protokollereignisdateien zur Anzeige der Protokollereignisse für Domäne, Anwendungsdienste und Benutzeraktivitäten.

Verwenden Sie das Administrator-Tool, um die folgenden Aufgaben mit der Protokollverwaltung auszuführen:

- Konfigurieren des Speicherorts für Protokolle. Konfigurieren des Knotens, auf dem die Protokollverwaltung ausgeführt wird, des Verzeichnispfads für die Protokolldateien, der Löschoptionen und der Zeitzone für Protokollereignisse.
- Konfigurieren der Protokollverwaltung. Konfigurieren der Protokollverwaltung für das automatische oder manuelle Löschen von Protokollen. Speichern von Protokollereignissen im XML-, Text- oder Binärformat. Konfigurieren der Zeitzone für den Zeitstempel in den Protokollereignisdateien.
- Anzeigen von Protokollereignissen. Anzeigen von Protokollereignissen für Domänenfunktion, Anwendungsdienst und Benutzeraktivitäten auf der Registerkarte "Protokolle". Filtern nach Domänenprotokollereignissen, Anwendungsdiensttyp und Benutzer.

Protokoll-Manager-Architektur

Der Service-Manager auf dem Master-Gateway-Knoten steuert den Protokoll-Manager. Der Protokoll-Manager startet, wenn Sie die Informatica Services starten. Nach dem Start wartet der Protokoll-Manager auf Protokollereignisse vom Service Manager und von Anwendungsdiensten. Wenn der Protokoll-Manager Protokollereignisse empfängt, erstellt er Protokollereignisdateien.

Der Protokoll-Manager wird beim Starten von PowerCenter Express aufgerufen. Nach dem Start wartet der Protokoll-Manager auf Protokollereignisse vom Service Manager und von den Anwendungsdiensten. Wenn der Protokoll-Manager Protokollereignisse empfängt, erstellt er Protokollereignisdateien.

Der Protokoll-Manager erzeugt folgenden Arten von Protokolldateien:

- Protokollereignisdateien. Speichert Protokollereignisse im Binärformat. Der Protokoll-Manager erzeugt Protokollereignisdateien zur Anzeige von Protokollereignissen auf der Registerkarte "Protokolle". Wenn Sie Ereignisse im Administrator-Tool anzeigen, ruft der Protokoll-Manager die Protokollereignisse von den Ereignis-Knoten ab.

Der Protokoll-Manager speichert die Dateien nach Datum und Knoten. Sie konfigurieren den Verzeichnispfad für den Protokoll-Manager im Administrator-Tool beim Konfigurieren von Gateway-Knoten für die Domäne. Standardmäßig wird als Verzeichnispfad das Verzeichnis server\logs verwendet.

- Dateien für die garantierte Meldungsauslieferung. Speichert Protokollereignisse für Domäne, Anwendungsdienst und Benutzeraktivität. Der Service Manager schreibt die Protokollereignisse in temporäre Dateien für die garantierte Meldungsauslieferung und sendet die Protokollereignisse an den Protokoll-Manager.

Wenn der Protokoll-Manager nicht verfügbar wird, bleibt die Datei für die garantierte Meldungsauslieferung im Verzeichnis `server\tomcat\logs` auf dem Knoten stehen, auf dem der Dienst ausgeführt wird. Wenn die Protokoll-Manager verfügbar wird, liest der Service Manager für den Knoten die Protokollereignisse aus den temporären Dateien, sendet die Protokollereignisse an den Protokoll-Manager und löscht die temporären Dateien.

Log-Ereignisse der PowerCenter-Sitzung und des Arbeitsablaufs

PowerCenter-Sitzungs- und Arbeitsablauf-Logs werden an einem Speicherort getrennt von Domänen-, Anwendungsdienst- und Benutzeraktivitäten-Logs gespeichert. Der PowerCenter Integration Service schreibt Sitzungs- und Arbeitsablauf-Log-Ereignisse in Binärdateien auf dem Knoten, auf dem der PowerCenter Integration Service läuft.

Der Log Manager führt die folgenden Tasks zur Verarbeitung der PowerCenter Sitzungs- und Arbeitsablauf-Log-Ereignisse durch:

1. Während einer Sitzung oder eines Arbeitsablaufs schreibt der PowerCenter Integration Service binäre Log-Dateien auf dem Knoten. Er sendet Informationen über die Logs an den Log Manager.
2. Der Log Manager speichert Informationen über Arbeitsablauf- und Sitzungs-Logs in der Domänenendatenbank. Die Domänenendatenbank speichert Informationen, wie z. B. den Pfad zum Speicherort der Log-Datei, den Knoten, der das Log enthält, und den PowerCenter Integration Service, der das Log erstellt hat.
3. Wenn Sie eine Sitzung oder einen Arbeitsablauf im Fenster "Log-Ereignisse" des Workflow Monitor anzeigen, ruft der Log Manager die Informationen aus der Domänenendatenbank ab. Der Log Manager verwendet die Informationen, um den Speicherort der Logs zu ermitteln.
4. Der Log Manager nutzt einen Log Agent, um die Log-Ereignisse auf den einzelnen Knoten abzurufen, die im Fenster "Log-Ereignisse" angezeigt werden.

Protokollmanager-Wiederherstellung

Wenn ein Dienst Protokollereignisse generiert, sendet er sie an die Protokollmanager auf dem Master-Gateway-Knoten. Wenn Sie über die Hochverfügbarkeitsoption verfügen und der Master-Gateway-Knoten nicht mehr erreichbar ist, senden die Anwendungsdienste Protokollereignisse an den Protokollmanager auf einem neuen Master-Gateway-Knoten.

Der Dienstmanager, die Anwendungsdienste und der Protokollmanager führen die folgenden Tasks aus:

1. Ein Anwendungsdienstprozess schreibt Protokollereignisse in eine Datei für die garantierte Meldungsauslieferung.
2. Der Anwendungsdienstprozess sendet die Protokollereignisse an den Dienstmanager auf dem Gateway-Knoten für die Domäne.
3. Der Protokollmanager verarbeitet die Protokollereignisse und schreibt Protokollereignis-Dateien. Der Anwendungsdienstprozess löscht die temporäre Datei.
4. Wenn der Protokollmanager nicht verfügbar ist, bleibt die Datei für die garantierte Meldungsauslieferung auf dem Knoten, auf dem der Dienstprozess läuft. Der Dienstmanager für den Knoten sendet die Protokollereignisse in den Dateien für die garantierte Meldungsauslieferung, wenn der Protokollmanager wieder bereitsteht, und der Protokollmanager schreibt die Protokollereignis-Dateien.

Fehlersuche für den Log Manager

Domänen- und Anwendungsdienste schreiben Protokollereignisse in die Dienstmanager-Protokolldateien, wenn der Protokollmanager keine Protokollereignisse verarbeiten kann. Die Dienstmanager-Protokolldateien befinden sich im Standardprotokollverzeichnis. Zu den Service Manager-Log-Dateien gehören catalina.out, localhost_<date>.txt, und node.log. Dienste schreiben Log-Ereignisse in unterschiedliche Log-Dateien, abhängig von der Art des Fehlers.

Verwenden Sie die Service Manager-Log-Dateien, um Probleme zu beheben, wenn der Log Manager Log-Ereignisse nicht verarbeiten kann. Außerdem benötigen Sie diese Dateien auch zum Beheben von Problemen, wenn Sie sich an den globalen Kundensupport von Informatica wenden.

Hinweis: Sie können Fehler in einer Informatica-Installation beheben, wenn Sie die Log-Dateien benutzen, die während der Installation generiert wurden. Sie können die zusammenfassende Log-Datei der Installation benutzen, um herauszufinden, welche Komponenten bei der Installation gescheitert sind.

Protokollspeicherort

Der Service Manager im Master-Gateway-Knoten schreibt Domänen-, Anwendungsdienst- und Benutzeraktivitäts-Protokollereignisdateien ins Protokolldateiverzeichnis. Wenn Sie einen Knoten für die Verwendung als Gateway konfigurieren, müssen Sie das Verzeichnis konfigurieren, in das der Service Manager des Knotens die Protokollereignisdateien schreibt. Jeder Gateway-Knoten muss Zugriff auf den Verzeichnispfad haben.

Konfigurieren Sie den Protokollspeicherort in der Ansicht "Eigenschaften" für die Domäne. Konfigurieren Sie einen Verzeichnisspeicherort, auf den beim Installieren oder beim Definieren der Domäne zugegriffen werden kann. Haben Sie mehr als einem Gateway-Knoten, speichern Sie die Protokolle auf einem gemeinsamen Laufwerk. Ist der Protokoll-Manager nicht in der Lage, in den Verzeichnispfad zu schreiben, schreibt er die Protokollereignisse in node.log auf dem Master-Gateway-Knoten.

Als standardmäßiger Verzeichnispfad wird das Verzeichnis server\logs verwendet. Beim Konfigurieren des Protokollspeicherorts validiert das Administrator-Tool das Verzeichnis während der Konfigurationsaktualisierung. Ist das Verzeichnis ungültig, schlägt die Aktualisierung fehl. Der Protokoll-Manager überprüft, dass das Protokollverzeichnis nach dem Starten über Lese- und Schreibberechtigung verfügt. Erfolgt die gemeinsame Nutzung des Protokollverzeichnisses nicht in einer hochverfügbaren Umgebung, besteht die Gefahr, dass die Protokolldateien Widersprüche aufweisen.

Bei mehreren Informatica-Domänen müssen Sie einen anderen Verzeichnispfad für den Protokoll-Manager in jeder Domäne konfigurieren. Die gemeinsame Nutzung desselben Verzeichnissespfades durch mehrere Domänen ist nicht möglich.

Hinweis: Wenn Sie den Verzeichnispfad ändern, müssen Sie die Informatica Services auf dem Knoten neu starten, den Sie geändert haben.

Hinweis: Wenn Sie den Verzeichnispfad ändern, müssen Sie PowerCenter Express neu starten.

Log-Verwaltung - Konfiguration

Der Service Manager und die Anwendungsdienste senden kontinuierlich Log-Ereignisse an den Log Manager. Im Laufe der Zeit kann der Inhalt des Verzeichnisses eine große Anzahl von Log-Ereignissen enthalten.

Sie können die Log-Ereignisse periodisch löschen, um die Anzahl der im Log Manager gespeicherten Log-Ereignisse optimal zu verwalten. Sie können die Logs vor dem Löschen exportieren und eine Sicherungskopie der älteren Log-Ereignisse aufbewahren.

Bereinigen von Log-Ereignissen.

Sie können Log-Ereignisse automatisch oder manuell entfernen. Der Service Manager entfernt die Log-Ereignisse gemäß den Bereinigungseigenschaften aus dem Log-Verzeichnis. Die Bereinigungseigenschaften definieren Sie im Dialogfeld "Log-Verwaltung". Sie können Log-Ereignisse manuell bereinigen, um die automatischen Bereinigungseigenschaften zu überschreiben.

Löschen von Protokollereignissen - Automatisch

Der Service Manager entfernt die Protokollereignisse gemäß den Bereinigungseigenschaften aus dem Protokollverzeichnis. Der Standardwert für die Aufbewahrung von Protokollen beträgt 30 Tage und die maximale Standardgröße für Protokollereignisdateien ist 200 MB.

Wenn die Anzahl der Tage oder die Größe des Protokollverzeichnisses die Grenze überschreitet, löscht der Log-Manager die Protokollereignisdateien, beginnend beim ältesten Protokollereignis. Der Protokoll-Manager prüft periodisch die Bereinigungsoptionen und entfernt die Protokollereignisse. Der Protokoll-Manager entfernt nicht die Ereignisdaten und den Ereignisordner des aktuellen Tages.

Hinweis: Der Log-Manager entfernt keine PowerCenter-Sitzungs- und Arbeitsablaufprotokolldateien.

Löschen von Log-Ereignissen - Manuell

Sie können Log-Ereignisse für die Domäne, Anwendungsdienste oder Benutzeraktivität löschen. Beim Löschen von Log-Ereignissen entfernt der Log Manager die Log-Ereignisdateien aus dem Log-Verzeichnis. Der Log Manager entfernt die Log-Ereignisdateien nicht, die derzeit in die Logs geschrieben werden.

Optional können Sie den Befehl `infacmd PurgeLog` zum Löschen von Log-Ereignissen verwenden.

In der folgenden Tabelle sind die Optionen für das Löschen von Logs aufgelistet:

Option	Beschreibung
Log-Typ	Typ des zu löschenden Log-Ereignisses. Sie können Domänen-, Dienst-, Benutzeraktivitäten- oder alle Log-Ereignisse löschen.
Diensttyp	Beim Löschen von Anwendungsdienst-Log-Ereignissen können Sie Log-Ereignisse für einen bestimmten Anwendungsdiensttyp oder für alle Anwendungsdiensttypen löschen.
Einträge bereinigen	Datumsbereich der zu löschenden Log-Ereignisse. Sie können die folgenden Optionen wählen: <ul style="list-style-type: none">- Alle Einträge Löscht alle Log-Ereignisse.- Vor Datum Löscht Log-Ereignisse, die vor diesem Datum eingetreten sind. Verwenden Sie zur Eingabe des Datums das Format yyyy-mm-dd. Optional können Sie den das Datum mithilfe des Kalenders auswählen. Um den Kalender zu verwenden, klicken Sie auf das Datumsfeld.

Zeitzone

Wenn der Log Manager Log-Ereignisdateien erstellt, generiert er basierend auf der Zeitzone für jedes Log-Ereignis einen Zeitstempel. Erstellt der Log Manager Log-Ordner, beschriftet er die Ordner entsprechend einem Zeitstempel. Beim Exportieren oder Bereinigen von Log-Ereignisdateien verwendet der Log Manager diese Eigenschaft für die Berechnung, welche Log-Ereignisdateien bereinigt oder exportiert werden sollen.

Stellen Sie als Zeitzone den Speicherort des Computers ein, auf dem die Log-Ereignisdateien gespeichert sind.

Überprüfen Sie, dass Sie keine Log-Ereignisdateien verlieren, wenn Sie die Zeitzone für den Log Manager konfigurieren. Befindet sich der Anwendungsdienst, der die Log-Ereignisse zum Log Manager überträgt, in einer anderen Zeitzone als der Master-Gateway-Knoten, verlieren Sie möglicherweise Log-Ereignisdateien, die Sie eigentlich nicht löschen wollten. Konfigurieren Sie für jeden Gateway-Knoten dieselbe Zeitzone.

Hinweis: Beim Ändern der Zeitzone müssen Sie Informatica Services auf dem geänderten Knoten neu starten.

Log-Management-Eigenschaften konfigurieren

Konfigurieren Sie die Protokollverwaltungseigenschaften in Informatica Administrator im Dialogfeld **Protokollverwaltung**.

1. Klicken Sie in der Administrator Console auf die Registerkarte **Protokolle**.
2. Wählen Sie **Protokollaktionen > Protokollverwaltung** aus.
3. Geben Sie die Anzahl von Tagen an, die der Log Manager die Log-Events aufbewahren soll.
4. Geben Sie die maximale Festplattenspeichergröße für das Verzeichnis an, das die Log-Ereignisdateien enthält.
5. Geben Sie die Zeitzone im folgenden Format an:
`GMT (+|-) <hours>:<minutes>`
Beispiel: GMT+08:00
6. Klicken Sie auf **OK**.

Die Registerkarte Logs

Auf der Registerkarte Logs des Administrator Tool können Sie Domänen, Anwendungsdienste und Log-Ereignisse für Benutzeraktivitäten anzeigen. Wenn Sie Log-Ereignisse auf der Registerkarte Logs anzeigen, erscheinen die generierten Log-Ereignisdateien im Log-Verzeichnis des Log-Manager. Erscheint eine Fehlermeldung im Administrator Tool, enthält diese einen Link zur Registerkarte Logs.

Die Registerkarte Logs lässt sich für folgende Aufgaben verwenden:

- Anzeigen von Log-Ereignissen und Operationsfehlern des Administrator Tools. Anzeigen von Log-Ereignissen für die Domäne, eines Anwendungsdienstes oder einer Benutzeraktivität.
- Zum Filtern der Ergebnisse von Log-Ereignissen. Nach der Anzeige der Log-Ereignisse können Sie diese nach bestimmten Kriterien filtern.
- Konfigurieren von Spalten. Legen Sie fest, welche Spalten auf der Registerkarte Logs erscheinen sollen.
- Speichern von Log-Ereignissen. Sie können Log-Ereignisse im Format XML, im Textformat oder im Binärformat abspeichern.
- Löschen von Log-Ereignissen. Sie können Log-Ereignisse manuell entfernen.
- Kopieren der Log-Ereignisse. Die Zeilen der einzelnen Log-Ereignisse lassen sich kopieren.

Anzeigen von Protokollereignissen

Um Protokollereignisse auf der Registerkarte "Protokolle" des Administrator-Tools anzuzeigen, wählen Sie die Domänenansicht, die Dienstanzeige oder die Benutzeraktivitätsansicht aus. Konfigurieren Sie dann die

Filteroptionen. Sie können die Protokollereignisse auf der Basis der Attribute (z. B. Logtyp, Domänenfunktionskategorie, Anwendungsdiensttyp, Anwendungsdienstname, Benutzer, Meldungscode, Aktivitätscode, Zeitstempel und Sicherheitslevel) filtern. Welche Option verfügbar ist, hängt davon ab, ob Sie Ereignisse der Domäne des Anwendungsdienstes oder der Benutzeraktivitätsprotokolle anzeigen.

Um weitere Informationen zu einem Protokollereignis anzuzeigen, klicken Sie in den Suchergebnissen auf das Protokollereignis.

Wenn der Protokoll-Manager eine interne Fehlermeldung vom PowerCenter Integration Service erhält, wird unter AIX und Linux ein Stacktrace in das Protokollereignisfenster geschrieben.

Sie können die Protokolle anzeigen, um zusätzliche Informationen über Fehler zu bekommen, die Sie während der Arbeit im Administrator-Tool erhalten haben.

1. Klicken Sie im Administrator-Tool auf die Registerkarte "Protokolle".
2. Wählen Sie im Inhaltsbereich die Ansicht "Domäne", "Dienst" oder "Benutzeraktivität" aus.
3. Konfigurieren Sie die Filterkriterien, um einen bestimmten Protokollereignistyp anzuzeigen.

In der folgenden Tabelle sind die Abfragemöglichkeiten aufgelistet:

Protokolltyp	Option	Beschreibung
Domäne	Kategorie	Die Kategorie des Domänendienstes, die Sie anzeigen möchten.
Dienst	Diensttyp	Der Anwendungsdienst, den Sie anzeigen möchten.
Dienst	Dienstname	Name des Anwendungsdienstes, für den Protokollereignisse angezeigt werden sollen. Sie können den Namen eines einzelnen Anwendungsdienstes wählen oder alle Anwendungsdienste.
Domäne Dienst	Schweregrad	Der Log-Manager gibt die Protokollereignisse mit dem zugehörigen Schweregrad aus.
Benutzeraktivität	Benutzer	Name des Benutzers des Administrator-Tools
Benutzeraktivität	Sicherheitsdomäne	Sicherheitsdomäne, zu welcher der Benutzer gehört.
Domäne Dienst, Benutzeraktivität	Zeitstempel	Datenbereich für Protokollereignisse, die Sie anzeigen möchten. Sie können die folgenden Optionen wählen: <ul style="list-style-type: none"> - Leer. Zeigt alle Protokollereignisse an. - Innerhalb des letzten Tages - Innerhalb des letzten Monats - Benutzerdefiniert Gibt Start- und Enddatum an. Voreinstellung ist "Innerhalb des letzten Tages"
Domäne Dienst	Thread	Filterkriterien für Text, der in Thread-Daten erscheint. In diesem Textfeld können Sie Platzhalter (*) verwenden.
Domäne Dienst	Meldungscode	Filterkriterien für Text, der in Meldungscode erscheint. In diesem Textfeld können Sie Platzhalter (*) verwenden.

Protokolltyp	Option	Beschreibung
Domäne Dienst	Meldung	Filterkriterien für Text, der in Meldungscode erscheint. In diesem Textfeld können Sie Platzhalter (*) verwenden.
Domäne Dienst	Knoten	Name des Knotens, für den Protokollereignisse angezeigt werden sollen.
Domäne, Dienst	Prozess	Die Prozessidentifikationsnummer derjenigen Windows- oder UNIX-Dienstprozesse, die das Protokollereignis generiert haben. Sie können die Prozessidentifikationsnummer dazu nutzen, Protokollereignisse von einem Prozess zu identifizieren, wenn ein Anwendungsdienst mehrere Prozesse auf demselben Knoten ausführt.
Benutzeraktivität	Aktivitätscode	Filterkriterien für Text, der im Aktivitätscode erscheint. In diesem Textfeld können Sie Platzhalter (*) verwenden.
Benutzeraktivität	Aktivität	Filterkriterien für Text, der in der Aktivität erscheint. In diesem Textfeld können Sie Platzhalter (*) verwenden.

4. Klicken Sie auf die Schaltfläche "Filter".

Der Log-Manager ruft die Protokollereignisse ab und zeigt sie in der Registerkarte "Protokolle" an, wobei das zuletzt eingetretene Protokollereignis zuerst angezeigt wird.

5. Klicken Sie auf die Schaltfläche "Filter zurücksetzen", um einen anderen Satz an Protokollereignissen anzuzeigen.

Tipp: Um nach Protokollen zu suchen, die zu einem Fehler oder einem fatalen Protokollereignis gehören, beachten Sie den Zeitstempel auf dem Protokollereignis. Setzen Sie dann den Filter zurück und verwenden Sie einen benutzerdefinierten Filter, um nach weiteren Protokollereignissen zu suchen, die während des Zeitstempels des Ereignisses aufgetreten sind.

Konfigurieren von Log-Spalten

Die Registerkarte Logs können Sie so konfigurieren, dass sie folgende Spalten aufweist:

- Kategorie
- Diensttyp
- Dienstname
- Schweregrad
- Benutzer
- Sicherheitsdomäne
- Zeitstempel
- Thread
- Meldungscode
- Meldung
- Knoten
- Prozess
- Aktivitätscode
- Aktivität

Hinweis: Die Spalten werden basierend auf den von Ihnen gewählten Abfrageoptionen angezeigt. Zeigen Sie zum Beispiel einen Diensttyp an, steht der Dienstname auf der Registerkarte Logs.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Logs**.
2. Wählen Sie die Ansicht **Domäne, Dienst** oder **Benutzeraktivität**.
3. Um eine Spalte hinzuzufügen, klicken Sie mit der rechten Maustaste auf einen Spaltennamen, wählen Sie **Spalten** und danach auf den Namen der Spalte, die Sie hinzufügen möchten.
4. Zum Entfernen einer Spalte klicken Sie mit der rechten Maustaste auf einen Spaltennamen, wählen Sie **Spalten** und löschen Sie die Markierung neben dem Spaltennamen, den Sie entfernen möchten.
5. Wenn Sie eine Spalte verschieben möchten, wählen Sie den Spaltennamen und ziehen Sie ihn an die Stelle, an der er stehen soll.

Der Log Manager aktualisiert die Spalten auf der Registerkarte Logs gemäß Ihren Angaben.

Speichern von Log-Ereignissen

Sie können die Log-Ereignisse speichern, die Sie im Log Viewer filtern und anzeigen. Wenn Sie Log-Ereignisse speichern, speichert der Log Manager die von Ihnen entsprechend den Filterkriterien angezeigten Logs. Um Log-Ereignisse in einer Datei zu speichern, klicken Sie im Log-Aktionen-Menü auf "Logs speichern".

Der Log Manager löscht die Log-Ereignisse nicht, wenn Sie sie speichern. Das Administrator Tool fordert Sie auf, die gespeicherte Datei der Log-Ereignisse zu speichern oder zu öffnen.

Optional können Sie mit dem Befehl *infacmd isp GetLog* Log-Ereignisse abrufen.

Das von Ihnen gewählte Format zum Speichern von Log-Ereignissen hängt davon ab, wie Sie die exportierte Datei der Log-Ereignisse verwenden möchten:

- XML-Datei Verwenden Sie das XML-Format, wenn Sie die Log-Ereignisse in einem externen Tool analysieren möchten, das XML verwendet, oder wenn Sie XML-Tools wie zum Beispiel XSLT benutzen möchten.
- Textdatei. Verwenden Sie eine Text-Datei, wenn Sie die Log-Ereignisse in einem Texteditor analysieren möchten.
- Binärdatei. Verwenden Sie das Binärformat, um die Log-Ereignisse im binären Format zu sichern. Möglicherweise müssen Sie dieses Format verwenden, um Log-Ereignisse an den globalen Kundensupport von Informatica zu senden.

Exportieren von Log-Ereignissen

Sie können die Log-Ereignisse im Format XML, im Textformat oder im Binärformat abspeichern. Um Log-Ereignisse in eine Datei zu exportieren, klicken Sie im Menü Log-Aktionen auf Logs exportieren.

Beim Exportieren von Log-Ereignissen können Sie wählen, welche Logs Sie speichern möchten. Wenn Sie Dienst-Logs gewählt haben, können Sie Logs für einen bestimmten Diensttyp exportieren. Sie können die Sortierreihenfolge für die Log-Ereignisse in der Exportdatei auswählen.

Die exportierten Log-Ereignisse werden nicht vom Log-Manager gelöscht. Das Administrator Tool fordert Sie auf, die exportierte Log-Ereignisdatei zu speichern oder zu öffnen.

Optional können Sie Log-Ereignisse auch mit dem GetLog-Befehl *infacmd* abrufen.

Welches Format Sie zum Exportieren von Log-Ereignissen auswählen, ist davon abhängig, wie Sie die exportierte Log-Ereignisdatei verwenden möchten:

- **XML-Datei** Verwenden Sie das XML-Format, wenn Sie die Log-Ereignisse in einem externen Tool analysieren möchten, das XML verwendet, oder wenn Sie XML-Tools wie zum Beispiel XSLT benutzen möchten.
- **Textdatei.** Verwenden Sie eine Text-Datei, wenn Sie die Log-Ereignisse in einem Texteditor analysieren möchten.
- **Binärdatei.** Verwenden Sie das Binärformat, um die Log-Ereignisse im binären Format zu sichern. Möglicherweise müssen Sie dieses Format verwenden, um Log-Ereignisse an den globalen Kundensupport von Informatica zu senden.

Die folgende Tabelle beschreibt die Optionen zum Export von Logs für die einzelnen Logtypen:

Option	Log-Typ	Beschreibung
Typ	Domäne, Dienst, Benutzeraktivität	Geben Sie die Logs an, die Sie exportieren möchten.
Diensttyp	Dienst	Typ des Anwendungsdienstes, für den Log-Ereignisse exportiert werden sollen. Sie können auch Log-Ereignisse für alle Diensttypen exportieren.
Exportieren von Einträgen	Domäne, Dienst, Benutzeraktivität	Datumsbereich der Log-Ereignisse, die Sie exportieren möchten. Sie können die folgenden Optionen wählen: <ul style="list-style-type: none"> - Alle Einträge Exportiert alle Log-Ereignisse. - Vor Datum. Exportiert Log-Ereignisse, die vor dem angegebenen Datum eingetreten sind. Das Datum muss im Format yyyy-mm-dd eingegeben werden. Optional können Sie das Datum auch aus dem Kalender auswählen. Um den Kalender zu benutzen, klicken Sie auf das Datumsfeld.
Exportieren von Logs in absteigender chronologischer Reihenfolge	Domäne, Dienst, Benutzeraktivität	Exportiert Log-Ereignisse beginnend mit dem neuesten Log-Ereignis.

XML-Format

Wenn Sie Log-Ereignisse in eine XML-Datei exportieren, exportiert der Log-Manager jedes Log-Ereignis als separates Element in die XML-Datei. Das nachstehende Beispiel zeigt einen Auszug aus einer XML-Datei mit Log-Ereignissen:

```
<log xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:common="http://
www.informatica.com/pcsf/common" xmlns:metadata="http://www.informatica.com/pcsf/
metadata" xmlns:domainservice="http://www.informatica.com/pcsf/domainservice"
xmlns:logservice="http://www.informatica.com/pcsf/logservice" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">
<logEvent xsi:type="logservice:LogEvent" objVersion="1.0.0" timestamp="1129098642698"
severity="3" messageCode="AUTHEN_USER_LOGIN_SUCCEEDED" message="User Admin successfully
logged in." user="Admin" stacktrace="" service="authenticationservice"
serviceType="PCSF" clientNode="sapphire" pid="0" threadName="http-8080-Processor24"
context="" />
<logEvent xsi:type="logservice:LogEvent" objVersion="1.0.0" timestamp="1129098517000"
severity="3" messageCode="LM 36854" message="Connected to node [garnet] on outbound
connection [id = 2]." user="" stacktrace="" service="Copper" serviceType="IS"
clientNode="sapphire" pid="4484" threadName="4528" context="" />
```

Text-Format

Wenn Sie Log-Ereignisse in eine Textdatei exportieren, exportiert der Log-Manager die Log-Ereignisse in ein ICE-Protokoll (Information and Content Exchange). Das nachstehende Beispiel zeigt einen Auszug aus einer Textdatei mit Log-Ereignissen:

```
2006-02-27 12:29:41 : INFO : (2628 | 2768) : (IS | Copper) : sapphire : LM_36522 :  
Started process [pid = 2852] for task instance Session task instance  
[s_DP_m_DP_AP_T_DISTRIBUTORS4]:Executor - Master.  
2006-02-27 12:29:41 : INFO : (2628 | 2760) : (IS | Copper) : sapphire : CMN_1053 :  
Starting process [Session task instance [s_DP_m_DP_AP_T_DISTRIBUTORS4]:Executor -  
Master].  
2006-02-27 12:29:36 : INFO : (2628 | 2760) : (IS | Copper) : sapphire : LM_36522 :  
Started process [pid = 2632] for task instance Session task instance  
[s_DP_m_DP_AP_T_DISTRIBUTORS4]:Preparer.  
2006-02-27 12:29:35 : INFO : (2628 | 2760) : (IS | Copper) : sapphire : CMN_1053 :  
Starting process [Session task instance [s_DP_m_DP_AP_T_DISTRIBUTORS4]:Preparer].
```

Binärformat

Wenn Sie Log-Ereignisse in eine Binärdatei exportieren, exportiert der Log-Manager die Log-Ereignisse in eine Datei, die der globale Kundensupport von Informatica importieren kann. Sie können die Datei erst anzeigen, wenn Sie diese in Text konvertiert haben. Verwenden Sie den Befehl *infacmd* ConvertLogFile, um die Log-Datei im Binärformat in Textdateien, XML-Dateien oder auf dem Bildschirm lesbaren Text zu konvertieren.

Fehlerprotokoll im Administrator Tool

Wenn ein Fehler auftritt, während Sie einen Dienst im Administrator Tool starten, aktualisieren oder entfernen, erscheint im Inhaltsbereich des Dienstes eine Fehlermeldung, die einen Link zur Registerkarte Logs enthält. Klicken Sie diesen Link in der Fehlermeldung an, um detaillierte Informationen über den Fehler in der Registerkarte Logs zu finden.

Protokollereignisse

Der Dienstmanager und die Anwendungsdienste senden kontinuierlich Protokollereignisse an den Protokollmanager. Der Protokollmanager generiert Protokollereignisse für jeden Diensttyp.

Sie können die folgenden Protokollereignistypen auf der Registerkarte „Protokolle“ anzeigen:

- Domänenprotokollereignisse Von Dienstmanager-Funktionen generierte Protokollereignisse.
- Protokollereignisse im Analyst-Dienst. Protokollereignisse zu den einzelnen Analyst-Diensten, die in der Domäne ausgeführt werden.
- Content-Managementdienst-Protokollereignisse. Protokollereignisse zu jedem in der Domäne ausgeführten Content-Managementdienst.
- Datenintegrationsdienst-Protokollereignisse. Protokollereignisse zu den einzelnen Datenintegrationsdiensten, die in der Domäne ausgeführt werden.
- Datenintegrationsdienst-Protokollereignisse. Protokollereignisse zum Datenintegrationsdienst, der in der Domäne ausgeführt wird.
- Protokollereignisse des Metadata Manager-Diensts. Protokollereignisse zu den einzelnen Metadata Manager-Diensten, die in der Domäne ausgeführt werden.
- Protokollereignisse des Modellrepository. Protokollereignisse zu den einzelnen Modellrepository-Diensten, die in der Domäne ausgeführt werden.

- Protokollereignisse des Modellrepository. Protokollereignisse zum Modellrepository-Dienst, der in der Domäne ausgeführt wird.
- Protokollereignisse des PowerCenter-Integrationsdiensts. Protokollereignisse zu den einzelnen PowerCenter-Integrationsdiensten, die in der Domäne ausgeführt werden.
- Protokollereignisse des PowerCenter-Repository-Diensts. Protokollereignisse von den einzelnen PowerCenter-Repository-Diensten, die in der Domäne ausgeführt werden.
- Protokollereignisse des Berichterstellungsdiensts. Protokollereignisse von den einzelnen Berichterstellungsdiensten, die in der Domäne ausgeführt werden.
- Protokollereignisse des SAP BW-Diensts. Protokollereignisse zur Interaktion zwischen dem PowerCenter und dem SAP NetWeaver BI-System.
- Protokollereignisse des Webdienst-Hub. Protokollereignisse zur Interaktion zwischen Anwendungen und dem Webdienst-Hub.
- Ultra Messaging Service-Protokollereignisse. Protokollereignisse zum Ultra Messaging Service, der in der Domäne ausgeführt wird.
- Protokollereignisse der Benutzeraktivität. Protokollereignisse zu Domänen und des Sicherheitsmanagement-Aufgaben, die ein Benutzer ausführt.

Protokollereignisse - Komponenten

Der Log Manager verwendet ein gemeinsames Format zum Speichern und Anzeigen von Protokollereignissen. Die Komponenten der Protokollereignisse können zur Fehlerbehebung bei Informatica verwendet werden.

Jedes Protokollereignis enthält folgende Komponenten:

- Diensttyp, Kategorie oder Benutzer. Auf der Registerkarte Logs sind die Ereignisse nach Domänenkategorie, Diensttyp oder Benutzer kategorisiert. Wenn Sie Anwendungsdienst-Logs anzeigen, enthält die Registerkarte Logs die Namen der Anwendungsdienste. Wenn Sie Domänen-Logs anzeigen, enthält die Registerkarte Logs die Domänenkategorien im Log. Wenn Sie Benutzeraktivitäten-Logs anzeigen, enthält die Registerkarte Logs die Benutzer im Log.
- Meldung oder Aktivität. Meldungs- oder Aktivitätstext für das Protokollereignis. Verwenden Sie den Meldungstext, um weitere Informationen zu den Protokollereignissen für Domänen- und Anwendungsdienste zu erhalten. Verwenden Sie den Aktivitätstext, um weitere Informationen zu den Protokollereignissen für Benutzeraktivitäten zu erhalten. Einige Protokollereignisse enthalten eingebettete Protokollereignisse in den Meldungstexten. Das folgende Protokollereignis enthält beispielsweise ein eingebettetes Protokollereignis:

```
Client application [PmDTM], connection [59]: recv failed.
```

Bei diesem Protokollereignis ist das folgende Protokollereignis das eingebettete Protokollereignis:

```
[PmDTM], connection [59]: recv failed.
```

Wenn der Log Manager das Protokollereignis anzeigt, wird der Schweregrad für das eingebettete Protokollereignis angezeigt.

- Meldung oder Aktivität. Meldungs- oder Aktivitätstext für das Protokollereignis. Verwenden Sie den Meldungstext, um weitere Informationen zu den Protokollereignissen für Domänen- und Anwendungsdienste zu erhalten. Verwenden Sie den Aktivitätstext, um weitere Informationen zu den Protokollereignissen für Benutzeraktivitäten zu erhalten. Einige Protokollereignisse enthalten eingebettete Protokollereignisse in den Meldungstexten. Das folgende Protokollereignis enthält beispielsweise ein eingebettetes Protokollereignis:

```
Client application [PmDTM], connection [59]: recv failed.
```

Bei diesem Protokollereignis ist das folgende Protokollereignis das eingebettete Protokollereignis:

```
[PmDTM], connection [59]: recv failed.
```

Wenn der Log Manager das Protokollereignis anzeigt, wird der Schweregrad für das eingebettete Protokollereignis angezeigt.

- Meldung oder Aktivität. Meldungs- oder Aktivitätstext für das Protokollereignis. Verwenden Sie den Meldungstext, um weitere Informationen zu den Protokollereignissen für Domänen- und Anwendungsdienste zu erhalten. Verwenden Sie den Aktivitätstext, um weitere Informationen zu den Protokollereignissen für Benutzeraktivitäten zu erhalten. Einige Protokollereignisse enthalten eingebettete Protokollereignisse in den Meldungstexten.

Wenn der Log Manager das Protokollereignis anzeigt, wird der Schweregrad für das eingebettete Protokollereignis angezeigt.

- Sicherheitsdomäne. Wenn Sie Benutzeraktivitäten-Logs anzeigen, enthält die Registerkarte Logs die Sicherheitsdomäne für die einzelnen Benutzer.
- Meldungs- oder Aktivitätscode. Protokollereigniscode. Wenn der Meldungstyp einen Fehler oder einen schwerwiegenden Fehler darstellt, klicken Sie auf den Meldungscode, um die Informatica-Wissensdatenbank zu öffnen und die Nachricht zu suchen. Sie müssen Anmeldedaten für das Supportportal im Benutzerkonto konfigurieren, um die Suche durchzuführen.
- Prozess Die Prozessidentifikationsnummer des Windows- oder UNIX-Dienstprozesses, der das Protokollereignis generiert hat. Sie können die Prozessidentifikationsnummer dazu nutzen, Protokollereignisse von einem Prozess zu identifizieren, wenn ein Anwendungsdienst mehrere Prozesse auf demselben Knoten ausführt.
- Knoten Name des Knotens, auf dem der Prozess ausgeführt wird, der das Protokollereignis generiert hat.
- Thread Identifikationsnummer oder Namen des von einem Dienstprozess gestarteten Threads.
- Zeitstempel Datum und Uhrzeit, wann das Protokollereignis eintrat.
- Schweregrad Der Schweregrad für das Protokollereignis. Wenn Sie Protokollereignisse anzeigen, können Sie die Registerkarte Logs so konfigurieren, dass Protokollereignisse für einen bestimmten Schweregrad angezeigt werden.

Domänenprotokollereignisse

Domänenprotokollereignisse sind Protokollereignisse, die von den vom Service Manager ausgeführten Domänenfunktionen generiert werden. Anhand von Domänenprotokollereignissen können Sie Informationen über die Domäne und Fehlersuchprobleme einblenden. Die Domänenprotokollereignisse können zur Fehlersuche bei Problemen während des Hochfahrens und der Initialisierung der Knoten und Anwendungsdienste für die Domäne genutzt werden.

Domänenprotokollereignisse umfassen Protokollereignisse der folgenden Funktionen:

- Autorisierung. Diese Protokollereignisse treten auf, wenn der Service Manager Benutzeranfragen für die Dienste autorisiert. Anfragen können vom Administrator-Tool ausgehen.
- Domänenkonfiguration. Protokollereignisse, die bei der Verwaltung der Domänenkonfigurations-Metadaten durch den Service Manager auftreten.
- Knotenkonfiguration. Protokollereignisse, die bei der Verwaltung der Knotenkonfigurations-Metadaten in der Domäne durch den Service Manager auftreten.
- Lizenzierung. Protokollereignisse, die beim Registrieren von Lizenzinformationen durch den Service Manager auftreten.
- Lizenznutzung. Diese Protokollereignisse treten auf, wenn der Service Manager Lizenzinformationen der Anwendungsdienste überprüft.

- **Protokoll-Manager.** Protokollereignisse des Log-Managers. Der Log-Manager wird auf dem Master-Gateway-Knoten ausgeführt. Er erfasst und verarbeitet Protokollereignisse für Service-Manager-Domänenoperationen und Anwendungsdienste.
- **Log Agent.** Protokollereignisse des Log Agent. Der Log Agent wird auf allen Knoten der Domäne ausgeführt. Er ruft PowerCenter-Arbeitsablauf- und Sitzungs-Protokollereignisse ab, um sie zur Überwachung des Arbeitsablaufs anzuzeigen.
- **Überwachen.** Protokollereignisse zu Domänenfunktionen.
- **Benutzerverwaltung.** Protokollereignisse, die eintreten, wenn der Service Manager Benutzer, Gruppen und Berechtigungen verwaltet.
- **Service Manager.** Protokollereignisse des Service Managers und Signalausnahmen von DTM-Prozessen. Der Service Manager verwaltet alle Domänenoperationen. Wurde der Fehlerschweregrad eines Knotens beim Starten des Dienstes auf Debug gesetzt, umfassen die Protokollereignisse die von diesem Dienst verwendeten Umgebungsvariablen.

Log-Ereignisse im Analyst Service

Log-Ereignisse im Analyst Service enthalten die folgenden Informationen

- **Projektverwaltung.** Log-Ereignisse zum Verwalten der Projekte im Informatica Analyst, z.B. zum Erstellen von Objekten, Ordnen und Projekten. Log-Ereignisse zum Erstellen von Profilen, Scorecards und Referenztabellen.
- **Jobs ausführen.** Log-Ereignisse zum Ausführen von Profilen und Scorecards. Logs über die Vorschau von Daten.
- **Benutzerberechtigungen** Log-Ereignisse über die Verwaltung von Benutzerberechtigungen in Projekten.

Protokollereignisse des Data Integration Service

Die Data Integration-Service-Protokolle enthalten Protokolle zu folgenden Ereignissen:

- **Konfiguration.** Protokollereignisse über Änderungen der Dienstkonfiguration, Anwendungsbereitstellung oder -entfernung und Protokolle über das zugehörige Profiling Warehouse.
- **Data Integration Service - Prozesse** Protokollereignisse über die Anwendungsbereitstellung, Data Object Cacheaktualisierung und Benutzeranfragen zum Ausführen von Mappings, Jobs oder Arbeitsabläufen.
- **Systemfehler.** Protokollereignisse über Fehler, die die Verfügbarkeit des Data Integration Service verhindern, z.B. Verbindungsfehler des Model Repository oder Fehler beim Start eines Dienstes.

Log-Ereignisse des Listener Service

Die Protokolle des PowerExchange Listener enthalten Informationen über den Anwendungsdienst, der den PowerExchange Listener verwaltet.

Die Protokolle des Listener Service enthalten die folgenden Informationen:

- **Client-Kommunikation.** Log-Ereignisse zur Kommunikation zwischen dem PowerCenter oder dem PowerExchange-Client und der Datenquelle.
- **Listener Service.** Log-Ereignisse zum Listener Service, einschließlich der Konfiguration, Aktivierung und Deaktivierung des Dienstes.
- **Operationen des Listener Service.** Log-Ereignisse zu Operationen wie Verwalten von Massendatenverschiebungen und Erfassen von Änderungsdaten.

Logger Service Konfigurationseigenschaften

Die Logs des PowerExchange Logger Service enthalten Informationen über den Anwendungsdienst, der den PowerExchange Logger verwaltet.

Der Logger Service enthält die folgenden Informationen:

- Verbindungen Log-Ereignisse zu Verbindungen zwischen dem Logger Service und den Quelldatenbanken.
- Logger Service. Log-Ereignisse zum Logger Service, einschließlich der Konfiguration, Aktivierung und Deaktivierung des Dienstes.
- Operationen des Logger Service. Log-Ereignisse für Operationen z. B. das Auffangen geänderter Daten und das Schreiben der Daten in die PowerExchange-Logger-Dateien.

Protokollereignisse des Modellrepository-Dienst

Protokollereignisse im Modellrepository-Dienst enthalten die folgenden Informationen:

- Modellrepository-Verbindungen. Protokollereignisse für Verbindungen zum Repository aus Informatica Developer, Informatica Analyst und dem Data Integration Service.
- Modellrepository-Dienst Protokollereignisse zum Modellrepository-Dienst, einschließlich der Aktivierung, Deaktivierung, des Starten und des Anhaltens des Dienstes.
- Repository-Operationen. Protokollereignisse zu Repository-Operationen, z. B. dem Erstellen und Löschen von Repository-Inhalten und das Hinzufügen bereit gestellter Anwendungen.
- Benutzerberechtigungen Protokollereignisse über das Verwalten von Benutzerberechtigungen im Repository.

Benutzerdefinierte Rollen für den Metadata Manager Service

Die Log-Ereignisse des PowerCenter Integration Service enthalten Informationen zu jedem PowerCenter Integration Service, der in der Domäne ausgeführt wird.

Log-Ereignisse des Metadata Manager Service enthalten die folgenden Informationen:

- Repository-Operationen. Log-Ereignisse für den Zugriff auf Metadaten im Metadata Manager-Repository.
- Konfiguration Log-Ereignisse über die Konfiguration des Metadata Manager Service.
- Laufzeitprozesse. Log-Ereignisse für die Ausführung eines Metadata Manager Service, wie z. B. fehlende native Bibliotheksdateien.
- Log-Ereignisse des PowerCenter Integration Service. Sitzungs- und Arbeitsablaufstatus für Sitzungen und Arbeitsabläufe, die eine PowerCenter Integration Service-Prozess verwenden, um Daten in das Metadata Manager Warehouse zu laden oder Quell-Metadaten zu extrahieren.

Um Log-Ereignisse anzuzeigen, wie der PowerCenter Integration Service einen PowerCenter-Arbeitsablauf verarbeitet, um Daten in das Metadata Manager-Warehouse zu laden, müssen Sie das Sitzungs- oder Arbeitsablauf-Log einsehen.

Log-Ereignisse des PowerCenter Integration Service

Die Log-Ereignisse des PowerCenter Integration Service enthalten Informationen zu jedem PowerCenter Integration Service, der in der Domäne ausgeführt wird.

Die Log-Ereignisse im PowerCenter Integration Service enthalten die folgenden Informationen:

- PowerCenter Integration Service-Prozesse. Log-Ereignisse zu den PowerCenter Integration Service-Prozessen, einschließlich Dienst-Ports, Codepage, Betriebsmodus, Dienstnamen sowie zum zugeordneten Repository und dem Status des PowerCenter Repository Service.
- Lizenzierung Log-Ereignisse für Lizenzverifikationen für das PowerCenter Integration Service durch den Service Manager.

Log-Ereignisse des PowerCenter Repository Service

Die Log-Ereignisse des PowerCenter Repository Service enthalten Informationen zu den einzelnen PowerCenter Repository Services, die in der Domäne laufen.

Log-Ereignisse des PowerCenter Repository Service enthalten die folgenden Informationen:

- PowerCenter Repository-Verbindungen. Protokollieren von Ereignissen für Verbindungen zum Repository von PowerCenter-Client-Anwendungen, einschließlich Benutzernamen und Hostnamen und Portnummer der Client-Anwendung.
- PowerCenter Repository-Objekte: Protokollieren von Ereignissen für Repository-Objekte, die durch den PowerCenter Repository Service gesperrt, geholt, eingefügt oder aktualisiert wurden.
- PowerCenter Repository Service-Prozesse. Protokollieren von Ereignissen zu PowerCenter Repository Service-Prozessen, einschließlich Starten und Stoppen des PowerCenter Repository Service und Informationen über die Repository-Datenbanken, die von den PowerCenter Repository Service-Prozessen genutzt werden. Hierzu gehören auch der Repository-Betriebsmodus, die Knoten, auf denen der PowerCenter Repository Service-Prozess läuft, Initialisierungsinformationen und genutzte interne Funktionen verwendet.
- Repository-Operationen. Protokollieren von Ereignissen für Repository-Operationen, einschließlich Erstellen, Löschen, Wiederherstellen und Aktualisieren von Repository-Contents, Kopieren von Repository-Contents und die Registrierung sowie Deregistrierung lokaler Repositories.
- Lizenzierung Protokollieren von Ereignissen zur PowerCenter Repository Service-Lizenzprüfung.
- Sicherheits-Audit-Trails. Protokollieren von Ereignissen für zu Benutzern, Gruppen und Berechtigungen. Um die Sicherheits-Audit-Trails in die Log-Ereignisse des PowerCenter-Repository Service aufzunehmen, müssen Sie die allgemeine Eigenschaft SecurityAuditTrail für den PowerCenter-Repository Service im Administrator Tool aktivieren.

Log-Ereignisse des Reporting Service

Die Log-Ereignisse des Berichtsdienstes enthalten Informationen zu jedem Berichtsdienst, der in der Domäne ausgeführt wird.

Log-Ereignisse des Reporting Service enthalten die folgenden Informationen:

- Reporting Service-Prozesse. Log-Ereignisse über das Starten und Anhalten des Berichtsdienstes.
- Repository-Operationen. Log-Ereignisse für die Operationen des Data Analyzer Repositories. Dazu zählen Informationen zum Erstellen, Löschen, Sichern, Wiederherstellen und Aktualisieren des Repository-Inhalts sowie die Aktualisierung von Benutzern und Gruppen.
- Lizenzierung Log-Ereignisse zur Lizenzverifizierung des Berichtsdienstes.
- Konfiguration Log-Ereignisse über das Konfigurieren des Berichtsdienstes.

Log-Ereignisse des SAP BW Service

Die Log-Ereignisse des SAP BW Service enthalten Informationen über die Interaktion zwischen dem PowerCenter und dem SAP NetWeaver BI-System.

Die Log-Ereignisse des SAP NetWeaver BI enthalten die folgenden Log-Ereignisse für einen SAP BW Service:

- Log-Ereignisse des SAP NetWeaver BI-Systems. Fordert das SAP NetWeaver BI-System auf, einen Arbeitsablauf zu starten und Statusinformationen vom ZPMSENDSTATUS ABAP-Programm in der Prozesskette anzugeben.
- Log-Ereignisse des PowerCenter Integration Service. Sitzungs- und Arbeitsablaufstatus für Sitzungen und Arbeitsabläufe, die einen PowerCenter Integration Service-Prozess verwenden, um Daten zu laden oder Daten aus SAP NetWeaver BI zu extrahieren.

Um Log-Ereignisse zu der Verfahrensweise anzuzeigen, mit der der PowerCenter Integration Service einen SAP NetWeaver BI-Arbeitsablauf verarbeitet, müssen Sie den Sitzungs- oder Arbeitsablauf-Log anzeigen.

Log-Ereignisse des Web Services Hub

Die Log-Ereignisse des Web Services Hub enthalten Informationen über die Interaktion zwischen Anwendungen und dem Web Services Hub.

Die Log-Ereignisse des Web Services Hub enthalten folgende Log-Ereignisse:

- Web Services-Prozesse Log-Ereignisse über Web-Dienstprozesse, einschließlich Starten und Stoppen des Web Services Hub, Web-Dienst-Anfragen, den Status der Anfragen und Fehlermeldungen zu Web-Dienstauffufen. Die Log-Ereignisse enthalten Informationen darüber, welche Dienstarbeitsabläufe vom Repository abgerufen werden.
- Log-Ereignisse des PowerCenter Integration Service. Arbeitsablauf- und Sitzungsstatus für Dienstarbeitsabläufe, einschließlich ungültiger Arbeitsablauffehler.

Protokollereignisse der Benutzeraktivität

Benutzeraktivitäts-Protokollereignisse beschreiben alle Domänen- und Sicherheitsmanagementaufgaben, die ein Benutzer ausführt. Verwenden Sie die Protokollereignisse der Benutzeraktivität, um festzustellen, wann ein Benutzer Dienste, Knoten, Benutzer, Gruppen oder Rollen erstellt, aktualisiert oder gelöscht hat. Verwenden Sie die Protokollereignisse der Benutzeraktivität, um festzustellen, wann ein Benutzer Dienste, Benutzer, Gruppen oder Rollen erstellt oder aktualisiert hat.

Der Service Manager schreibt Benutzeraktivitäts-Protokollereignisse, wenn der Service Manager einen Benutzer genehmigen muss, damit er eine der folgenden Domänenaktionen durchführen kann:

- Aktivieren oder Deaktivieren eines Dienstprozesses.
- Starten, Beenden, Aktivieren oder Deaktivieren eines Dienstes.
- Fügt einen Knoten hinzu, aktualisiert oder fährt ihn herunter.
- Ändert die Domäneneigenschaften.
- Verschiebt einen Ordner in die Domäne.

Der Dienstmanager schreibt auch jedes Mal Benutzeraktivitäts-Protokollereignisse, wenn ein Benutzer eine der folgenden Sicherheitsaktionen ausführt:

- Fügt Benutzer, Gruppen, Betriebssystemprofile oder Rollen hinzu, aktualisiert oder entfernt sie. Das Benutzeraktivitäts-Protokoll zeigt Informationen über den Benutzer, der die Sicherheitsaktion durchgeführt hat, jedoch nicht den Zeitstempel der Aktion.

Der Service Manager schreibt auch jedes Mal ein Benutzeraktivitäts-Protokollereignis, wenn ein Benutzerkonto gesperrt oder entsperrt ist.

Protokoll-Aggregator

Sie können die Protokolldateien eines Anwendungsdiensts zusammenfassen, der nicht mehr reagiert oder unerwartet heruntergefahren wurde. Möglicherweise müssen Sie mehrere Protokolldateien analysieren, um die Probleme mit einem Anwendungsdienst zu ermitteln.

Mit dem Protokoll-Aggregator können Sie alle mit einem Anwendungsdienst verbundenen Protokolldateien zusammenfassen und die erforderlichen Protokolldateien in einer ZIP-Datei komprimieren. Sie können die ZIP-Datei herunterladen und die Protokolldateien analysieren oder die ZIP-Datei zum globalen Kundensupport von Informatica zwecks Analyse hochladen.

Sie können den Verlauf der aggregierten Protokolle nicht speichern. Sie müssen die Datei herunterladen oder an den globalen Kundensupport von Informatica senden, nachdem Sie die Protokolldateien aggregiert haben.

Sie können die Protokolle über die folgenden hängenden oder abgestürzten Anwendungsdienste aggregieren:

- Analyst-Dienst
- Datenintegrationsdienst
- Modellrepository-Dienst
- PowerCenter-Integrationsdienst
- PowerCenter-Repository-Dienst

Zusätzlich zu den Anwendungsdienstprotokollen erfasst der Protokoll-Aggregator Debug-Informationen für die Knoten in der Domäne. Der Protokoll-Aggregator aggregiert die Protokolldateien der zugehörigen Anwendungsdienste, wenn Sie die Protokolldateien eines Anwendungsdiensts aggregieren. Beispiel: Wenn Sie die Protokolldateien eines Analyst-Diensts aggregieren, aggregiert der Protokoll-Aggregator die Protokolldateien des mit dem Analyst-Dienst verbundenen Datenintegrationsdiensts und Modellrepository-Diensts.

Das Verzeichnis für Protokollsammlung in der Master-Gateway-Knoten speichert die Anwendungsdienstprotokolle, wenn Sie die Protokolle aggregieren. Alle Knotenprozesse in der Domäne müssen Lese- und Schreibzugriff auf das Verzeichnis für die Protokollsammlung haben. Wenn die Knotenprozesse nicht auf das Verzeichnis für die Protokollsammlung zugreifen können, werden die zusammengefassten Protokolle nicht im Listengitter der zusammengefassten Protokolle angezeigt. Das Hauptspeicherverzeichnis speichert die Hauptspeicherdateien des Knotens in der Domäne. Konfigurieren Sie das Verzeichnis für Protokollsammlung im Master-Gateway-Knoten und das Hauptspeicherverzeichnis für jeden Knoten in der Domäne.

Beim Verarbeiten der aggregierten Protokolle können Sie die Sammlungen auswählen, aus denen Sie Protokollinformationen sammeln möchten. Die Sammlungen sind mit dem Anwendungsdienst verbundene Anwendungsdienste und Knoten.

Aggregieren von Anwendungsdienstprotokollen

Sie können die Protokolldateien aggregieren, die mit einem Anwendungsdienst verbunden sind, der hängt oder abstürzt.

1. Klicken Sie im Administrator-Tool auf die Registerkarte **Protokolle**.
2. Klicken Sie auf die Registerkarte **Protokoll-Aggregator**.

3. Wählen Sie den Anwendungsdienst aus, für den Sie Protokolle aggregieren möchten.
4. Wählen Sie das Szenario aus, für das Sie Protokolle aggregieren möchten.
Sie können zwischen dem Absturz und dem Hängen eines Anwendungsdiensts auswählen.
5. Wählen Sie das Zeitintervall zum Aggregieren der Protokolle aus.
Sie können Protokolle der letzten 6 Stunden bis hin zu den letzten 3 Tagen aggregieren.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie die Sammlungen aus, aus denen Sie die Protokolle aggregieren möchten.
Der Protokoll-Aggregator zeigt die Protokolldateien und die Sammlungen basierend auf dem Knoten an, zu dem sie gehören.
8. Klicken Sie auf **Fertig stellen**.
Die Liste der verbundenen Protokolle mit dem Szenario wird im rechten Bereich angezeigt. Sie können die aggregierten Protokolle herunterladen oder die Protokolle an den globalen Kundensupport von Informatica senden.

Verarbeiten von aggregierten Anwendungsdienstprotokollen

Nach dem Aggregieren von Anwendungsdienstprotokollen müssen Sie die aggregierte ZIP-Datei herunterladen oder die Protokolle an den globalen Kundensupport von Informatica senden.

Aggregieren Sie die Anwendungsdienstprotokolle basierend auf Ihren Anforderungen.

1. Wählen Sie die Protokolle aus, die Sie verarbeiten möchten.
2. Klicken Sie auf **Aktionen > Protokolle komprimieren**.
Das Dialogfeld **Komprimierten Szenario-Ausgabe** wird angezeigt.
3. Klicken Sie auf der Registerkarte **Komprimierte Ausgabe** auf **Herunterladen**, um die aggregierten Protokolldateien als ZIP-Datei herunterzuladen.
4. Klicken Sie optional auf die Registerkarte **An Support senden**.
5. Geben Sie den Benutzernamen, das Passwort und das TFTP-Verzeichnis des Informatica MySupport-Portals ein.
6. Klicken Sie auf **Senden**, um die aggregierten Protokolldateien an den globalen Kundensupport von Informatica zu senden.

KAPITEL 11

Überwachung

Dieses Kapitel umfasst die folgenden Themen:

- [Überwachen - Übersicht, 201](#)
- [Konfigurieren der Überwachung, 208](#)
- [Data Integration Services überwachen , 210](#)
- [Überwachen von Jobs, 211](#)
- [Überwachen von Anwendungen, 212](#)
- [Bereitgestellte Mapping-Jobs überwachen, 213](#)
- [Logische Datenobjekte überwachen, 215](#)
- [SQL-Datendienste überwachen, 216](#)
- [Web-Dienste überwachen, 219](#)
- [Überwachen von Arbeitsabläufen, 220](#)
- [Überwachen eines Ordners von Objekten, 230](#)
- [Überwachen eines Objekts, 232](#)

Überwachen - Übersicht

Beim Überwachen handelt es sich um eine Domänenfunktion, die der Dienstmanager ausführt. Der Dienstmanager speichert die Überwachungskonfiguration im Modellrepository.

Der Dienstmanager unternimmt auch das Halten, Aktualisieren, Abrufen und Veröffentlichen von Laufzeit-Statistiken für Integrationsobjekte im Modellrepository. Integrationsobjekte umfassen Jobs, Anwendungen, logische Datenobjekte, SQL-Datendienste, Webdienste und Arbeitsabläufe. Verwenden Sie die Registerkarte **Überwachen** im Administrator-Tool, um Integrationsobjekte zu überwachen, die auf einem Datenintegrationsdienst ausgeführt werden. Die Registerkarte **Überwachen** zeigt Eigenschaften, Laufzeit-Statistiken und Laufzeit-Berichte über die Integrationsobjekte an. Zum Beispiel kann die Registerkarte **Überwachen** die allgemeinen Eigenschaften und den Status eines Profiling-Jobs anzeigen. Sie kann auch den Benutzer anzeigen, der den Auftrag initiiert hat und wie lange es dauerte, den Job zu beenden. Wenn Sie den Job auf einem Gitter ausgeführt haben, werden auf der Registerkarte "Überwachen" die Knoten angezeigt, die den Job ausgeführt haben. Sie können auch eine grafische Darstellung des Arbeitsablaufs im Monitoring-Tool anzeigen.

Sie können auch unter den folgenden Adressen auf die Überwachung zugreifen:

Informatica Monitoring Tool

Sie können auf die Überwachung vom Informatica Monitoring Tool aus zugreifen. Das Monitoring Tool ist eine direkte Anbindung an die Registerkarte **Überwachen** im Administrator-Tool. Das Monitoring Tool ist nützlich, wenn Sie keinen Zugriff auf andere Funktionen im Administrator-Tool benötigen. Sie müssen über mindestens eine Überwachungsberechtigung verfügen, um auf das Monitoring Tool zugreifen zu können. Sie können mithilfe der folgenden URL auf das Monitoring-Tool zugreifen:

```
http://<Administrator tool host> <Administrator tool port>/monitoring
```

Analyst-Tool

Sie können auf die Überwachung vom Informatica Analyst-Tool aus zugreifen. Wenn Sie auf die Überwachung vom Analyst-Tool aus zugreifen, werden die Ergebnisse der Überwachung in der Registerkarte **Job-Status** angezeigt. Die Registerkarte **Jobstatus** zeigt den Status der Analyst-Tool-Jobs, wie Profil-Jobs, Scorecard-Jobs und solcher Jobs, die Mapping-Spezifikationsergebnisse zum Ziel laden.

Developer-Tool

Sie können auf die Überwachung vom Developer-Tool aus zugreifen. Wenn Sie die Überwachung vom Developer-Tool aus zugreifen, erscheinen die Ergebnisse der Überwachung im Informatica Monitoring Tool. Das Informatica Monitoring Tool zeigt den Status der Developer-Tool-Jobs an, wie z. B. Mapping-Jobs, Webdienste und SQL-Datendienste.

Navigator der Registerkarte "Überwachen"

Wählen Sie ein Objekt im Navigator der Registerkarte **Überwachen** aus, um das Objekt zu überwachen.

Sie können die folgenden Objekttypen im Navigator der Registerkarte **Überwachen** auswählen:

Data Integration Service

Anzeigen aller allgemeinen Eigenschaften zum Data Integration Service und Anzeigen statistischer Daten zu Objekten, die im Data Integration Service ausgeführt werden.

Ordner

Anzeigen einer Liste der Objekte im Ordner. Der Ordner ist eine logische Gruppierung von Objekten. Wenn Sie einen Ordner auswählen, wird eine Liste von Objekten im Inhaltsbereich angezeigt. Der Inhaltsbereich zeigt mehrere Ansichten, die verschiedene Informationen zu einem Objekt anzeigen. Sie können die im Inhaltsbereich angezeigten Spalten konfigurieren.

Die folgende Tabelle zeigt die Ordner, die im Navigator angezeigt werden:

Ordner	Speicherort
Jobs	Wird unter dem Data Integration Service angezeigt.
Bereitgestellte Mapping-Jobs	Wird unter der entsprechenden Anwendung angezeigt.
Logische Datenobjekte	Wird unter der entsprechenden Anwendung angezeigt.
SQL-Datendienste	Wird unter der entsprechenden Anwendung angezeigt.

Ordner	Speicherort
Web-Dienste	Wird unter der entsprechenden Anwendung angezeigt.
Arbeitsabläufe	Wird unter der entsprechenden Anwendung angezeigt.

Ordner	Speicherort
Jobs	Wird unter dem Data Integration Service angezeigt.
Bereitgestellte Mapping-Jobs	Wird unter der entsprechenden Anwendung angezeigt.
Logische Datenobjekte	Wird unter der entsprechenden Anwendung angezeigt.
Arbeitsabläufe	Wird unter der entsprechenden Anwendung angezeigt.

Integrationsobjekte

Anzeigen von Informationen zum ausgewählten Integrationsobjekt. Integrationsobjekte umfassen Instanzen von Anwendungen, bereitgestellte Mapping-Jobs, logische Datenobjekte, SQL-Datendienste, Webdienste und Arbeitsabläufe.

Ansichten der Registerkarte "Überwachen"

Wenn Sie im Navigator oder in einem Objektlink im Inhaltsbereich der Registerkarte **Überwachen** ein Integrationsobjekt auswählen, erscheinen viele Ansichten mit verschiedenen Informationen im Inhaltsbereich. Diese Ansichten enthalten Informationen zu dem ausgewählten Objekt, z. B. Eigenschaften, Laufzeit-Statistiken und Laufzeitberichte.

Je nach Objekttyp, den Sie im Navigator wählen, zeigt der Inhaltsbereich die folgenden Ansichten an:

Eigenschaftenansicht

Führt die allgemeinen Eigenschaften und Laufzeit-Statistiken zum ausgewählten Objekt auf. Allgemeine Eigenschaften können den Namen und die Beschreibung des Objekts enthalten. Die Statistiken variieren basierend auf dem ausgewählten Objekttyp.

Ansicht Berichte

Zeigt Berichte zum ausgewählten Objekt an. Berichte enthalten die Schlüsselmetriken für das Objekt. Zum Beispiel: Sie können Berichte anzeigen, um die am längsten ausgeführten Jobs in einem Data Integration Service innerhalb einer bestimmten Zeitspanne ausfindig zu machen.

Verbindungsansicht

Zeigt Verbindungen an, die für das ausgewählte Objekt definiert wurden. Sie können Statistiken zu jeder Verbindung anzeigen, z. B. die Anzahl der geschlossenen, abgebrochenen und gesamten Verbindungen.

Ansicht Anfragen

Zeigt die Details zu Anfragen an. Es gibt zwei Typen von Anfragen: SQL-Anfragen und Web-Dienst-Anfragen. Die Benutzer können ein Client-Tool von einem Drittanbieter verwenden, um SQL-Abfragen gegen die virtuellen Tabellen in einem SQL-Datendienst auszuführen. Die Benutzer können einen Web-Dienst-Client zum Ausführen von Web-Dienst-Anfragen gegen einen Web-Dienst verwenden. Jede Web-Dienst-Anfrage führt eine Web-Dienst-Operation aus.

Eine Anfrage ist entweder eine Web-Dienst-Anfrage oder eine SQL-Abfrage, die der Benutzer gegen eine virtuelle Tabelle im SQL-Datendienst ausführt.

Virtuelle Tabellenansicht

Zeigt die virtuellen Tabellen an, die in einem SQL-Datendienst definiert sind. Auch die Eigenschaften und Cache-Aktualisierungsdetails lassen sich für jede virtuelle Tabelle anzeigen.

Operationsansicht

Zeigt die Operationen, die für den Web-Dienst definiert wurden.

Statistik auf der Registerkarte "Überwachen"

Der Abschnitt **Statistik** in der Ansicht **Eigenschaften** zeigt eine aggregierte Statistik zum ausgewählten Objekt an. Beispiel: Wenn Sie einen Datenintegrationsdienst im Navigator der Registerkarte **Überwachen** auswählen, wird im Abschnitt **Statistik** die Gesamtzahl der laufenden, fehlgeschlagene, abgebrochenen und abgeschlossenen Jobs angezeigt, die auf dem ausgewählten Datenintegrationsdienst laufen.

Sie können eine Statistik zu folgenden Integrationsobjekten anzeigen:

Anwendungen

Beinhaltet Bereitgestellte Mapping-Jobs, logische Datenobjekte, SQL-Datendienste und Web-Dienste.

Enthält bereitgestellte Mapping-Jobs und logische Datenobjekte.

Verbindungen

Beinhaltet SQL-Verbindungen zu virtuellen Datenbanken.

Jobs

Beinhaltet Jobs für Profile, Vorschauen, nicht bereitgestellte Mappings, Referenztabellen und Scorecards.

Beinhaltet Jobs für Profile, Vorschauen und nicht bereitgestellte Mappings.

Anfragen

Beinhaltet SQL-Anfragen und Web-Dienst-Anfragen.

Arbeitsabläufe

Beinhaltet Arbeitsablaufinstanzen.

Die folgende Tabelle zeigt die Statistik für jeden Objekttyp:

Objekttyp	Statistik
Anwendungsobjekte	<ul style="list-style-type: none">- Gesamt. Gesamtzahl der Anwendungen.- Wird ausgeführt. Anzahl der ausgeführten Anwendungen.- Fehlgeschlagen. Anzahl der fehlgeschlagenen Anwendungen.- Gestoppt. Anzahl der gestoppten Anwendungen.- Deaktiviert. Anzahl der deaktivierten Anwendungen.
Verbindungsobjekte	<ul style="list-style-type: none">- Gesamt. Gesamtanzahl der Verbindungen.- Geschlossen. Anzahl der geschlossenen Verbindungen. Geschlossene Verbindungen sind Datenbankverbindungen, auf denen vorher SQL-Datendienst-Anfragen ausgeführt wurden, die aber jetzt geschlossen sind. Sie können keine Anfragen auf geschlossenen Verbindungen ausführen.- Abgebrochen. Anzahl der abgebrochenen Verbindungen. Sie wählen das Abbrechen der Verbindung aus oder der Datenintegrationsdienst wurde im Abbruchmodus bei laufender Anwendung recycelt oder deaktiviert.

Objekttyp	Statistik
Jobs	<ul style="list-style-type: none"> - Gesamt. Gesamtzahl der Jobs. - Fehlgeschlagen. Anzahl der fehlgeschlagenen Jobs. - Abgebrochen. Anzahl der abgebrochenen Jobs. Der Datenintegrationsdienst wurde im Abbruchmodus bei laufendem Job recycelt oder deaktiviert. - Abgeschlossen. Anzahl der abgeschlossenen Jobs. - Storniert. Anzahl der stornierten Jobs.
Anfrageobjekte	<ul style="list-style-type: none"> - Gesamt. Gesamtzahl der Anfragen. - Abgeschlossen. Anzahl der abgeschlossenen Anfragen. - Abgebrochen. Anzahl der abgebrochenen Anfragen. Der Datenintegrationsdienst wurde im Abbruchmodus bei laufender Anfrage recycelt oder deaktiviert. - Fehlgeschlagen. Anzahl der fehlgeschlagenen Anfragen.
Arbeitsabläufe	<ul style="list-style-type: none"> - Gesamt. Gesamtzahl der Arbeitsablaufinstanzen. - Abgeschlossen. Anzahl der abgeschlossenen Arbeitsablaufinstanzen. - Storniert. Anzahl der stornierten Arbeitsablaufinstanzen. - Abgebrochen. Anzahl der abgebrochenen Arbeitsablaufinstanzen. - Fehlgeschlagen. Anzahl der fehlgeschlagenen Arbeitsablaufinstanzen.

Objekttyp	Statistik
Anwendungsobjekte	<ul style="list-style-type: none"> - Gesamt. Gesamtzahl der Anwendungen. - Wird ausgeführt. Anzahl der ausgeführten Anwendungen. - Fehlgeschlagen. Anzahl der fehlgeschlagenen Anwendungen. - Gestoppt. Anzahl der gestoppten Anwendungen. - Deaktiviert. Anzahl der deaktivierten Anwendungen.
Jobs	<ul style="list-style-type: none"> - Gesamt. Gesamtzahl der Jobs. - Fehlgeschlagen. Anzahl der fehlgeschlagenen Jobs. - Abgebrochen. Anzahl der abgebrochenen Jobs. Der Datenintegrationsdienst wurde im Abbruchmodus bei laufendem Job recycelt oder deaktiviert. - Abgeschlossen. Anzahl der abgeschlossenen Jobs. - Storniert. Anzahl der stornierten Jobs.
Anfrageobjekte	<ul style="list-style-type: none"> - Gesamt. Gesamtzahl der Anfragen. - Abgeschlossen. Anzahl der abgeschlossenen Anfragen. - Abgebrochen. Anzahl der abgebrochenen Anfragen. Der Datenintegrationsdienst wurde im Abbruchmodus bei laufender Anfrage recycelt oder deaktiviert. - Fehlgeschlagen. Anzahl der fehlgeschlagenen Anfragen.
Arbeitsabläufe	<ul style="list-style-type: none"> - Gesamt. Gesamtzahl der Arbeitsablaufinstanzen. - Abgeschlossen. Anzahl der abgeschlossenen Arbeitsablaufinstanzen. - Storniert. Anzahl der stornierten Arbeitsablaufinstanzen. - Abgebrochen. Anzahl der abgebrochenen Arbeitsablaufinstanzen. - Fehlgeschlagen. Anzahl der fehlgeschlagenen Arbeitsablaufinstanzen.

Berichte auf der Registerkarte "Überwachen"

Sie können Überwachungsberichte in der Ansicht **Berichte** der Registerkarte **Überwachen** anzeigen. Die Ansicht **Berichte** wird angezeigt, wenn Sie das entsprechende Objekt im Navigator auswählen. Sie können Berichte anzeigen, um Objekte zu überwachen, die für einen Data Integration Service bereitgestellt wurden, wie z. B. Jobs, Webdienste, Webdienstoperationen, SQL-Datendienste und Arbeitsabläufe.

Die Berichte in der **Berichtsansicht** basieren auf dem ausgewählten Objekttyp und darauf, welche Berichte für die Anzeige in der Ansicht konfiguriert wurden. Sie müssen die Überwachungseinstellungen konfigurieren,

damit Berichte in der Ansicht **Berichte** aufgeführt werden. Gemäß Voreinstellung werden in der Ansicht **Berichte** keine Berichte aufgeführt.

Sie können die folgenden Überwachungsberichte anzeigen:

Jobs mit längster Dauer

Zeigt die Jobs an, die während des angegebenen Zeitraums am längsten liefen. Der Bericht zeigt Namen, ID, Typ, Status und Dauer des Jobs an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Data Integration Service überwachen.

Mapping-Jobs mit längster Dauer

Zeigt Mapping-Jobs an, die während des angegebenen Zeitraums am längsten liefen. Der Bericht zeigt Namen, ID, Status und Dauer des Jobs an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Data Integration Service überwachen.

Profil-Jobs mit längster Dauer

Zeigt Profil-Jobs an, die während des angegebenen Zeitraums am längsten liefen. Der Bericht zeigt Namen, ID, Status und Dauer des Jobs an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Data Integration Service überwachen.

Referenztabellen-Jobs mit längster Dauer

Zeigt Referenztabellen-Jobs an, die während des angegebenen Zeitraums am längsten liefen. Bei Referenztabellen-Jobs handelt es sich um Jobs, bei denen Sie Referenztabellendaten importieren oder exportieren. Der Bericht zeigt Namen, ID, Status und Dauer des Jobs an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Data Integration Service überwachen.

Scorecard-Jobs mit längster Dauer

Zeigt Scorecard-Jobs an, die während des angegebenen Zeitraums am längsten liefen. Der Bericht zeigt Namen, ID, Status und Dauer des Jobs an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Data Integration Service überwachen.

SQL-Datendienstverbindungen mit längster Dauer

Zeigt SQL-Datendienstverbindungen an, die während des angegebenen Zeitraums am längsten liefen. Der Bericht zeigt Verbindungs-ID, SQL-Datendienst, Verbindungsstatus und Dauer an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Data Integration Service, einen SQL-Datendienst oder eine Anwendung überwachen.

SQL-Datendienstanfragen mit längster Dauer

Zeigt SQL-Datendienstanfragen an, die während des angegebenen Zeitraums am längsten liefen. Der Bericht zeigt Nummer der Anfrage, SQL-Datendienst, Anfragestatus und Dauer an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Data Integration Service, einen SQL-Datendienst oder eine Anwendung überwachen.

Web-Dienst-Anfragen mit längster Dauer

Zeigt Web-Dienst-Anfragen an, die während des angegebenen Zeitraums am längsten liefen. Der Bericht zeigt Nummer der Anfrage, Web-Dienst-Operation, Anfragestatus und Dauer an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Data Integration Service, einen Web-Dienst oder eine Anwendung überwachen.

Arbeitsabläufe mit längster Dauer

Zeigt alle Arbeitsabläufe an, die im angegebenen Zeitraum am längsten ausgeführt werden. Der Bericht zeigt den Namen, den Status, die Instanz-ID und die Dauer des Arbeitsablaufs an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Data Integration Service oder eine Anwendung überwachen.

Arbeitsabläufe mit längster Dauer, ausgenommen Human-Tasks

Zeigt Arbeitsabläufe an, die keine Human-Task enthalten, die im angegebenen Zeitraum am längsten ausgeführt werden. Der Bericht zeigt den Namen, den Status, die Instanz-ID und die Dauer des Arbeitsablaufs an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Data Integration Service oder eine Anwendung überwachen.

Bericht für minimale, maximale und durchschnittliche Dauer

Zeigt die Gesamtzahl der SQL-Datendienst- und Web-Dienst-Anfragen während des angegebenen Zeitraums an. Außerdem werden die minimale, maximale und durchschnittliche Dauer für die Anfragen während des angegebenen Zeitraums angezeigt. Der Bericht zeigt Objekttyp, Gesamtzahl an Anfragen, Mindestdauer, Maximaldauer und durchschnittliche Dauer an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Data Integration Service, einen SQL-Datendienst, einen Web-Dienst oder eine Anwendung überwachen.

Aktivste IP für SQL-Datendienstanfragen

Zeigt die Gesamtzahl der SQL-Datendienst- und Web-Dienst-Anfragen von jeder IP-Adresse während des angegebenen Zeitraums an. Der Bericht zeigt die IP-Adresse und die Gesamtanzahl der Anfragen an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Data Integration Service, einen SQL-Datendienst oder eine Anwendung überwachen.

Aktivste SQL-Datendienstverbindungen

Zeigt SQL-Datendienstverbindungen an, die während des angegebenen Zeitraums die meisten Verbindungsanfragen erhalten haben. Der Bericht zeigt Verbindungs-ID, SQL-Datendienst und Gesamtanzahl der Verbindungsanfragen an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Data Integration Service, eine Anwendung oder einen SQL-Datendienst überwachen.

Aktivste Benutzer für Jobs

Zeigt die Benutzer an, die während des angegebenen Zeitraums die meisten Jobs ausgeführt haben. Der Bericht zeigt den Benutzernamen und die Gesamtzahl der vom Benutzer ausgeführten Jobs an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Data Integration Service überwachen.

Aktivste Web-Dienst-Client-IP

Zeigt die IP-Adressen an, die während des angegebenen Zeitraums die meisten Web-Dienst-Anfragen erhalten haben. Der Bericht zeigt die IP-Adresse und die Gesamtzahl der Anfragen an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Data Integration Service, eine Anwendung, einen Web-Dienst oder eine Web-Dienst-Operation überwachen.

Häufigste Fehler für Jobs

Zeigt die häufigsten Fehler für Jobs während des angegebenen Zeitraums unabhängig vom jeweiligen Jobtyp an. Der Bericht zeigt Jobtyp, Fehlernummer, Status und Anzahl der Fehler an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Data Integration Service überwachen.

Häufigste Fehler für SQL-Datendienstanfragen

Zeigt die häufigsten Fehler bei SQL-Datendienstanfragen während des angegebenen Zeitraums an. Der Bericht zeigt die Fehlernummer und die Anzahl der Fehler an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Data Integration Service, einen SQL-Datendienst oder eine Anwendung überwachen.

Häufigste Fehler für Web-Dienst-Anfragen

Zeigt die häufigsten Fehler bei Web-Dienst-Anfragen während des angegebenen Zeitraums an. Der Bericht zeigt die Fehlernummer und die Anzahl der Fehler an. Sie können diesen Bericht in der Ansicht

Berichte anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Data Integration Service, einen Web-Dienst oder eine Anwendung überwachen.

Konfigurieren der Überwachung

Sie können die Domäne so konfigurieren, dass Statistiken und Berichte zu Objekten in der Domäne angezeigt werden. Statistiken und Berichte werden auf der Registerkarte **Verwalten** in der Ansicht **Historie** und auf der Registerkarte **Überwachen** in den Ansichten **Übersichtsstatistik** und **Ausführungsstatistiken** angezeigt. Zur Anzeige von Statistiken und Berichten müssen Sie die Überwachung für die Domäne konfigurieren.

Wenn Sie die Überwachung in der Domäne konfigurieren, werden die Statistiken und Berichte von den Datenintegrationsdiensten in einem Modellrepository gespeichert. Zu den Statistiken zählen historische Informationen zu Objekten, die von den Datenintegrationsdiensten ausgeführt werden. In den Berichten werden Schlüsselmetriken zu Integrationsobjekten angezeigt.

Wenn Sie die Überwachung in der Domäne konfigurieren, werden die Statistiken und Berichte vom Datenintegrationsdienst in einem Modellrepository gespeichert. Zu den Statistiken zählen historische Informationen zu Objekten, die vom Datenintegrationsdienst ausgeführt werden. In den Berichten werden Schlüsselmetriken zu Integrationsobjekten angezeigt.

Falls Sie die Überwachung nicht konfigurieren, weisen einige Ansichten auf den Registerkarten **Verwalten** und **Überwachen** keinen Inhalt auf. Auch das Arbeitsablaufdiagramm ist leer und Benachrichtigungen werden nicht mehr angezeigt, wenn Sie die Seite aktualisieren.

Zum Einrichten von Überwachungsstatistiken und -berichten führen Sie die folgenden Aufgaben durch:

1. Konfigurieren der Überwachungseinstellungen. Konfigurieren Sie ein Modellrepository, in dem Laufzeitstatistiken für Objekte gespeichert werden, die von den Datenintegrationsdiensten ausgeführt werden.
2. Konfigurieren der Überwachungseinstellungen. Konfigurieren Sie ein Modellrepository, in dem Laufzeitstatistiken für Objekte gespeichert werden, die vom Datenintegrationsdienst ausgeführt werden.
3. Konfigurieren der Ansichten „Berichte“ und „Statistiken“. Wählen Sie aus, welche Statistiken in den Ansichten **Statistiken** und **Berichte** angezeigt werden.

Hinweis: In einer Domäne mit Kerberos-Authentifizierung müssen die Benutzer über die Administratorrolle für den Modellrepository-Dienst verfügen, von dem die Statistiken gespeichert werden. Falls Benutzer nicht über die Administratorrolle verfügen, werden einige Statistiken nicht angezeigt.

Schritt 1. Konfigurieren der globalen Einstellungen

Globale Einstellungen müssen Sie für die Domäne konfigurieren, um das Modellrepository anzugeben, in dem die Laufzeitstatistiken über die den Datenintegrationsdiensten zur Verfügung gestellten Objekte gespeichert sind. Die globalen Einstellungen gelten für alle in der Domäne definierten Datenintegrationsdienste. Wenn Sie die globalen Einstellungen nicht konfigurieren, ist das Arbeitsablaufdiagramm leer und die Benachrichtigungen werden beim Aktualisieren der Seite nicht mehr angezeigt.

1. Klicken Sie im Administrator-Tool auf die Registerkarte **Überwachen**.
2. Wählen Sie die Domäne im Navigator aus.
3. Klicken Sie im Inhaltsbereich auf **Aktionen > Globale Einstellungen**.

4. Bearbeiten Sie folgende Optionen:

Option	Beschreibung
Modellrepository-Dienst	Name des Modellrepository-Diensts, der die Verlaufsdaten speichert.
Benutzername	Benutzername für den Modellrepository-Dienst.
Passwort	Passwort für den Modellrepository-Diensts.
Anzahl der Tage für die Aufbewahrung von Verlaufsdaten	Anzahl der Tage, für die der Datenintegrationsdienst historische Laufzeitstatistiken speichert. Geben Sie '0' an, wenn Sie keine Aufbewahrung von Laufzeit-Verlaufsstatistiken durch den Datenintegrationsdienst wünschen.
Statistiken bereinigen alle	Häufigkeit in Tagen, mit der der Datenintegrationsdienst die Statistiken bereinigt. Der Standardwert ist 1.
Tage bei	Tageszeit, zu der der Datenintegrationsdienst alte Statistiken bereinigt. Der Standardwert ist 1:00 morgens.
Maximale Anzahl der sortierbaren Datensätze	Die maximale Anzahl der Datensätze, die auf der Registerkarte Überwachen sortiert werden können. Übersteigt die Anzahl der Datensätze auf der Registerkarte Überwachen diesen Wert, können Sie nur die Spalten Startzeit und Endezeit sortieren. Der Standardwert ist 3.000.
Maximale Verzögerung für Aktualisierungsbenachrichtigungen	Maximaler Zeitraum in Sekunden, für den der Datenintegrationsdienst die Statistiken zwischenspeichert, bevor er sie dauerhaft im Modellrepository ablegt und auf der Registerkarte Überwachen anzeigt. Wenn der Datenintegrationsdienst unerwartet heruntergefahren wird, bevor der Dienst die Statistiken im Modellrepository gespeichert hat, gehen die Statistiken verloren. Standardwert ist 10.
Millisekunden einblenden	Auf der Registerkarte Überwachen werden bei Datums- und Zeitfeldern die Millisekunden mit angezeigt.

Hinweis: Wenn Sie Kerberos-Sicherheit in der Domäne aktivieren, werden die Felder „Benutzername“ und „Passwort“ nicht angezeigt.

5. Klicken Sie auf **OK**.

6. Klicken Sie auf **Speichern**, um die globalen Einstellungen zu speichern.

Starten Sie alle Datenintegrationsdienste in der Domäne neu, um die Einstellungen zu übernehmen.

Schritt 2. Konfigurieren der Ansichten „Berichte“ und „Statistiken“

Die Ansichten **Statistiken** und **Berichte** in der Ansicht **Ausführungsstatistiken** sind standardmäßig leer. Wenn Sie Statistiken und Berichte anzeigen möchten, müssen Sie die Berichts- und Statistikeinstellungen in der Domäne konfigurieren. Diese Einstellungen werden auf alle Datenintegrationsdienste in der Domäne angewendet.

Bevor Sie Statistiken und Berichte konfigurieren, müssen Sie in der Überwachungskonfiguration einen Modellrepository-Dienst angeben und diesen aktivieren.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Überwachen**.

2. Klicken Sie auf **Aktionen > Berichts- und Statistikeinstellungen**.
3. Konfigurieren Sie auf der Registerkarte **Statistiken** die Zeiträume, die Sie für Statistiken verwenden möchten, und wählen Sie dann aus, wie häufig die den verschiedenen Zeiträumen zugeordneten Statistiken aktualisiert werden sollen.
4. Wählen Sie einen Standard-Zeitbereich, der für alle Statistiken angezeigt werden soll.
5. Klicken Sie auf die Registerkarte **Berichte**
6. Aktivieren Sie die Zeitbereiche, die Sie für die Berichte benutzen möchten, und wählen Sie eine Frequenz zum Aktualisieren der den verschiedenen Zeitbereichen zugeordneten Berichte.
7. Wählen Sie einen Standard-Zeitbereich aus, der in allen Berichten erscheint, und klicken Sie auf **OK**.
8. Klicken Sie auf **Berichte auswählen**.
9. Fügen Sie die Berichte hinzu, die Sie im Feld **Ausgewählte Berichte** ausführen möchten.
10. Ordnen Sie die Berichte in der Reihenfolge, in der Sie sie auf der Registerkarte **Überwachung** anzeigen möchten.
11. Mit **OK** schließen Sie das Fenster **Berichte auswählen**.
12. Klicken Sie für die Einstellungen auf **OK** und schließen Sie das Fenster **Berichts- und Statistikeinstellungen**.

Data Integration Services überwachen

Sie können Datenintegrationsdienste auf der Registerkarte **Überwachen** in der Ansicht **Ausführungsstatistiken** überwachen.

Wenn Sie im Navigator einen Datenintegrationsdienst auswählen, werden im Inhaltsbereich die folgenden Informationen angezeigt:

- **Eigenschaftenansicht**
- Ansicht **Berichte**

Eigenschaftenansicht für einen Data Integration Service

Die Ansicht **Eigenschaften** zeigt die allgemeinen Eigenschaften und die Laufzeitstatistik für Objekte, die vom ausgewählten Datenintegrationsdienst ausgeführt wurden.

Wenn Sie einen Data Integration Service im Navigator auswählen, können Sie die allgemeinen Eigenschaften und die Laufzeit-Statistik einsehen.

Allgemeine Eigenschaften für einen Data Integration Service

Sie können die allgemeine Eigenschaften einsehen, wie z. B. Name des Dienstes, Objekttyp und eine Beschreibung. Die Eigenschaft "Beibehalten der Statistik aktiviert" gibt an, ob der Data Integration Service persistente Statistik im Model Repository speichert. Diese Option ist aktiviert, wenn Sie die globalen Einstellungen für die Domäne konfigurieren.

Außerdem können Sie Informationen zu Objekten anzeigen, die vom Datenintegrationsdienst ausgeführt werden. Um Informationen zu einem Objekt anzuzeigen, wählen Sie das Objekt im Navigator oder Inhaltsbereich aus. Je nach Objekttyp erscheinen Details zum Objekt im Inhalts- oder Detailbereich.

Statistik für einen Data Integration Service

Sie können die Laufzeitstatistik zu Objekten anzeigen, die vom Datenintegrationsdienst ausgeführt werden. Wählen Sie den Objekttyp und den Zeitraum aus, für den die Statistik angezeigt werden soll. Sie können die Statistik über Jobs, Anwendungen Verbindungen, Anfragen und Arbeitsabläufe anzeigen. Beispielsweise können Sie die Anzahl der fehlgeschlagenen, abgebrochenen und abgeschlossenen Profiling-Jobs in den letzten vier Stunden anzeigen.

Berichtsansicht für einen Data Integration Service

Die Ansicht **Berichte** zeigt die Überwachungsberichte zu Objekten an, die auf dem ausgewählten Data Integration Service ausgeführt werden.

Wenn Sie einen Data Integration Service auf der Registerkarte **Überwachen** überwachen, werden in der Ansicht **Berichte** Berichte über Jobs, SQL-Datendienste, Webdienste und Arbeitsabläufe angezeigt. Zum Beispiel: Sie können den Bericht "Aktivste Benutzer von Jobs" anzeigen lassen, um jene Benutzer zu ermitteln, die die meisten Jobs innerhalb eines bestimmten Zeitraums ausführen. Klicken Sie auf einen Link in einem Bericht, um weitere Details zu den Objekten, die in dem Link enthalten sind, anzuzeigen. Zum Beispiel: Wenn Sie auf die Anzahl fehlgeschlagener, bereitgestellter Mappings klicken, sehen Sie Details zu jedem bereitgestellten Mapping, das fehlgeschlagen ist.

Überwachen von Jobs

Sie können bereitgestellte Data Integration Service-Jobs auf der Registerkarte **Überwachen** überwachen. Ein Job ist ein Vorschau-, Scorecard-, Profil-, Mapping- oder Referenztabellenprozess, der auf einem Data Integration Service ausgeführt wird. Bei Referenztabellen-Jobs handelt es sich um Jobs, bei denen Sie Referenztabellendaten importieren oder exportieren. Ein Job ist ein Vorschau-, Profil- oder Mapping-Prozess, der auf einem Data Integration Service ausgeführt wird.

Wenn Sie **Jobs** im Navigator der Registerkarte **Überwachen** wählen, erscheint im Inhaltsbereich eine Liste der Jobs. Der Inhaltsbereich gruppiert zugehörige Jobs basierend auf dem Jobtyp. Sie können einen Jobtyp erweitern, um die zugehörigen Jobs darunter anzuzeigen.

Wenn Sie zum Beispiel einen Profiljob auf einem Knoten ausführen, teilt der Data Integration Service die Arbeit in mehrere Mappings auf. Die Mappings werden unter dem Profiljob in der Inhaltsmaske angezeigt. Die Inhaltsmaske zeigt außerdem den Knoten an, der jedes Mapping des Profils ausführt.

Standardmäßig können Sie Jobs anzeigen, die Sie erstellt haben. Wenn Sie die entsprechende Monitoring-Berechtigung haben, können Sie Jobs anderer Benutzer einsehen. Sie können die Eigenschaften zu jedem Job im Inhaltsbereich anzeigen. Sie können auch Protokolle oder den Kontext von Jobs anzeigen und Jobs abbrechen.

Sie führen Jobs aus dem Developer-Tool aus. Das Developer-Tool kann bis zu fünf Jobs gleichzeitig ausführen. Alle übrigen Jobs befinden sich in einer Warteschlange. Das Administrator-Tool zeigt dem Developer-Tool Jobs an, die derzeit ausgeführt werden. Es werden keine Jobs angezeigt, die sich in Warteschlangen im Developer-Tool befinden.

Wenn Sie im Inhaltsbereich einen Job auswählen, werden die Eigenschaften des ausgewählten Jobs im Detailbereich angezeigt. Abhängig von der Art des Jobs kann der Detailbereich die allgemeinen Eigenschaften und die Mapping-Eigenschaften anzeigen.

Allgemeine Eigenschaften für einen Job

Der Detailbereich zeigt die allgemeinen Eigenschaften zum ausgewählten Job an, wie z. B. den Namen, die Art des Jobs, den Benutzer, der den Job gestartet hat sowie die Startzeit des Jobs. Bei Ausführung des Jobs auf einem Gitter wird im Detailbereich auch der Knoten angezeigt, der den Job ausgeführt hat.

Mapping-Eigenschaften für einen Job

Der Abschnitt **Mapping** wird im Detailbereich angezeigt, wenn Sie einen Profil- oder Scorecard-Job im Inhaltsbereich auswählen. Diese Jobs haben ein dazugehöriges Mapping. Sie können die Mapping-Eigenschaften, wie z. B. die Nummer der Anfrage, den Mapping-Namen und den Namen der Protokolldatei anzeigen.

Anzeigen von Protokollen für einen Ad-hoc-Job

Sie können die Logs für einen Job herunterladen, um die Jobdetails zu sehen.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Überwachen**.
2. Klicken Sie auf die Ansicht für das **Ausführen von Statistiken**.
3. Erweitern Sie im Domänen-Navigator einen Datenintegrationsdienst und wählen Sie **Ad-hoc-Jobs** aus.
4. Im Inhaltsbereich wählen Sie einen Job aus.
5. Klicken Sie auf **Aktionen > Protokolle für gewähltes Objekt anzeigen**.

Es erscheint ein Dialog mit der Option zum Öffnen oder Speichern der Protokolldatei.

Abbrechen eines Ad-hoc-Jobs

Sie können einen aktuell ausgeführten Job abbrechen. Wenn ein Job zu umfangreich ist und zu viel Verarbeitungszeit benötigt, können Sie diesen wieder abbrechen.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Überwachen**.
2. Klicken Sie auf die Ansicht für das **Ausführen von Statistiken**.
3. Erweitern Sie im Domänen-Navigator einen Datenintegrationsdienst und wählen Sie **Ad-hoc-Jobs** aus.
4. Im Inhaltsbereich wählen Sie einen Job aus.
5. Klicken Sie auf **Aktionen > Ausgewählten Objekt abbrechen**.

Überwachen von Anwendungen

Sie können Anwendungen auf der Registerkarte **Überwachen** überwachen.

Wenn Sie im Navigator auf der Registerkarte **Überwachen** eine Anwendung auswählen, zeigt der Inhaltsbereich folgende Ansichten an:

- Ansicht **Eigenschaften**
- Ansicht **Berichte**

Sie können eine Anwendung im Navigator erweitern, um die Objekte in der Anwendung zu überwachen, wie zum Beispiel bereitgestellte Mapping-Jobs, logische Datenobjekte, SQL-Datendienste, Webdienste und Arbeitsabläufe.

Eigenschaftenansicht für eine Anwendung

Die Ansicht **Eigenschaften** zeigt allgemeine Informationen und Laufzeit-Statistiken zu den einzelnen Anwendungen und den Objekten in einer Anwendung. Anwendungen können bereitgestellte Mapping-Jobs, logische Datenobjekte, SQL-Datendienste, Webdienste und Arbeitsabläufe enthalten.

Wenn Sie eine Anwendung im Inhaltsbereich der Ansicht **Eigenschaften** auswählen, können Sie die allgemeinen Eigenschaften und Laufzeit-Statistiken einsehen.

Allgemeine Eigenschaften für eine Anwendung

Sie können die allgemeine Eigenschaften einsehen, wie z. B. Name und Beschreibung der Anwendung. Außerdem können Sie weitere Informationen zu den Objekten in einer Anwendung anzeigen. Um Informationen zu einem Objekt anzuzeigen, wählen Sie den Ordner im Navigator und das Objekt im Inhaltsbereich aus. Das Objekt wird im Navigator unter der Anwendung angezeigt. Die Details zu dem Objekt erscheinen im Detailbereich.

Statistiken für eine Anwendung

Sie können Laufzeit-Statistiken über eine Anwendung und über die mit der Anwendung verknüpften Jobs, Verbindungen, Anfragen und Arbeitsabläufe anzeigen. Beispielsweise können Sie die Anzahl der aktivierten und deaktivierten Anwendungen, die Anzahl der abgebrochenen Verbindungen und die Anzahl der abgeschlossenen, fehlgeschlagenen und abgebrochenen Jobs und Arbeitsabläufe anzeigen.

Berichtsansicht einer Anwendung

Die Ansicht **Berichte** zeigt Überwachungsberichte zu der ausgewählten Anwendung an.

Wenn Sie eine Anwendung auf der Registerkarte **Überwachen** überwachen, zeigt die Ansicht **Berichte** die Berichte zu den Objekten in dieser Anwendung an. Zum Beispiel: Sie können den Bericht "Aktivste Client-IP des Webdienstes" anzeigen lassen, um die IP-Adressen zu ermitteln, die die meisten Webdienstanfragen innerhalb eines bestimmten Zeitraums erhalten haben.

Bereitgestellte Mapping-Jobs überwachen

Sie können bereitgestellte Mapping-Jobs auf der Registerkarte **Überwachen** überwachen.

Sie können Informationen zu bereitgestellten Mapping-Jobs in einer Anwendung anzeigen. Wenn Sie **Logische Datenobjekte** unter einer Anwendung im Navigator auf der Registerkarte **Überwachen** wählen, erscheint eine Liste der logischen Datenobjekte im Inhaltsbereich. Die Inhaltsmaske zeigt die Eigenschaften zu jedem bereitgestellten Mapping-Job, wie Job-ID, Mappingname, Jobstatus und Anfangszeitpunkt des Jobs. Bei Ausführung des Jobs auf einem Gitter wird im Inhaltsbereich auch der Knoten angezeigt, der den Job ausgeführt hat.

Wählen Sie einen bereitgestellten Mapping-Job im Inhaltsbereich aus, um die Protokolle für den Job anzuzeigen, den Job zu wiederholen oder den Job abubrechen.

Wenn Sie den Link für einen bereitgestellten Mapping-Job im Inhaltsbereich auswählen, wird im Inhaltsbereich die Ansicht **Mapping-Eigenschaften** angezeigt. Die Ansicht enthält die Mapping-Eigenschaften, wie z. B. die Nummer der Anfrage, den Namen der Zuordnung und den Namen der Protokolldatei.

Logs für einen bereitgestellten Mapping-Job anzeigen

Sie können die Logs für einen bereitgestellten Mapping-Job herunterladen, um die Jobdetails zu sehen.

Hinweis: Die Protokollinhalte für einen bereitgestellten Mapping-Job hängen von der Konfiguration des Datenintegrationsdiensts ab. Weitere Informationen zu Protokollen für den Fall, dass ein Datenintegrationsdienst-Gitter zur Ausführung von Jobs in separaten Remoteprozessen konfiguriert wurde, finden Sie im *Informatica Application Service-Handbuch*.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Überwachen**.
2. Klicken Sie auf die Ansicht für das **Ausführen von Statistiken**.
3. Erweitern Sie im Domänen-Navigator einen Datenintegrationsdienst.
4. Erweitern Sie eine Anwendung und wählen Sie **Bereitgestellte Mapping-Jobs** aus.
Eine Liste der Mapping-Jobs erscheint im Inhaltsbereich.
5. Wählen Sie einen Mapping-Job aus.
6. Klicken Sie auf **Aktionen > Protokolle für gewähltes Objekt anzeigen**.

Es erscheint ein Dialog mit der Option zum Öffnen oder Speichern der Protokolldatei.

Bereitgestellten Zuordnungsjob erneut ausgeben

Sie können einen bereitgestellten Zuordnungsjob erneut ausgeben, wenn der Job fehlgeschlagen ist. Wenn Sie einen bereitgestellten Zuordnungsjob erneut ausgeben, führt der Datenintegrationsdienst den Job wieder aus.

1. Klicken Sie auf die Ansicht für das **Ausführen von Statistiken**.
2. Erweitern Sie im Domänen-Navigator einen Datenintegrationsdienst.
3. Erweitern Sie eine Anwendung und wählen Sie **Bereitgestellte Zuordnungsjobs** aus.
Im Inhaltsbereich erscheint eine Liste der bereitgestellten Zuordnungsjobs.
4. Wählen Sie einen bereitgestellten Zuordnungsjob aus.
5. Klicken Sie auf **Aktionen > Ausgewähltes Objekt erneut ausgeben**.

Bereitgestellten Mapping-Job abbrechen

Sie können einen bereitgestellten Mapping-Job abbrechen. Wenn ein bereitgestellter Mapping-Job zu umfangreich ist und zu viel Verarbeitungszeit benötigt, können Sie diesen wieder abbrechen.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Überwachen**.
2. Klicken Sie auf die Ansicht für das **Ausführen von Statistiken**.
3. Erweitern Sie im Domänen-Navigator einen Datenintegrationsdienst.
4. Erweitern Sie eine Anwendung und wählen Sie **Bereitgestellte Mapping-Jobs** aus.
Im Inhaltsbereich erscheint eine Liste der bereitgestellten Mapping-Jobs.
5. Wählen Sie einen bereitgestellten Mapping-Job aus.
6. Klicken Sie auf **Aktionen > Ausgewählten Job abbrechen**.

Logische Datenobjekte überwachen

Sie können logische Datenobjekte auf der Registerkarte **Überwachen** in der Ansicht **Ausführungsstatistiken** oder im Monitoring Tool überwachen.

Sie können Informationen über logische Datenobjekte anzeigen, die in einer Anwendung enthalten sind. Zum Überwachen eines logischen Datenobjekts erweitern Sie im Navigator einen Datenintegrationsdienst. Erweitern Sie eine Anwendung und wählen Sie dann den Ordner **Logische Datenobjekte** aus. Im Inhaltsbereich wird eine Liste der logischen Datenobjekte eingeblendet. Im Inhaltsbereich erscheinen die Eigenschaften der logischen Datenobjekte.

Wählen Sie ein logisches Datenobjekt im Inhaltsbereich aus, um die Logs für ein Datenobjekt herunterzuladen.

Wenn Sie im Inhaltsbereich ein logisches Datenobjekt auswählen, werden im Detailbereich die folgenden Ansichten angezeigt:

- Ansicht **Eigenschaften**
- **Cache-Aktualisierungsdurchläufe**

Eigenschaftenansicht für ein logisches Datenobjekt

Die Ansicht **Eigenschaften** zeigt allgemeine Informationen und Laufzeitstatistiken zum gewählten Objekt an.

Sie können Eigenschaften wie den Datenobjektnamen, das logische Datenobjektmodell, den Ordnerpfad, Cache-Status und Informationen zur letzten Cache-Aktualisierung anzeigen.

Ansicht "Cache-Aktualisierungsdurchläufe" für ein logisches Datenobjekt

Die Ansicht **Cache-Aktualisierungsdurchläufe** zeigt Details zur Cache-Aktualisierung des ausgewählten logischen Datenobjekts.

Die Ansicht **Cache-Aktualisierungsdurchläufe** zeigt Details zur Cache-Aktualisierung wie zum Beispiel die Cache-Durchlauf-ID, die Anzahl der Cache-Anfragen und die Anzahl der Zeilen.

Logs für Datenobjekt-Cache-Aktualisierungsdurchläufe

Sie können die Logs für Datenobjekt-Cache-Aktualisierungsdurchläufe herunterladen, um die Cache-Aktualisierungsdetails anzuzeigen.

1. Klicken Sie auf die Ansicht **Ausführungsstatistiken**.
2. Erweitern Sie im Domänen-Navigator einen Datenintegrationsdienst.
3. Erweitern Sie eine Anwendung und wählen Sie **Logische Datenobjekte** aus.
Im Inhaltsbereich erscheint eine Liste der logischen Datenobjekte.
4. Wählen Sie ein logisches Datenobjekt aus.
Die Details zu dem gewählten Datenobjekt erscheinen im Detailbereich.
5. Wählen Sie die Ansicht **Cache-Aktualisierungsdurchläufe** aus.
6. Klicken Sie auf **Protokolle für ausgewähltes Objekt anzeigen**.

SQL-Datendienste überwachen

Sie können logische Datenobjekte auf der Registerkarte **Überwachen** überwachen. Ein SQL-Datendienst ist eine virtuelle Datenbank, die Sie abfragen können. Sie enthält ein Schema und andere Objekte, die die zugrunde liegenden physischen Daten repräsentieren.

Sie können Informationen zu SQL-Datendiensten in einer Anwendung anzeigen. Wenn Sie **SQL-Datendienste** unter einer Anwendung im Navigator der Registerkarte **Überwachen** wählen, erscheint im Inhaltsbereich eine Liste der SQL-Datendienste. Der Inhaltsbereich zeigt die Eigenschaften zu den einzelnen SQL-Datendiensten an, wie z. B. Name, Beschreibung und Status.

Wenn Sie die Verknüpfung für einen SQL-Datendienst im Inhaltsbereich auswählen, werden im Inhaltsbereich die folgenden Ansichten angezeigt:

- Ansicht **Eigenschaften**
- Ansicht **Verbindungen**.
- Ansicht **Anfragen**
- **Virtuelle Tabellen**
- Ansicht **Berichte**

Eigenschaftenansicht für einen SQL-Datendienst

Die Ansicht **Eigenschaften** zeigt allgemeine Informationen und Laufzeitstatistiken für einen SQL-Datendienst an.

Wenn Sie einen SQL-Datendienst im Inhaltsbereich der Ansicht **Eigenschaften** auswählen, können Sie die allgemeinen Eigenschaften und die Laufzeitstatistiken anzeigen.

Allgemeine Eigenschaften für einen SQL-Datendienst

Hierzu gehören der Name des SQL-Datendienstes und die Beschreibung.

Statistiken für einen SQL-Datendienst

Sie können die Laufzeitstatistiken zu Verbindungen und Anfragen an den SQL-Datendienst anzeigen. Zu den Statistiken gehören die Anzahl der Verbindungen zum SQL-Datendienst, die Anzahl der Anfragen und die Anzahl der abgebrochenen Verbindungen.

Verbindungsansicht für einen SQL Data Service

In der Ansicht **Verbindungen** sind die Eigenschaften der Verbindungen von Drittparteien-Clients aufgelistet. Die Ansicht enthält Eigenschaften wie die Verbindungs-ID, den Verbindungsstatus, die Verbindungszeit, die abgelaufene Zeit und den Zeitpunkt der Trennung.

Beim Auswählen einer Verbindung in der Inhaltsübersicht können Sie die Verbindung abbrechen oder in die Ansicht **Eigenschaften** und die Ansicht **Anfragen** in der Maske Details gehen.

Eigenschaften-Ansicht

Die Ansicht **Eigenschaften** in der Maske Details zeigt den Benutzer, der die Verbindung nutzt, den Verbindungsstatus und den Zeitpunkt der Verbindung.

Anfragen-Ansicht

Die Ansicht **Anfragen** in der Maske Details enthält Informationen über die Anfragen für die SQL-Verbindung. Jede Verbindung kann mehr als eine Anfrage aufweisen. In jeder Ansicht sind die Eigenschaften der Anfrage eingeblendet, wie Anfrage-ID, Benutzername, Anfragestatus, Startzeit, abgelaufene Zeit und Endezeit.

Verbindung abbrechen

Sie können eine Verbindung abbrechen, um zu verhindern, dass weitere Anfragen an den SQL-Datendienst verschickt werden.

1. Klicken Sie auf die Ansicht **Ausführungsstatistiken**.
2. Erweitern Sie im Domänennavigator einen Datenintegrationsdienst.
3. Erweitern Sie eine Anwendung und wählen Sie **SQL-Datendienste** aus.
Im Inhaltsbereich werden die SQL-Datendienste in der Anwendung aufgeführt.
4. Wählen Sie einen SQL-Datendienst aus.
Im Inhaltsbereich erscheinen mehrere Ansichten des SQL-Datendienstes.
5. Klicken Sie auf die Ansicht **Verbindungen**.
Der Inhaltsbereich listet die aktiven Verbindungen zum SQL-Datendienst auf.
6. Wählen Sie eine Verbindung.
7. Klicken Sie auf **Aktionen > Ausgewählte Verbindung abbrechen**.

Anfrageansicht eines SQL-Datendienstes

Die Ansicht **Anfragen** zeigt die Eigenschaften für die Anfragen zu jeder SQL-Verbindung an.

Die Ansicht **Anfragen** zeigt die Eigenschaften für die Anfragen zu einer SQL-Verbindung an. Jede Verbindung kann mehr als eine Anfrage haben. Die Ansicht zeigt Anfrageeigenschaften wie die Anfrage-ID, die Verbindungs-ID, den Benutzernamen, den Status der Anfrage, die Startzeit, die Ausführungszeit und die Endezeit an.

Wählen Sie eine Anfrage im Inhaltsbereich aus, um zusätzliche Informationen zu der Anfrage im Detailbereich zu erhalten.

Abbrechen einer Verbindungsanfrage für SQL-Datendienst

Sie können eine Verbindungsanfrage für einen SQL-Datendienst jederzeit abbrechen. Wenn eine Verbindungsanfrage hängt oder zu viel Verarbeitungszeit benötigt, können Sie diese abbrechen.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Überwachen**.
2. Erweitern Sie im Navigator einen Data Integration Service.
3. Erweitern Sie im Navigator eine Anwendung und wählen Sie **SQL-Datendienste**.
Im Inhaltsbereich erscheint eine Liste der SQL-Datendienste.
4. Wählen Sie daraus einen SQL-Datendienst aus.
5. Klicken Sie im Inhaltsbereich auf die Ansicht **Anfragen**.
Eine Liste der Verbindungsanfragen an den SQL-Datendienst erscheint.
6. Wählen Sie im Inhaltsbereich eine Anfragezeile aus.
7. Klicken Sie auf **Aktionen > Abbrechen der ausgewählten Anfrage**.

Logs für eine SQL-Datendienstanfrage anzeigen

Sie können die Logs für eine SQL-Datendienstanfrage herunterladen, um die Abfragedetails zu sehen.

1. Klicken Sie auf die Ansicht für das **Ausführen von Statistiken**.
2. Erweitern Sie im Domänennavigator einen Datenintegrationsdienst.

3. Erweitern Sie eine Anwendung und wählen Sie **SQL-Datendienste** aus.
Im Inhaltsbereich erscheint eine Liste der SQL-Datendienste.
4. Wählen Sie einen SQL-Datendienst aus.
5. Klicken Sie auf die Ansicht **Anfragen**.
Eine Liste der Anfragen für den SQL-Datendienst wird angezeigt.
6. Wählen Sie eine Anfragezeile aus.
7. Klicken Sie auf **Aktionen > Logs für gewähltes Objekt anzeigen**.

Virtuelle Tabellen für einen SQL-Datendienst anzeigen

Die Ansicht **Virtuelle Tabellen** zeigt die Eigenschaften der virtuellen Tabellen im SQL-Datendienst an.

Zu den Eigenschaften für virtuelle Tabellen gehören zum Beispiel der Name und die Beschreibung. Wenn Sie im Inhaltsbereich eine virtuelle Tabelle wählen, können Sie die Ansicht **Eigenschaften** anzeigen lassen und im Detailbereich die Ansicht **Cache-Aktualisierungsdurchläufe**.

Die Eigenschaftenansicht

Die Ansicht **Eigenschaften** zeigt allgemeine Informationen und Laufzeitstatistiken zur gewählten virtuellen Tabelle an. Die allgemeinen Eigenschaften enthalten den Namen der virtuellen Tabelle und den Schemanamen. Das Überwachen von Statistiken beinhaltet die Anzahl von Anfragen, die Anzahl zwischengespeicherter Zeilen und den Zeitpunkt der letzten Cache-Aktualisierung.

Die Ansicht "Cache-Aktualisierungsdurchläufe"

Die Ansicht **Cache-Aktualisierungsdurchläufe** zeigt die Cache-Informationen für die gewählte virtuelle Tabelle an. Dazu gehören die Cache-Durchlauf-ID, die Anfragezählung, die Zeilenzählung und die Cache-Trefferquote. Die Cache-Trefferquote ist die Gesamtanzahl der Anfragen an den Cache dividiert durch die Gesamtanzahl der Anfragen für das Datenobjekt.

Logs für eine SQL-Datendienst-Tabellen-Cache anzeigen

Sie können die Logs für einen SQL-Datendienst-Tabellen-Cache herunterladen, um die Tabellen-Cache-Details zu sehen.

1. Klicken Sie auf die Ansicht für das **Ausführen von Statistiken**.
2. Erweitern Sie im Domänennavigator einen Datenintegrationsdienst.
3. Erweitern Sie eine Anwendung und wählen Sie **SQL-Datendienste** aus.
Im Inhaltsbereich erscheint eine Liste der SQL-Datendienste.
4. Wählen Sie einen SQL-Datendienst aus.
5. Klicken Sie auf die Ansicht **Virtuelle Tabellen**.
Eine Liste der virtuellen Tabellen für den SQL-Datendienst wird angezeigt.
6. Wählen Sie eine Tabellenzeile aus.
Die Details zu der gewählten Tabelle erscheinen im Detailbereich.
7. Wählen Sie die Ansicht **Cache-Aktualisierungsdurchläufe** aus.
8. Klicken Sie auf **Protokolle für ausgewähltes Objekt anzeigen**.

Berichtsansicht eines SQL-Datendienstes

Die Ansicht **Berichte** zeigt Überwachungsberichte zum ausgewählten SQL-Datendienst an.

Wenn Sie einen SQL-Datendienst überwachen, werden in der Ansicht **Berichte** Berichte über den SQL-Datendienst angezeigt. Zum Beispiel: Sie können den Bericht "Aktivste SQL-Verbindungen" anzeigen lassen, um jene SQL-Verbindungen zu ermitteln, die die meisten Verbindungsanfragen innerhalb eines bestimmten Zeitraums erhalten haben.

Web-Dienste überwachen

Sie können Webdienste auf der Registerkarte **Überwachen** in der Ansicht **Ausführungsstatistiken** überwachen. Web-Dienste sind Geschäftsfunktionen, die im Web operieren. Sie beschreiben eine Sammlung von Operationen, die durch das standardisierte XML-Messaging Zugang zu Netzwerken haben.

Sie können Informationen über Web-Dienste anzeigen, die in einer Anwendung enthalten sind. Zum Überwachen eines Webdiensts erweitern Sie im Navigator eine Anwendung und wählen den Ordner **Webdienste** aus. Im Inhaltsbereich wird eine Liste der Webdienste eingeblendet. Der Inhaltsbereich zeigt die Eigenschaften eines jeden Web-Dienstes an, z. B. den Namen, die Beschreibung und den Status jedes Web-Dienstes.

Wenn Sie im Inhaltsbereich den Link zu einem Web-Dienst auswählen, zeigt das Inhaltsfenster die folgenden Ansichten:

- Ansicht **Eigenschaften**
- Ansicht **Berichte**
- **Ansicht Operationen**
- Ansicht **Anfragen**

Eigenschaftenansicht für einen Web-Dienst

Die Ansicht **Eigenschaften** zeigt allgemeine Informationen und Laufzeitstatistiken zum gewählten Web-Dienst an.

Wenn Sie einen Web-Dienst im Inhaltsbereich der Ansicht **Eigenschaften** auswählen, können Sie die allgemeinen Eigenschaften und die Überwachungsstatistiken anzeigen.

Allgemeine Eigenschaften für einen Web-Dienst

Zu den allgemeinen Eigenschaften eines Web-Dienstes gehören der Name und der Objekttyp.

Statistiken für einen Web-Dienst

Sie können die Laufzeitstatistiken zu den Anfragen an einen Web-Dienst innerhalb eines bestimmten Zeitraums anzeigen. Der Abschnitt **Statistiken** zeigt die Anzahl der abgeschlossenen und fehlgeschlagenen Anfragen sowie die Gesamtanzahl an.

Berichtsansicht eines Web-Dienstes

Die Ansicht **Berichte** zeigt Überwachungsberichte zum ausgewählten Web-Dienst an.

Beim Überwachen eines Webdiensts werden in der Ansicht **Berichte** Berichte über den Webdienst angezeigt. Sie können beispielsweise den Bericht „Aktivste Client-IP des Webdiensts“ anzeigen, um die IP-Adressen zu ermitteln, die die meisten Webdienstanfragen innerhalb eines bestimmten Zeitraums erhalten haben.

Operationsansicht für einen Web-Dienst

Die Ansicht **Operationen** zeigt den Namen und die Beschreibung der einzelnen Operationen im Web-Dienst an. Außerdem zeigt die Ansicht auch Eigenschaften, Anfragen und Berichte zu jeder Operation.

Wenn Sie eine Web-Dienst-Operation im Inhaltsbereich auswählen, werden im Detailbereich die Ansichten **Eigenschaften**, **Anfragen** und **Berichte** angezeigt.

Eigenschaftenansicht für eine Web-Dienst-Operation

Die Ansicht **Eigenschaften** zeigt allgemeine Informationen und Statistiken zur gewählten Web-Dienst-Operation an. Zu den allgemeinen Eigenschaften gehören der Name der Operation und der Typ des Objekts. Die Ansicht zeigt auch Statistiken zur Web-Dienst-Operation während eines bestimmten Zeitraums. Die Statistik umfasst die Anzahl der abgeschlossenen und fehlgeschlagenen Web-Service-Anfragen sowie deren Gesamtanzahl.

Anfrageansicht für eine Web-Dienst-Operation

Die Ansicht **Anfragen** zeigt Eigenschaften zu den einzelnen Web-Dienst-Operationen, wie Nummer der Anfrage, Benutzernamen, Status, Startzeit, verstrichene Zeit und Endzeit. Sie können die Liste der Anfragen filtern. Außerdem können Sie Logs für die ausgewählte Web-Dienst-Anfrage anzeigen.

Berichtsansicht für eine Web-Dienst-Operation

Die Ansicht **Berichte** zeigt Berichte über Web-Service-Operationen.

Anfrageansicht eines Webdienstes

Die Ansicht **Anfragen** zeigt die Eigenschaften jeder Webdienstanfrage an, z. B. die Anfrage-ID, den Benutzernamen, Status, Startzeit, Ausführungszeit und Endezeit. Sie können diese Anfrageliste filtern.

Wenn Sie eine Webdienstanfrage im Inhaltsbereich auswählen, erscheinen die Protokolle zu der Anfrage im Detailbereich. Der Detailbereich zeigt die allgemeinen Eigenschaften und Statistiken zu der ausgewählten Webdienstanfrage an. Die Statistiken enthalten die Anzahl der abgeschlossenen und fehlgeschlagenen Anfragen sowie die Gesamtanzahl der Anfragen an den Webdienst.

Sie können auch eine Webdienstanfrage über die Ansicht **Anfragen** abbrechen. Wählen Sie zum Abbrechen einer Webdienstanfrage die Arbeitsablauf-Anfrage aus und klicken Sie im Inhaltsbereich auf **Aktionen** > **Ausgewählte Anfrage abbrechen**.

Überwachen von Arbeitsabläufen

Sie können Arbeitsabläufe auf der Registerkarte **Überwachen** überwachen.

Sie können Informationen über Arbeitsablaufinstanzen anzeigen, die über einen Arbeitsablauf in einer bereitgestellten Anwendung ausgeführt werden. Wenn Sie die Option **Arbeitsabläufe** unter einer Anwendung im Navigator auf der Registerkarte **Überwachen** auswählen, wird eine Liste der Arbeitsablaufinstanzen im Inhaltsbereich angezeigt. Im Inhaltsbereich werden die Eigenschaften zu jeder Arbeitsablaufinstanz angezeigt, wie zum Beispiel Name, Status, Anfangszeitpunkt und verstrichene Zeit für jede Arbeitsablaufinstanz. Wenn Sie eine Ablaufinstanz auf einem Gitter ausgeführt haben, zeigt der Inhaltsbereich auch den Knoten an, der jedes Mapping in der Ablaufinstanz ausgeführt hat.

Wählen Sie eine Arbeitsablaufinstanz im Inhaltsbereich, um die folgenden Aufgaben auszuführen:

- Anzeigen von Protokollen für die Arbeitsablaufinstanz

- Anzeigen des Kontexts der Arbeitsablaufinstanz, um andere Arbeitsablaufinstanzen anzuzeigen, die ungefähr zur gleichen Zeit wie die ausgewählte Arbeitsablaufinstanz begonnen hat.
- Abbrechen der Arbeitsablaufinstanz
- Wiederherstellen der unterbrochen Arbeitsablaufinstanz

Erweitern Sie eine Arbeitsablaufinstanz, um die Eigenschaften zu jedem Arbeitsablaufobjekt einschließlich Aufgaben und Gateways anzuzeigen.

Arbeitsablaufgrafik

Sie können die Details eines im Monitoring-Tool ausgeführten Arbeitsablaufs in einer Grafik anzeigen.

Nach dem Ausführen eines Arbeitsablaufs wird die Grafikanzeige des Arbeitsablaufs im Monitoring-Tool angezeigt. In der Arbeitsablaufgrafik wird die sequenzielle Ausführung der Mapping-Aufgaben im Arbeitsablauf dargestellt. In der Arbeitsablaufgrafik können Sie Fehlerpunkte in einem Arbeitsablauf sofort erkennen.

In der Arbeitsablaufgrafik werden die folgenden Details eines Arbeitsablaufs dargestellt:

- Mapping-Aufgaben im Arbeitsablauf
- Aufgabendetails
- Wiederherstellungsdetails

In der Arbeitsablaufgrafik können Sie die folgenden Aufgaben durchführen:

- Beenden eines laufenden Arbeitsablaufs
- Abbrechen eines laufenden Arbeitsablaufs
- Wiederherstellen eines fehlgeschlagenen Arbeitsablaufs
- Anzeigen der Arbeitsablaufprotokolle

Anzeigen einer Arbeitsablaufgrafik

In einer Arbeitsablaufgrafik können Sie die sequenzielle Ausführung der Zuordnungsaufgaben im Arbeitsablauf anzeigen.

1. Klicken Sie auf die Ansicht für das **Ausführen von Statistiken**.
2. Erweitern Sie im Domänennavigator eine Anwendung.
3. Wählen Sie den Ordner **Arbeitsabläufe** aus.
Eine Liste mit Arbeitsabläufen wird im Inhaltsbereich angezeigt.
4. Wählen Sie den Arbeitsablauf aus, den Sie anzeigen möchten.
5. Klicken Sie auf **Aktionen > Arbeitsablaufdiagramm anzeigen**.
Die Arbeitsablaufgrafik wird in einem neuen Fenster geöffnet.

Anzeigen von Arbeitsablaufobjekten

Wenn Sie eine Arbeitsablaufinstanz im Inhaltsbereich erweitern, können Sie die Eigenschaften der Arbeitsablaufobjekte anzeigen, wie zum Beispiel Name, Status, Anfangszeitpunkt und verstrichene Zeit für das Objekt.

Arbeitsablaufobjekte beinhalten Ereignisse, Aufgaben und Gateways. Wenn Sie Arbeitsabläufe überwachen, können Sie ebenfalls Aufgaben und Gateways überwachen, die in einer Arbeitsablaufinstanz ausgeführt

werden. Die Registerkarte "Überwachen" zeigt keine Informationen über Ereignisse in der Arbeitsablaufinstanz an.

Wenn ein Ausdruck in einem bedingten Sequenzfluss als "false" bewertet wird, führt der Data Integration Service nicht das nächste Objekt oder nachfolgende Objekte in diesem Zweig aus. Die Registerkarte "Überwachen" listet keine Objekte auf, die nicht in der Arbeitsablaufinstanz ausgeführt werden. Wenn eine Arbeitsablaufinstanz Objekte enthält, die nicht ausgeführt werden, kann die Instanz trotzdem erfolgreich abgeschlossen werden.

Sie können eine Aufgabe in der Inhaltskonsolle erweitern, um Informationen über das Arbeitselement anzuzeigen, das von der Aufgabe ausgeführt wird. Sie können beispielsweise eine Mapping-Aufgabe erweitern, um Informationen über die Mapping-Ausführung durch die Mapping-Aufgabe anzuzeigen.

Arbeitsablaufstatus

Wenn Sie eine Arbeitsablaufinstanz überwachen, können Sie den Status der Arbeitsablaufinstanz anzeigen. Trifft die Arbeitsablaufinstanz während eines Wiederherstellungslaufs auf den Status, wird an den Status der Text (Wiederherstellung) angehängt.

Eine Arbeitsablaufinstanz kann einen der folgenden Status annehmen:

Abgebrochen

Eine Arbeitsablaufinstanz bricht in folgenden Situationen ab:

- Der Arbeitsablauf ist für die Wiederherstellung aktiviert, und eine Aufgabe mit einer Neustart-Wiederherstellungsstrategie trifft auf einen wiederherstellbaren Fehler.
- Sie können die Arbeitsablaufinstanz im Tool "Überwachen" oder über den Befehl "infacmd wfs abortWorkflow" vorzeitig beenden. Sie können sich auch zum Stornieren einer laufenden Arbeitsablaufinstanz entscheiden, wenn Sie den Data Integration Service deaktivieren oder recyceln, wenn Sie die Anwendung beenden, die den Arbeitsablauf enthält, oder wenn Sie den Arbeitsablauf in der Anwendung deaktivieren.
- Der Arbeitsablauf ist für die Wiederherstellung aktiviert ist, und der Data Integration Service-Prozess fährt unerwartet herunter, während diese Arbeitsablaufinstanz ausgeführt wird.

Während der Datenintegrationsdienst nach dem Herunterfahren einen deaktivierten Status aufweist, verbleibt die Arbeitsablaufinstanz im Ausführungsstatus, auch wenn die Instanz nicht mehr ausgeführt wird. Wenn der Arbeitsablauf für die automatische Wiederherstellung nicht konfiguriert ist, ändert der Dienstprozess den Arbeitsablaufinstanzstatus in „Storniert“, wenn der Dienstprozess neu startet. Wenn der Arbeitsablauf für die automatische Wiederherstellung konfiguriert ist, stellt der Dienstprozess die Arbeitsablaufinstanz wieder her, wenn der Dienstprozess neu startet. Der Dienst ändert die Arbeitsablaufinstanz in „Wird ausgeführt“ (Wiederherstellung).

Eine Arbeitsablaufinstanz wird abgebrochen, wenn Sie die Arbeitsablaufinstanz über das Überwachungs-Tool oder mithilfe des infacmd wfs abortWorkflow-Befehls abbrechen. Sie können eine laufende Arbeitsablaufinstanz auch abbrechen, wenn Sie den Datenintegrationsdienst deaktivieren oder recyceln, wenn Sie die Anwendung beenden, die den Arbeitsablauf enthält, oder wenn Sie den Arbeitsablauf in der Anwendung deaktivieren.

Während der Datenintegrationsdienst nach dem Herunterfahren einen deaktivierten Status aufweist, verbleibt die Arbeitsablaufinstanz im Ausführungsstatus, auch wenn die Instanz nicht mehr ausgeführt wird. Der Dienstprozess ändert den Status der Arbeitsablaufinstanz in "Abgebrochen", wenn der Dienstprozess neu gestartet wird.

Storniert

Sie können die Arbeitsablaufinstanz auf der Registerkarte „Überwachen“ oder über den infacmd wfs cancelWorkflow-Befehl abbrechen.

Abgeschlossen

Der Datenintegrationsdienst schließt die Arbeitsablaufinstanz erfolgreich ab. Eine abgeschlossene Arbeitsablaufinstanz bedeutet, dass alle Aufgaben, Gateways und Sequenzflussauswertungen entweder erfolgreich abgeschlossen oder in einer Verzweigung waren, die nicht ausgeführt wurde.

Fehlgeschlagen

Eine Arbeitsablaufinstanz schlägt in folgenden Situationen fehl:

- Ein Arbeitsablauffehler ist aufgetreten. Arbeitsablauffehler können auftreten, wenn der Datenintegrationsdienst die Parameterdatei am Anfang des Arbeitsablaufs liest, Arbeitsablaufparameter und Variablenwerte in die Aufgabeneingabe kopiert oder Ausdrücke in konditionalen Sequenzflüssen auswertet. Zusätzlich tritt ein Arbeitsablauffehler auf, wenn eine Zuweisungsaufgabe oder ein exklusives Gateway fehlschlägt.

Wenn ein Arbeitsablauffehler auftritt, beendet der Datenintegrationsdienst die Verarbeitung zusätzlicher Objekte und schlägt bei der Arbeitsablaufinstanz sofort fehl.

- Ein Befehl, ein Mapping oder eine Benachrichtigung in der Arbeitsablaufinstanz ist fehlgeschlagen.

Eine Befehls-, Mapping-, Benachrichtigungs- oder Human-Aufgabe in der Arbeitsablaufinstanz ist fehlgeschlagen.

Wenn diese Aufgaben fehlschlagen, führt der Datenintegrationsdienst zusätzliche Objekte in der Arbeitsablaufinstanz weiter aus, wenn Ausdrücke in den konditionalen Sequenzflüssen als True ausgewertet werden oder wenn die Sequenzflüsse keine Bedingungen enthalten. Wenn die Arbeitsablaufinstanz die Ausführung ohne weitere Unterbrechung beendet, aktualisiert der Datenintegrationsdienst den Arbeitsablaufstatus auf „Fehlgeschlagen“. Eine fehlgeschlagene Arbeitsablaufinstanz kann sowohl fehlgeschlagene als auch abgeschlossene Aufgaben enthalten.

Wird ausgeführt

Der Datenintegrationsdienst führt die Arbeitsablaufinstanz aus.

Unbekannt

Eine Arbeitsablaufinstanz hat in folgenden Situationen einen Status "Unbekannt":

- Der Arbeitsablauf ist für die Wiederherstellung nicht aktiviert, und der Datenintegrationsdienst-Prozess fährt unerwartet herunter, während diese Arbeitsablaufinstanz ausgeführt wird.

Während der Datenintegrationsdienst in einem deaktivierten Status bleibt, bleibt die Arbeitsablaufinstanz im Ausführungsstatus, auch wenn die Instanz nicht mehr ausgeführt wird. Wenn der Dienstprozess neu startet, ändert der Dienst den Arbeitsablaufinstanzstatus in "Unbekannt".

- Der Arbeitsablauf ist für die Wiederherstellung aktiviert, und die Arbeitsablaufinstanz hat einen abgebrochenen Status. Sie ändern die Arbeitsablaufdefinition im Developer-Tool und stellen die Anwendung, die den Arbeitsablauf enthält, erneut bereit. Da sich die Metadaten des Arbeitsablaufs geändert haben, kann die Arbeitsablaufinstanz nicht mehr wiederhergestellt werden. Als Ergebnis aktualisiert der Datenintegrationsdienst den Status der Arbeitsablaufinstanz auf "Unbekannt".
- Sie können eine laufende Arbeitsablaufinstanz abbrechen, wenn Sie den Datenintegrationsdienst deaktivieren oder recyceln, wenn Sie die Anwendung beenden, die den Arbeitsablauf enthält, oder wenn Sie den Arbeitsablauf in der Anwendung deaktivieren. Der Datenintegrationsdienst versucht 60 Sekunden lang, den Prozess für alle laufenden Aufgaben zu beenden. Wenn der Dienst die laufende Aufgabe nicht innerhalb von 60 Sekunden abbrechen kann, fährt der Dienst die Arbeitsablaufinstanz herunter und ändert den Status der Arbeitsablaufinstanz in "Unbekannt".

Sie können eine laufende Arbeitsablaufinstanz abbrechen, wenn Sie den Datenintegrationsdienst deaktivieren oder recyceln, wenn Sie die Anwendung beenden, die den Arbeitsablauf enthält, oder wenn Sie den Arbeitsablauf in der Anwendung deaktivieren. Der Datenintegrationsdienst versucht 60 Sekunden lang, den Prozess für alle laufenden Aufgaben zu beenden. Wenn der Dienst die laufende Aufgabe nicht

innerhalb von 60 Sekunden abbrechen kann, fährt der Dienst die Arbeitsablaufinstanz herunter und ändert den Status der Arbeitsablaufinstanz in "Unbekannt".

Arbeitsablaufobjektstatus

Wenn Sie eine Arbeitsablaufinstanz überwachen, können Sie den Status aller Aufgaben und Gateways anzeigen, die in der Arbeitsablaufinstanz ausgeführt werden. Trifft die Aufgabe oder das Gateway während eines Wiederherstellungslaufs auf den Status, wird an den Status der Text (Wiederherstellung) angehängt.

Aufgaben und Gateways können einen der folgenden Status annehmen:

Abgebrochen

Aufgaben und Gateways können aus verschiedenen Gründen abbrechen.

Die folgende Tabelle beschreibt die Ursachen, die zu einem Abbruch von Aufgaben und Gateways führen können:

Grund für den Abbruch	Aufgaben- und Gateway-Typ	Beschreibung
Sie entscheiden sich zum Abbrechen der Arbeitsablaufinstanz.	Befehl Mapping Benachrichtigung	<p>Eine Aufgabe wird in folgenden Situationen abgebrochen:</p> <ul style="list-style-type: none"> - Die Ausgabe befindet sich in einem nicht für die Wiederherstellung aktivierten Arbeitsablauf und läuft, wenn Sie sich entschließen, die Arbeitsablaufinstanz abbrechen. - Bei der Aufgabe wurde eine Neustart-Wiederherstellungsstrategie in einem Arbeitsablauf für die Wiederherstellung aktiviert und wird ausgeführt, wenn Sie sich entschließen, die Arbeitsablaufinstanz abbrechen. <p>Nach Abbruch der Aufgabe bricht der Datenintegrationsdienst die Arbeitsablaufinstanz ab. Wenn Sie die Arbeitsablaufinstanz abbrechen, während eine Zuweisungsaufgabe oder ein Gateway ausgeführt wird, schließt der Datenintegrationsdienst die Ausführung der Aufgabe oder des Gateways ab. Der Dienst bricht dann die Arbeitsablaufinstanz ab und beginnt nicht mit der Ausführung zusätzlicher Objekte.</p>
Aufgabe mit einer Neustart-Wiederherstellungsstrategie trifft auf einen wiederherstellbaren Fehler.	Befehl Mapping Benachrichtigung	Bei der Aufgabe wurde eine Neustart-Wiederherstellungsstrategie in einem Arbeitsablauf für die Wiederherstellung aktiviert, und die Aufgabe trifft auf einen wiederherstellbaren Fehler.
Der Dienstprozess fährt unerwartet herunter.	Alle Aufgabentypen Exklusives Gateway	<p>Eine Aufgabe mit einer Neustart-Wiederherstellungsstrategie, eine Zuweisungsaufgabe oder ein exklusives Gateway befindet sich in einem für die Wiederherstellung aktivierten Arbeitsablauf. Die Aufgabe oder das Gateway wird ausgeführt, wenn der Dienstprozess unerwartet heruntergefahren wird.</p> <p>Während sich der Datenintegrationsdienst-Prozess in einem deaktivierten Status befindet, verbleibt die Aufgabe im Ausführungsstatus, auch wenn die Aufgabe nicht mehr ausgeführt wird. Der Dienstprozess ändert den Aufgabenstatus in „Abgebrochen“, wenn der Dienstprozess erneut gestartet wird.</p> <p>Wenn der Arbeitsablauf nicht für die automatische Wiederherstellung konfiguriert ist, ändert der Dienstprozess den Aufgabenstatus in Abgebrochen, wenn der Dienstprozess neu startet.</p> <p>Wenn der Arbeitsablauf für die automatische Wiederherstellung konfiguriert ist, stellt der Dienstprozess die Arbeitsablaufinstanz wieder her und startet die unterbrochene Aufgabe neu, wenn der Dienstprozess neu startet. Der Dienstprozess ändert den Aufgabenstatus in „Wird ausgeführt“ (Wiederherstellung).</p>

Abgeschlossen

Der Datenintegrationsdienst schließt die Aufgabe oder das Gateway erfolgreich ab.

Fehlgeschlagen

Eine Aufgabe oder ein Gateway schlägt in folgenden Situationen fehl:

- Eine Aufgabe oder ein Gateway in einem Arbeitsablauf, der nicht für die Wiederherstellung aktiviert ist, trifft auf einen beliebigen Fehlertyp.
- Eine Zuweisungsaufgabe oder ein exklusives Gateway in einem Arbeitsablauf, das für die Wiederherstellung aktiviert ist, trifft auf einen beliebigen Fehlertyp.
- Eine Befehls-, Mapping- oder Benachrichtigungsaufgabe mit einer Neustart-Wiederherstellungsstrategie in einem Arbeitsablauf, der für die Wiederherstellung aktiviert ist, trifft auf einen nicht wiederherstellbaren Fehler.
- Eine Befehls-, Mapping- oder Benachrichtigungsaufgabe mit einer Strategie zum Überspringen der Wiederherstellung in einem Arbeitsablauf, der für die Wiederherstellung aktiviert ist, trifft auf einen beliebigen Fehlertyp, wird ausgeführt, wenn die Arbeitsablaufinstanz abbricht, oder wird ausgeführt, wenn der Dienstprozess unerwartet herunterfährt.

Wird ausgeführt

Der Datenintegrationsdienst führt die Aufgabe oder das Gateway aus.

Unbekannt

Eine Aufgabe oder ein Gateway hat in folgenden Situationen einen Status "Unbekannt":

- Eine Aufgabe oder ein Gateway befindet sich in einem Arbeitsablauf, der nicht für die Wiederherstellung aktiviert ist. Die Aufgabe oder das Gateway wird ausgeführt, wenn der Dienstprozess unerwartet heruntergefahren wird.

Während sich der Datenintegrationsdienst-Prozess in einem deaktivierten Status befindet, verbleibt der Aufgaben- oder Gatewaystatus im Ausführungsstatus, auch wenn die Aufgabe oder das Gateway nicht mehr ausgeführt wird. Wenn der Dienstprozess neu startet, ändert der Dienst den Aufgaben- oder Gatewaystatus in "Unbekannt".

- Sie können eine laufende Arbeitsablaufinstanz abbrechen, wenn Sie den Datenintegrationsdienst deaktivieren oder recyceln, wenn Sie die Anwendung beenden, die den Arbeitsablauf enthält, oder wenn Sie den Arbeitsablauf in der Anwendung deaktivieren. Der Datenintegrationsdienst versucht 60 Sekunden lang, den Prozess für alle laufenden Aufgaben oder Gateways zu beenden. Wenn der Dienst die laufende Aufgabe oder das laufende Gateway nicht innerhalb von 60 Sekunden abbrechen kann, fährt der Dienst die Arbeitsablaufinstanz herunter und ändert den Status der Aufgabe oder des Gateways in "Unbekannt".

Arbeitselementstatus der Mapping-Aufgabe

Wenn Sie eine Mapping-Aufgabe erweitern, können Sie den Status der Mapping-Ausführung anzeigen. Wenn Sie eine neu gestartete Mapping-Aufgabe erweitern, können Sie die Mapping-Jobs anzeigen, die für jeden Wiederherstellungsversuch der Arbeitsablaufinstanz ausgeführt wurden.

Trifft die Mapping-Aufgabe während eines Wiederherstellungslaufs auf den Status, wird an den Status der Text (Wiederherstellung) angehängt. Sie können auch den Status der Mapping-Ausführung im Arbeitsablaufdiagramm des Arbeitsablaufs anzeigen, der die Mapping-Aufgabe enthält.

Mappings, die von einer Mapping-Aufgabe ausgeführt werden, können einen der folgenden Status annehmen:

Abgebrochen

Die Mapping-Aufgabe bricht ab, während das Mapping ausgeführt wird, da Sie sich entscheiden, die Arbeitsablaufinstanz abzubrechen.

Abgeschlossen

Der Datenintegrationsdienst schließt das Mapping erfolgreich ab.

Fehlgeschlagen

Das Mapping trifft auf einen Fehler. Wenn bei der Mapping-Aufgabe eine Neustart-Wiederherstellungsstrategie in einem Arbeitsablauf für die Wiederherstellung aktiviert ist und das Mapping auf einen Fehler trifft, schlägt das Mapping fehl, aber die Mapping-Aufgabe bricht ab.

Wird ausgeführt

Der Datenintegrationsdienst führt das Mapping aus.

Unbekannt

Die Mapping-Aufgabe ist in einem Arbeitsablauf, der für die Wiederherstellung aktiviert ist oder nicht für die Wiederherstellung aktiviert ist. Das Mapping wird ausgeführt, wenn der Datenintegrationsdienst unerwartet heruntergefahren wird.

Während sich der Datenintegrationsdienst-Prozess in einem deaktivierten Status befindet, verbleibt der Mapping-Status im Ausführungsstatus, auch wenn das Mapping nicht mehr ausgeführt wird. Wenn der Dienstprozess neu startet, ändert der Dienst den Mapping-Status in Unbekannt.

Abbrechen eines Arbeitsablaufs

Sie können eine Arbeitsablaufinstanz jederzeit abbrechen. Sie möchten beispielsweise eine Arbeitsablaufinstanz abbrechen, die nicht mehr reagiert oder die zu viel Zeit in Anspruch nimmt, um abzuschließen.

Wenn Sie eine Arbeitsablaufinstanz abbrechen, beendet der Datenintegrationsdienst die Verarbeitung aller laufenden Aufgaben sowie die Verarbeitung der Arbeitsablaufinstanz. Der Dienst beginnt nicht mit der Ausführung von nachfolgenden Arbeitsablaufobjekten.

Wenn Sie eine Arbeitsablaufinstanz abbrechen, versucht der Datenintegrationsdienst, den Prozess für alle laufenden Aufgaben abzubrechen. 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.

Sie können einen Arbeitsablauf auch im Arbeitsablaufdiagramm abbrechen oder daraus entfernen.

1. Klicken Sie im Administrator-Tool auf die Registerkarte **Überwachen**.
2. Erweitern Sie im Navigator einen Datenintegrationsdienst.
3. Erweitern Sie im Navigator eine Anwendung und wählen Sie **Arbeitsabläufe** aus.
Eine Liste mit Arbeitsablaufinstanzen wird im Inhaltsbereich angezeigt.
4. Wählen Sie im Inhaltsbereich eine Arbeitsablaufinstanz aus.
5. Klicken Sie auf **Aktionen > Ausgewählten Arbeitsablauf stornieren** oder **Aktionen > Ausgewählten Arbeitsablauf abbrechen**.

Arbeitsablauf-Wiederherstellung

Bei der Arbeitsablaufwiederherstellung handelt es sich um den Abschluss einer Arbeitsablaufinstanz ab dem Unterbrechungspunkt.

Bei einem für die Wiederherstellung aktivierten Arbeitsablauf können Sie eine Arbeitsablaufinstanz wiederherstellen, wenn eine Aufgabe mit einer Neustart-Wiederherstellungsstrategie auf einen

wiederherstellbaren Fehler trifft, wenn Sie die Arbeitsablaufinstanz abbrechen oder stornieren oder wenn der Data Integration Service unerwartet herunterfährt.

Der Abbruch einer Arbeitsablaufinstanz kann mehrere Gründe haben. Zeigen Sie das Arbeitsablaufprotokoll an, um die Ursache der Unterbrechung zu identifizieren. Nach dem Beheben aller wiederherstellbaren Fehler können Sie die unterbrochene Arbeitsablaufinstanz wiederherstellen, wenn sie für die Wiederherstellung aktiviert ist.

Zwischen der unterbrochenen Ausführung und dem Wiederherstellungslauf kann eine Arbeitsablaufdefinition nicht geändert werden. Wenn eine Arbeitsablaufinstanz einen wiederherstellbaren Status hat und Sie die Arbeitsablaufmetadaten im Developer-Tool ändern und die Anwendung erneut bereitstellen, die den Arbeitsablauf enthält, kann die Arbeitsablaufinstanz nicht wiederhergestellt werden.

Wenn Sie eine Arbeitsablaufinstanz wiederherstellen, startet der Data Integration Service neu oder überspringt die unterbrochene Aufgabe basierend auf der Aufgabenwiederherstellungsstrategie. Der Dienst fährt mit der Verarbeitung der nachfolgenden Arbeitsablaufobjekte fort. Wenn eine Arbeitsablaufinstanz im Wiederherstellungsmodus ausgeführt wird, zeigt der Inhaltsbereich auf der Registerkarte "Überwachen" einen blauen Pfeil über den Symbolen für Arbeitsablauf- und Arbeitsablaufobjektstatus an. Der Inhaltsbereich listet jede Arbeitsablaufinstanz und jede Aufgabe einmal auf, auch wenn Sie die Arbeitsablaufinstanz mehrmals wiederherstellen. Beim Erweitern einer neu gestarteten Mapping-Aufgabe listet der Inhaltsbereich mehrere Mapping-Jobs auf, wenn Sie die Arbeitsablaufinstanz mehrmals wiederherstellen.

Eine Arbeitsablaufinstanz kann in einem Wiederherstellungslauf auf denselben Status treffen wie im ursprünglichen Lauf. Trifft die Arbeitsablaufinstanz während eines Wiederherstellungslaufs auf den Status, wird an den Status der Text (Wiederherstellung) angehängt. Der Status "Abgeschlossen" (Wiederherstellung) bedeutet beispielsweise, dass die Arbeitsablaufinstanz während eines Wiederherstellungslaufs abgeschlossen wurde.

Wiederherstellungseigenschaften

Die schreibgeschützten Wiederherstellungseigenschaften werden für jede Arbeitsablaufinstanz angezeigt. Sie konfigurieren die Wiederherstellungseigenschaften für die Arbeitsablaufdefinition im Developer Tool. Sie können die Werte der Eigenschaften für die Arbeitsablaufinstanz nicht ändern.

Die folgende Tabelle beschreibt die schreibgeschützten Wiederherstellungseigenschaften für eine Arbeitsablaufinstanz:

Eigenschaft	Beschreibung
Wiederherstellung aktiviert	Gibt an, dass der Arbeitsablauf für die Wiederherstellung aktiviert ist.
Arbeitsabläufe automatisch wiederherstellen	Gibt an, dass der Datenintegrationsdienstprozess versucht, unterbrochene Arbeitsablaufinstanzen automatisch wiederherzustellen. Die Arbeitsablaufwiederherstellung beginnt nach dem Neustart des Datenintegrationsdienstprozesses.
Wiederherstellungsversuche	Anzahl an Wiederherstellungsversuchen, die für diese Arbeitsablaufinstanz durchgeführt wurden. Wenn eine Arbeitsablaufinstanz die maximale Anzahl an Wiederherstellungsversuchen erreicht hat, kann die Arbeitsablaufinstanz nicht mehr wiederhergestellt werden.

Wiederherstellen eines Arbeitsablaufs

Sie können abgebrochene Arbeitsablaufinstanzen wiederherstellen, die für die Wiederherstellung aktiviert sind.

1. Klicken Sie im Administrator-Tool auf die Registerkarte **Überwachen**.
2. Erweitern Sie im Navigator einen Data Integration Service.
3. Erweitern Sie im Navigator eine Anwendung und wählen Sie **Arbeitsabläufe** aus.
Eine Liste mit Arbeitsablaufinstanzen wird im Inhaltsbereich angezeigt.
4. Wählen Sie im Inhaltsbereich die abgebrochene Arbeitsablaufinstanz, die Sie wiederherstellen möchten.
5. Klicken Sie auf **Aktionen > Ausgewählten Arbeitsablauf wiederherstellen**.
Überwachen Sie den Status der Arbeitsablaufwiederherstellung im Inhaltsbereich.

Arbeitsablaufprotokolle

Der Data Integration Service generiert Protokollereignisse, wenn Sie eine Arbeitsablaufinstanz ausführen. Protokollereignisse beinhalten Informationen über Fehler, Aufgabenverarbeitung, Ausdrucksbewertung in Sequenzflüssen sowie Arbeitsablaufparameter und Variablenwerte.

Wenn eine Arbeitsablaufinstanz eine Mapping-Aufgabe enthält, generiert der Data Integration Service eine separate Protokolldatei für das Mapping. Die Mapping-Protokolldatei beinhaltet alle während der Mapping-Ausführung und aufgetretenen Fehler sowie eine Auslastungszusammenfassung und Umwandlungsstatistik.

Die Arbeitsablauf- und Mapping-Protokolle werden auf der Registerkarte "Überwachen" angezeigt.

Wenn Sie eine unterbrochene Arbeitsablaufinstanz wiederherstellen, hängt der Data Integration Service Protokollereignisse an das vorhandene Arbeitsablaufprotokoll an. Wenn die wiederhergestellte Arbeitsablaufinstanz eine Mapping-Aufgabe enthält, die neu gestartet wurde, hängt der Data Integration Service Protokollereignisse an das vorhandene Mapping-Protokoll an.

Wenn der Arbeitsablauf auf einem Raster läuft, wird die Wiederherstellung der Arbeitsablaufinstanz möglicherweise auf einem anderen Knoten als die ursprüngliche Arbeitsablaufinstanz ausgeführt. Wenn die Wiederherstellung auf einem anderen Knoten läuft und das Protokollverzeichnis kein gemeinsam genutzter Speicherort ist, erstellt der Data Integration Service eine Protokolldatei mit demselben Namen für den aktuellen Knoten.

Format für Arbeitsablauf-Protokolldateien

Die Informationen in der Arbeitsablauf-Protokolldatei hängt von der Sequenz der Ereignisse während der Ausführung der Ablaufinstanz ab. Die Menge von Informationen, die der Data Integration Service an die Protokolle sendet, hängt von der für den Arbeitsablauf festgelegten Tracingebene ab.

Der Data Integration Service aktualisiert die Protokolldatei mit den folgenden Informationen, wenn Sie eine Arbeitsablaufinstanz ausführen:

Arbeitsablauf-Initialisierungsmeldungen

Enthalten Informationen über den Arbeitsablaufnamen und die Instanz-ID, die für die Ausführung der Arbeitsablaufinstanz verwendete Parameterdatei und die anfänglichen Variablenwerte.

Arbeitsablauf-Verarbeitungsmeldungen

Enthält Informationen über die Ergebnisse der Ausdrucksbewertung für bedingte Sequenzflüsse, die ausgeführten Aufgaben und den gewählten ausgehenden Zweig nach der Verwendung eines Gateways, um eine Entscheidung zu treffen.

Aufgaben-Verarbeitungsmeldungen

Enthält Informationen über Eingabedaten, die an die Aufgabe, an das Arbeitselement, das die Aufgabe abgeschlossen hat, übergeben wurden sowie über Ausgabedaten, die von der Aufgabe an den Arbeitsablauf übergeben wurden. Die Informationen hängt vom Typ der Aufgabe ab.

Die Protokolldatei des Arbeitsablaufs zeigt den Zeitstempel, Thread-Namen, Schweregrad, Meldungscode und Meldungstext für jedes Protokollereignis an.

Anzeigen von Protokollen für einen Arbeitsablauf

Sie können das Protokoll für eine Arbeitsablaufinstanz herunterladen, um die Details der Arbeitsablaufinstanz anzuzeigen.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Überwachen**.
2. Erweitern Sie im Navigator einen Data Integration Service.
3. Erweitern Sie im Navigator eine Anwendung und wählen Sie **Arbeitsabläufe** aus.
Eine Liste mit Arbeitsablaufinstanzen wird im Inhaltsbereich angezeigt.
4. Wählen Sie im Inhaltsbereich eine Arbeitsablaufinstanz aus.
5. Klicken Sie auf **Aktionen > Protokolle für gewähltes Objekt anzeigen**.
Es erscheint ein Dialog mit der Option zum Öffnen oder Speichern der Protokolldatei.

Anzeigen von Protokollen für eine Mapping-Ausführung in einem Arbeitsablauf

Sie können das Protokoll für eine Mapping-Ausführung in einen Arbeitsablauf herunterladen, um die Mapping-Details anzuzeigen.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Überwachen**.
2. Erweitern Sie im Navigator einen Data Integration Service.
3. Erweitern Sie im Navigator eine Anwendung und wählen Sie **Arbeitsabläufe** aus.
Eine Liste mit Arbeitsablaufinstanzen wird im Inhaltsbereich angezeigt.
4. Erweitern Sie im Inhaltsbereich eine Arbeitsablaufinstanz.
5. Erweitern Sie eine Mapping-Aufgabe und wählen Sie die Mapping-Ausführung anhand der Aufgabe aus.
6. Klicken Sie auf **Aktionen > Protokolle für gewähltes Objekt anzeigen**.
Es erscheint ein Dialog mit der Option zum Öffnen oder Speichern der Protokolldatei.

Überwachen eines Ordners von Objekten

Sie können die Eigenschaften und die Statistik aller Objekte in einem Ordner im Navigator der Registerkarte **Überwachen** anzeigen. Sie können einen der folgende Ordner auswählen: Jobs, bereitgestellte Mapping-Jobs, logische Datenobjekte, SQL-Datendienste, Web-Dienste und Arbeitsabläufe.

Sie können einen Filter für die Anzahl der Objekte angeben, die im Inhaltsbereich erscheinen. Sie können benutzerdefinierte Filter basierend auf einem Zeitbereich erstellen. Benutzerdefinierte Filter ermöglichen es Ihnen, bestimmte Termine und Zeiten für Job-Startzeiten, -Endzeiten, und verstrichene Zeit auszuwählen. Benutzerdefinierte Filter können Sie auch zum Filtern der Ergebnisse von mehreren Filterkriterien verwenden.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Überwachen**.

2. Wählen Sie den Ordner im Navigator aus.
Der Inhaltsbereich zeigt eine Liste der Objekte im Ordner an.
3. Klicken Sie mit der rechten Maustaste auf die Kopfzeile der Tabelle, um Spalten hinzuzufügen oder zu entfernen.
4. Wählen Sie **Benachrichtigungen empfangen** aus, um neue Jobs, Operationen, Anfragen oder Arbeitsabläufe auf der Registerkarte **Überwachen** dynamisch anzuzeigen.
5. Geben Sie Filterkriterien ein, um die Anzahl der Objekte zu reduzieren, die im Inhaltsbereich erscheinen.
6. Wählen Sie das Objekt im Inhaltsbereich, um Details über das Objekt im Detailbereich anzuzeigen.
Der Detailbereich zeigt im Inhaltsbereich mehr Informationen über das ausgewählte Objekt.
7. Um andere Jobs anzuzeigen, die ungefähr zur gleichen Zeit wie der gewählte Job begonnen wurden, klicken Sie auf **Aktionen > Kontext anzeigen**.
Der ausgewählte Job und andere Jobs, die etwa zur gleichen Zeit begonnen wurden, werden auf der Registerkarte **Kontextansicht** angezeigt. Sie können auch den Kontext von Verbindungen, bereitgestellten Mappings, Anfragen und Arbeitsabläufen anzeigen.
8. Klicken Sie auf die Schaltfläche **Schließen**, um die Registerkarte **Kontextansicht** zu schließen.

Anzeigen des Kontexts eines Objekts

Sie können den Kontext eines Objekts anzeigen, um andere Objekte desselben Typs sichtbar zu machen, die zur selben Zeit gestartet wurden wie das ausgewählte Objekt. Dies kann sinnvoll sein, um ein Problem zu lösen oder ein besseres Verständnis davon zu erhalten, was innerhalb einer bestimmten Zeitperiode passiert ist. Sie können den Kontext von Jobs, bereitgestellten Mappings, Verbindungen, Anfragen und Arbeitsabläufen anzeigen.

Angenommen, Sie stellen fest, dass ein bereitgestelltes Mapping fehlgeschlagen ist. Wenn Sie den Kontext dieses bereitgestellten Mappings anzeigen, erscheint eine ungefilterte Liste der bereitgestellten Mappings in einer eigenen Arbeitsansicht. Dieser Liste können Sie entnehmen, welche bereitgestellten Mappings etwa zur selben Zeit gestartet wurden wie Ihr Mapping. Sie stellen fest, dass auch andere bereitgestellte Mappings fehlgeschlagen sind. Sie können ermitteln, dass der Data Integration Service nicht verfügbar war.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Überwachen**.
2. Im Navigator erweitern Sie einen Data Integration Service und wählen die Kategorie der Objekte aus.
Wählen Sie beispielsweise **Jobs**.
3. Im Inhaltsbereich wählen Sie das Objekt aus, dessen Kontext Sie anzeigen möchten.
Wählen Sie beispielsweise einen Job aus.
4. Klicken Sie auf **Aktionen > Kontext anzeigen**.

Konfigurieren des benutzerdefinierten Filters für Datum und Uhrzeit

Zum Filtern von Ergebnissen können Sie auf der Registerkarte **Überwachen** in den Spalten „Startzeit“ oder „Endezeit“ des Inhaltsbereichs einen benutzerdefinierten Filter anwenden.

1. Wählen Sie als Filteroption "Benutzerdefiniert" für die Spalten Startzeit oder Endezeit.
Der **benutzerdefinierte Filter: Das Dialogfeld Datum und Uhrzeit** erscheint.
2. Geben Sie die Datumsbereich mit den vorgegebenen Datums- und Uhrzeitformaten an.
3. Klicken Sie auf **OK**.

Konfigurieren des benutzerdefinierten Filters für abgelaufene Zeit

Zum Filtern von Ergebnissen können Sie auf der Registerkarte **Überwachen** in der Spalte „Abgelaufene Zeit“ des Inhaltsbereichs einen benutzerdefinierten Filter anwenden.

1. Wählen Sie als Filteroption "Benutzerdefiniert" für die Spalte Abgelaufene Zeit.
Der **benutzerdefinierte Filter: Das Dialogfeld Abgelaufene Zeit** erscheint.
2. Geben Sie den Zeitbereich ein.
3. Klicken Sie auf **OK**.

Konfigurieren des benutzerdefinierten Filters Mehrfachauswahl

Zum Filtern von Ergebnissen können Sie auf der Registerkarte **Überwachen** für die Spalten im Inhaltsbereich mehrere benutzerdefinierte Filter anwenden.

1. Wählen Sie für eine Spalte als Filteroption "Benutzerdefiniert".
Der **benutzerdefinierte Filter: Das Dialogfeld Mehrfachauswahl** erscheint.
2. Wählen Sie einen oder mehrere Filter aus.
3. Klicken Sie auf **OK**.

Überwachen eines Objekts

Sie können ein Objekt auf der Registerkarte **Überwachen** überwachen. Sie können Informationen über das Objekt anzeigen, z. B. Eigenschaften, Laufzeit-Statistiken und Laufzeitberichte.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Überwachen**.
2. Wählen Sie im Navigator das Objekt aus.
Der Inhaltsbereich zeigt mehrere Ansichten an, die verschiedene Informationen zu einem Objekt anzeigen. Die Ansichten unterscheiden sich, je nach Art des Objekts, das im Navigator gewählt wurde.
3. Wählen Sie eine Ansicht aus, um Informationen zum Objekt anzuzeigen.

KAPITEL 12

Domänenberichte

Dieses Kapitel umfasst die folgenden Themen:

- [Domänenberichte - Übersicht, 233](#)
- [Lizenzverwaltungsbericht, 233](#)
- [Web Services-Bericht, 240](#)

Domänenberichte - Übersicht

Aus der Registerkarte Berichte im Administrator Tool heraus können Sie die folgenden Domänenberichte ausführen:

- **Lizenzverwaltungsbericht** Überwachen der Liste der für eine Lizenz erworbenen Softwareoptionen und der Anzahl von Überschreitungen des Nutzungslimits Im Lizenzmanagerbericht werden die Informationen zur Verwendung der Lizenz wie CPU- und Repository-Nutzung und die Knotenkonfigurationsdetails eingeblendet.
- **Web Services Report** Zur Überwachung der auf einem Web Services Hub laufenden Web-Dienste. Der Web-Dienste-Bericht enthält Informationen wie die Anzahl erfolgreicher oder fehlgeschlagener Anfragen und durchschnittliche Dauer des Dienstes Sie können auch Verlaufsstatistiken für einen bestimmten Zeitraum anzeigen.

Hinweis: Läuft der Master-Gateway-Knoten auf einem UNIX-Computer und der UNIX-Computer hat keinen Grafikanzeigeserver, müssen Sie X Virtual Frame Buffer auf dem UNIX-Computer aktivieren, um die Berichtsdiagramme im Lizenzbericht oder im Web-Dienste-Bericht anzuzeigen. Laufen mehrere Gateway-Knoten auf UNIX-Computern, installieren Sie X Virtual Frame Buffer auf jedem UNIX-Computer.

Lizenzverwaltungsbericht

Sie haben die Möglichkeit, die Liste der mit Lizenz erworbenen Software-Optionen zu überwachen und zu überprüfen, wie oft die Benutzungsgrenzen einer Lizenz überschritten wurden. Im Lizenzverwaltungsbericht werden die allgemeinen Eigenschaften, die CPU- und Repository-Nutzung, die Benutzerdetails, die Details der Hardware- und Knotenkonfiguration sowie die für jede Lizenz erworbenen Optionen angezeigt.

Sie können den Lizenzverwaltungsbericht in PDF-Format auf Ihrem lokalen Computer speichern. Außerdem können Sie eine PDF-Berichtsversion per E-Mail versenden.

Führen Sie den Lizenzverwaltungsbericht aus, um folgende Informationen über die Nutzung der Lizenz zu überwachen:

- **Lizenzdetails.** Zeigt die allgemeinen Eigenschaften jeder in der Domäne zugeordneten Lizenz an.
- **CPU-Nutzung** Die Anzahl der für die Ausführung von Anwendungsdiensten in der Domäne verwendeten logischen CPUs wird eingeblendet. Zum Zweck der Lizenzerzwingung werden im Lizenzverwaltungsbericht anstatt der physischen CPUs die logischen CPUs gezählt. Übersteigt die Anzahl der logischen CPUs die Anzahl der autorisierten CPUs, steht im Lizenzverwaltungsbericht, dass die CPU-Grenze der Domäne überschritten wurde.
- **Repository-Nutzung** Zeigt die Anzahl der PowerCenter Repository Services in der Domäne.
- **Benutzerinformationen.** Zeigt Informationen über die Benutzer in der Domäne.
- **Hardwarekonfiguration** Enthält Details zu den in der Domäne eingesetzten Computern.
Knotenkonfiguration. Gibt die Details jedes Knotens in der Domäne an.
- **Lizenzierte Optionen.** Blendet eine Liste der für jede Lizenz erworbenen PowerCenter- und anderen Informatica-Optionen ein.

Lizenzierung

Der Lizenzierungsabschnitt im Lizenzverwaltungsbericht enthält Informationen zu jeder Lizenz in der Domäne.

Die folgende Tabelle beschreibt die Lizenzierungsinformationen im Lizenzverwaltungsbericht:

Eigenschaft	Beschreibung
Name	Name der Lizenz.
Edition	PowerCenter Edition
Version	Version der Informatica-Plattform.
Ablaufdatum	Datum, an dem die Lizenz erlischt
Seriennummer	Seriennummer der Lizenz. Die Seriennummer kennzeichnet den Kunden oder das Projekt. Hat der Kunde mehrere multiple PowerCenter-Installationen, erhält jedes Projekt eine separate Seriennummer. Die Original- und inkrementellen Schlüssel für eine Lizenz haben dieselbe Seriennummer.
Bereitstellungsebene	Ebene der Bereitstellung Die Werte sind Bereitstellung und Produktion.
Betriebssystem/Bitmodus	Betriebssystem und Bitmodus, zu der/dem die Lizenz gehört. Gibt an, ob die Lizenz auf einem 32-Bit- oder einem 64-Bit-Betriebssystem installiert ist.
CPU	Maximale Anzahl der autorisierten logischen CPUs.
Repository	Maximale Anzahl der autorisierten PowerCenter Repositories.
AT-benannte Benutzer	Maximale Anzahl der Benutzer, denen der Lizenzzugriff für die Informatica Analyst Berechtigung zugeordnet wurde.
Produkt-Bitmodus	Bitmodus der installierten Server-Binaries auf dem Server. Die Werte sind 32 Bit oder 64 Bit.

CPU-Zusammenfassung

Im Abschnitt CPU-Zusammenfassung des Lizenzverwaltungsberichts steht die maximale Anzahl der logischen CPUs, die zum Ausführen von Anwendungsdiensten in der Domäne verwendet werden. Anhand der Informationen aus der CPU-Zusammenfassung können Sie erkennen, ob die CPU-Nutzung die Lizenzgrenzwerte überschreitet. Ist die Anzahl der logischen CPUs größer als die per Lizenz zugelassene Gesamtanzahl CPUs, weist der Lizenzverwaltungsbericht darauf hin, dass der CPU-Grenzwert überschritten wurde.

Der Lizenzverwaltungsbericht bestimmt die Anzahl der logischen CPUs basierend auf der Anzahl von Prozessoren, Cores und Threads. Mit folgender Formel können Sie die Anzahl logischer CPUs berechnen:

$N \times C \times T$, wobei

N die Anzahl der Prozessoren angibt.

C die Anzahl der Cores in jedem Prozessor darstellt.

und T die Anzahl der Threads in jedem Knoten beziffert.

Beispiel: Ein Computer enthält 4 Prozessoren. Jeder Prozessor hat 2 Cores. Der Computer enthält 8 (4*2) physische Cores. Hyper-Threading ist aktiviert, wobei auf jeden Core 3 Threads entfallen. Die Anzahl der logischen CPUs beträgt 24 (4*2*3).

Hinweis: Obwohl der Lizenzverwaltungsbericht Threads in die Berechnung der logischen CPUs mit einbezieht, basiert die Einhaltung der Informatica Lizenzvorschriften auf der Anzahl physischer Cores, nicht auf Threads. Um die Lizenzvorschriften einzuhalten, muss die Anzahl der physischen Cores kleiner oder gleich der maximalen Anzahl lizenzierter CPUs sein. Zeigt der Lizenzverwaltungsbericht, dass Sie die Lizenzgrenze zwar überschritten haben, die Anzahl der physischen Cores jedoch kleiner oder gleich der maximalen Anzahl lizenzierter CPUs ist, können Sie die Meldung ignorieren. Sollten Sie Probleme mit der Einhaltung der Lizenzvorschriften haben, setzen Sie sich bitte mit Ihrem Informatica-Kontoverwalter in Verbindung.

Die folgende Tabelle beschreibt die zusammenfassenden Informationen über die CPUs im Lizenzverwaltungsbericht.

Eigenschaft	Beschreibung
Domäne	Name der Domäne, auf der der Bericht ausgeführt wird.
Aktuelle Nutzung	Maximale Anzahl der logischen CPUs, die zum Datum der Berichtsausführung gleichzeitig verwendet werden.
Spitzenauslastung	Maximale Anzahl der logischen CPUs, die in den letzten 12 Monaten gleichzeitig genutzt wurden.
Spitzenauslastungsdatum	Datum der gleichzeitigen Nutzung der maximalen Anzahl logischer CPUs in den letzten 12 Monaten.
Tage Überschreitung Lizenzlimit	Anzahl der Tage, an denen die CPU-Nutzung die Lizenzgrenzen überschritten hat. Überschreitet die Anzahl gleichzeitig genutzter logischer CPUs die zulässige Anzahl CPUs, bedeutet dies, dass die Domäne die CPU-Lizenzgrenze überschreitet.

CPU-Detail

Im Abschnitt CPU-Details des Lizenzverwaltungsberichts erhalten Sie Informationen zur Nutzung der CPU für jeden Host in der Domäne. Der Abschnitt CPU-Details zeigt die maximale Anzahl der logischen CPUs, die während eines ausgewählten Zeitraums täglich verwendet werden.

Der Bericht zählt die Anzahl der logische CPUs auf jedem Host, auf dem Anwendungsdienste in der Domäne laufen. Im Bericht sind die Gesamtzahlen der logischen CPUs nach Knoten aufgeführt.

Die folgende Tabelle beschreibt die CPU-Detailinformationen im Lizenzverwaltungsbericht:

Eigenschaft	Beschreibung
Hostname	Hostname des Computers.
Aktuelle Nutzung	Maximale Anzahl der logischen CPUs, die der Host am Tage der Berichtsausführung gleichzeitig nutzt.
Spitzenauslastung	Maximale Anzahl der logischen CPUs, die der Host in den letzten 12 Monaten gleichzeitig genutzt hat.
Spitzenauslastungsdatum	Datum innerhalb der letzten 12 Monate, an dem der Host die maximale Anzahl logischer CPUs gleichzeitig genutzt hat.
Zugewiesene Lizenzen	Name aller Lizenzen, die auf dem Knoten laufenden Diensten zugeordnet sind.

Repository-Zusammenfassung

Der Abschnitt Repository-Zusammenfassung des Lizenzverwaltungsberichts enthält Informationen zur Verwendung des Repositories für die Domäne. Verwenden Sie die Repository-Zusammenfassungsinformationen, um festzulegen, wann die Repository-Verwendung die Lizenzbeschränkungen übersteigt.

Die nachstehende Tabelle beschreibt die Repository-Zusammenfassungsinformationen im Lizenzverwaltungsbericht:

Eigenschaft	Beschreibung
Aktuelle Verwendung	Maximale Anzahl von aktuell in der Domäne verwendeten Repositories zum Zeitpunkt der Berichtsausführung.
Spitzenauslastung	Maximale Anzahl von gleichzeitig in der Domäne verwendeten Repositories während der letzten 12 Monate.
Spitzenauslastungsdatum	Datum innerhalb der letzten 12 Monate, an dem gleichzeitig eine maximale Anzahl von Repositories ausgeführt wurde.
Tage haben Lizenzlimit überschritten	Anzahl von Tagen, die die Repository-Verwendung das Limit bereits überschreitet.

Benutzerzusammenfassung

Der Abschnitt Benutzerzusammenfassung des Lizenzverwaltungsberichts enthält Informationen über die Benutzer des Analyst Tools in der Domäne.

Die nachstehende Tabelle beschreibt die Benutzerzusammenfassungen im Lizenzverwaltungsbericht:

Eigenschaft	Beschreibung
Benutzertyp	Typ des Benutzers in der Domäne.
Aktuell benannter Benutzer	Maximale Anzahl der Benutzer, denen die Informatica Analyst Berechtigung des Lizenzzugriffs am Tag der Berichtsausführung zugewiesen wurde.
Höchste Anzahl benannter Benutzer	Maximale Anzahl der Benutzer, denen die Informatica Analyst Berechtigung des Lizenzzugriffs in den letzten 12 Monaten zugewiesen wurde.
Höchstwert für benannte Benutzer - Datum	Datum während der letzten 12 Monate, an dem einer maximalen Anzahl gleichzeitiger Nutzer die Informatica Analyst Berechtigung des Lizenzzugriffs zugewiesen wurde.

Benutzerdetail

Der Bereich "Benutzerdetail" im Lizenzverwaltungsbericht liefert Details zu den einzelnen Benutzern des Analyst Tools in der Domäne.

Die folgende Tabelle beschreibt die Benutzerdetails im Lizenzverwaltungsbericht:

Eigenschaft	Beschreibung
Benutzertyp	Typ des Benutzers in der Domäne.
Benutzername	Benutzername
Tage seit der Anmeldung	Anzahl der Tage, die der Benutzer während der letzten 12 Monate beim Analyst Tool angemeldet war und Profiling durchgeführt hat
Höchstwert für eindeutige IP-Adressen an einem Tag	Anzahl der Computer, bei denen der Benutzer an einem einzelnen Tag während der letzten 12 Monate angemeldet war und Profiling durchgeführt hat.
Durchschnittswert für eindeutige IP-Adressen	Tagesdurchschnitt der Computer, bei denen der Benutzer an einem während der letzten 12 Monate angemeldet war und Profiling ausführen hat.
Höchstwert für IP-Adressdatum	Datum, wann der Benutzer an einem einzelnen Tag während der letzten 12 Monate bei der Höchstanzahl der Computer angemeldet war und Profiling durchgeführt hat.
Höchstwert für tägliche Sitzungen	Maximale Häufigkeit an einem einzigen Tag während der letzten 12 Monate, die der Benutzer bei einem Analyst Tool angemeldet war und Profiling durchgeführt hat.
Durchschnittswert für tägliche Sitzungen	Durchschnittliche Häufigkeit pro Tag während der letzten 12 Monate, die der Benutzer bei einem Analyst Tool angemeldet war und Profiling durchgeführt hat.
Höchstwert für Sitzungsdatum	Datum in den letzten 12 Monaten, wann der Benutzer die meisten täglichen Sitzungen im Analyst Tool hatte.

Hardwarekonfiguration

Der Abschnitt Hardwarekonfiguration des Lizenzverwaltungsberichts enthält Details über die in der Domäne verwendeten Maschinen.

Die nachstehende Tabelle beschreibt die Hardwarekonfigurationsinformationen im Lizenzverwaltungsbericht:

Eigenschaft	Beschreibung
Hostname	Hostname des Computers.
Logische CPUs	Anzahl der logischen CPUs, die zur Ausführung von Anwendungsdiensten in der Domäne verwendet werden.
Sockets	Anzahl der Sockets auf dem Computer.
Benutzte Kerne	Anzahl der Kerne auf dem Computer.
Kerne pro Socket	Anzahl der Kerne für jedes Socket auf dem Computer.
CPU-Modell	Modell der CPU.
Hyperthreading aktiviert	Gibt an, ob die Hyperthread-Funktion aktiv ist.
Virtuelle Maschine	Gibt an, ob der Computer eine virtuelle Maschine ist.

Knotenkonfiguration

Der Bereich "Knotenkonfiguration" im Lizenzverwaltungsbericht liefert Details zu den einzelnen Knoten in der Domäne.

Die folgende Tabelle beschreibt die Knotenkonfigurationsinformationen im Lizenzverwaltungsbericht:

Eigenschaft	Beschreibung
Knotenname	Name der Knoten, die einem Computer für eine Lizenz zugeordnet sind.
Hostname	Hostname des Computers.
IP-Adresse	IP-Adresse des Knotens.
Betriebssystem	Betriebssystem des Computers, auf dem der Knoten läuft.
Status	Status des Knotens.
Gateway	Gibt an, ob der Knoten ein Gateway ist.
Diensttyp	Typ des Anwendungsdienstes, der auf dem Knoten laufen soll.
Dienstname	Name des Anwendungsdienstes, der auf dem Knoten laufen soll.
Dienststatus	Status des Anwendungsdienstes.
Zugewiesener Dienst	Dem Anwendungsdienst zugeordnete Lizenz.

Lizenzierte Optionen

Der Abschnitt Lizenzierte Optionen des Lizenzverwaltungsberichts enthält Details über jede Option für jede Lizenz, die einer Domäne zugewiesen ist.

Die nachstehende Tabelle beschreibt die Lizenzoptionsinformationen im Lizenzverwaltungsbericht:

Eigenschaft	Beschreibung
Lizenzname	Name der Lizenz.
Beschreibung	Name der Lizenzoption.
Status	Status der Lizenzoption.
Ausstellungsdatum	Datum, an dem die Lizenzoption ausgestellt wurde.
Ablaufdatum	Datum, an dem die Lizenzoption abläuft.

Lizenzverwaltungsbericht ausführen

Führen Sie den Lizenzverwaltungsbericht von der Registerkarte **Berichte** im Administrator Tool aus.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Berichte**.
2. Klicken Sie auf die Ansicht **Lizenzverwaltungsbericht**.
Der Lizenzverwaltungsbericht erscheint.
3. Klicken Sie auf **Speichern**, um den Lizenzverwaltungsbericht als PDF-Datei zu speichern.
Wenn ein Lizenzverwaltungsbericht Multibyte-Zeichen enthält, müssen Sie den Service Manager so konfigurieren, dass er eine Unicode-Schriftart verwendet.
4. Klicken Sie auf **E-Mail**, um eine Kopie des Lizenzverwaltungsberichts in einer E-Mail zu versenden.
Die Seite **Lizenzverwaltungsbericht senden** erscheint.

Konfigurieren der Unicode-Schriftart für den Bericht

Bevor Sie einen Lizenzverwaltungsbericht speichern können, der Multibyte-Zeichen enthält, müssen Sie den Dienstmanager für die Nutzung einer Unicode-Schriftart beim Generieren der PDF-Datei konfigurieren.

1. Installieren Sie eine Unicode-Schriftart auf dem Master-Gateway-Knoten.
2. Verwenden Sie einen Texteditor, um eine Datei mit dem Namen AcUtil.properties zu erstellen.
3. Fügen Sie der Datei die folgenden Eigenschaften hinzu:

```
PDF.Font.Default=Unicode_font_name  
PDF.Font.MultibyteList=Unicode_font_name
```

Unicode_font_name ist der Name der auf dem Master-Gateway-Knoten installierten Unicode-Schriftart.

Möglicherweise müssen Sie auch die folgende Eigenschaft hinzufügen, wenn die Schriftartdatei im Gebietsschema nicht verfügbar ist:

```
Unicode_font_name_path=Unicode_font_file_location
```

Beispiel:

```
PDF.Font.Default=Arial Unicode MS  
PDF.Font.MultibyteList=Arial Unicode MS  
Arial Unicode MS_path=/usr/lib/X11/fonts/TrueType
```

4. Speichern Sie die Datei AcUtil.properties an folgendem Speicherort:
InformaticaInstallationDir\services\AdministratorConsole\administrator
5. Benutzen Sie einen Texteditor, um die Datei licenseUtility.css am folgenden Speicherort zu öffnen:
InformaticaInstallationDir\services\AdministratorConsole\administrator\css

6. Hängen Sie den Namen der Unicode-Schriftart an den Wert jeder Eigenschaft der Schriftartenfamilie an.
Beispiel:
`Schriftartenfamilie: Arial Unicode MS, Verdana, Arial, Helvetica, sans-serif;`
7. Starten Sie die Informatica-Dienste auf jedem Knoten der Domäne neu.

Lizenzverwaltungsbericht in einer E-Mail verschicken

Sie müssen die SMTP-Einstellungen für die Domäne konfigurieren, bevor Sie den Lizenzverwaltungsbericht in einer E-Mail verschicken können.

Der Domänen-Administrator kann den Lizenzverwaltungsbericht von der Lizenzverwaltungsbericht-Seite im Administrator Tool in einer E-Mail verschicken.

1. Geben Sie die folgenden Informationen ein:

Eigenschaft	Beschreibung
E-Mail-Empfänger	E-Mail-Adresse, an die Sie den Lizenzverwaltungsbericht senden.
Betreff	Betreff der E-Mail.
Kundenname	Name der Organisation, die die Lizenz erworben hat.
Anforderungs-ID	Nummer der Anfrage, die das Projekt identifiziert, für das die Lizenz erworben wurde.
Kontakt: Name	Name der Kontaktperson in der Organisation.
Kontakt: Telefonnummer	Telefonnummer der Kontaktperson.
Kontakt: E-Mail	E-Mail-Adresse der Kontaktperson beim Kunden vor Ort.

2. Klicken Sie auf OK.

Das Administrator Tool verschickt den Lizenzverwaltungsbericht in einer E-Mail.

Web Services-Bericht

Um die Performance von Web-Diensten zu analysieren, die auf einem Web Services Hub ausgeführt werden, können Sie einen Bericht für den Web Services Hub oder einen Web-Dienst, der auf dem Web Services Hub ausgeführt wird, erstellen.

Der Web-Dienste-Bericht enthält Laufzeit- und Historieninformationen zu denjenigen Web-Dienst-Anfragen, die von diesem Web Services Hub behandelt werden. Der Bericht zeigt die gesammelten Informationen für alle Web-Dienste in diesem Web Services Hub an und Informationen für alle Web-Dienste, die auf diesem Web Services Hub ausgeführt werden. Der Web-Dienst-Bericht enthält auch historische Informationen.

Über den Web-Dienste-Bericht

Sie können den Web-Dienste-Bericht für ein gewähltes Zeitintervall ausführen. Der Web-Dienste-Hub sammelt Informationen zu den Aktivitäten des Web-Dienstes und speichert diese 24 Stunden zur Verwendung im Web-Dienste-Bericht. Ferner schreibt er die Informationen in einen Historiendatei.

Zeitintervall

Standardmäßig zeigt der Web-Dienste-Bericht die Aktivitätsinformationen in einem Fünf-Minuten-Intervall an. Sie können eines der folgenden Zeitintervalle wählen, in denen die Aktivitätsinformationen für einen Web-Dienst oder Web Service Hub angezeigt werden sollen:

- 5 Sekunden
- 1 Minute
- 5 Minuten
- 1 Stunde
- 24 Stunden

Der Web-Dienste-Bericht zeigt die Aktivitätsinformationen für das gewählte Zeitintervall an, das vor der Ausführung des Berichts endet. Zum Beispiel: Wenn Sie den Web-Dienste-Bericht um 8:05 Uhr für ein Zeitintervall von einer Stunde ausführen, so zeigt der Web-Dienste-Bericht die Aktivität des Web Service Hub für die Zeit von 7:05 Uhr bis 8:05 Uhr an.

Zwischenspeichern

Der Web-Dienst-Hub speichert die Aktivitätsdaten im Zeitraum von 24 Stunden. Der Cache wird jedes Mal neu initialisiert, wenn der Web-Dienst-Hub neu gestartet wird. Der Web-Dienstbericht enthält die statistischen Daten des Caches für das Zeitintervall, in dem der Bericht ausgeführt wurde.

Historiendatei

Der Web Services Hub schreibt die zwischengespeicherten Aktivitätsdaten in eine Historiendatei. Der Web Services Hub speichert die Daten in der Historiendatei für die Anzahl von Tagen, die Sie in der Eigenschaft MaxStatsHistory des Web Services Hub angegeben haben. Zum Beispiel: Wenn der Wert in der Eigenschaft MaxStatsHistory 5 beträgt, bewahrt der Web Services Hub die Daten fünf Tage lang in der Historiendatei auf.

Inhalte des Web-Dienste-Berichts

Die Ansicht „Web Services Report“ enthält Informationen über die Webdienste in einer Domäne. Wenn Sie einen Webdienst-Hub im Navigator auswählen, können Sie die folgenden Informationen über die darin enthaltenen Webdienste anzeigen:

- **Eigenschaftenansicht:** Zeigt Allgemeine Eigenschaften, Zusammenfassung für Webdienst-Hub und historische Statistiken für den Webdienst-Hub an.
- **Ansicht „Webdienste“:** Enthält eine Liste der Webdienste im Webdienst-Hub. Wenn Sie einen Webdienst auswählen, können Sie Eigenschaften, Top-IP-Adressen und Historische Statistik für den Webdienst anzeigen.

Allgemeine Eigenschaften und Zusammenfassung für den Web Services Hub

Zum Einblenden der allgemeinen Eigenschaften und der Zusammenfassung für den Web Services Hub wählen Sie bitte die Ansicht Eigenschaften in der Inhaltsübersicht.

In der folgenden Tabelle werden die allgemeinen Eigenschaften beschrieben:

Eigenschaft	Beschreibung
Name	Name des Web Services Hub
Beschreibung	Kurzbezeichnung des Web Services Hub
Diensttyp	Typ des Dienstes. Bei einem Web Services Hub ist der Diensttyp ServiceWSHubService.

Die folgende Tabelle beschreibt die zusammengefassten Eigenschaften des Web Services Hub:

Eigenschaft	Beschreibung
Anzahl der erfolgreichen Nachrichten	Anzahl der Anfragen, die der Web Services Hub erfolgreich bearbeitet hat
Anzahl der Fehler-Antworten	Anzahl der von Web-Diensten im Web Services Hub generierten Fehlerantworten. Die Fehlerantworten können durch einen beliebigen Fehler bedingt sein:
Nachrichten gesamt	Gesamtanzahl der vom Web Services Hub erhaltenen Anfragen
Neustart-Zeit des letzten Servers	Datum und Uhrzeit des letzten Starts des Web Services Hub
Durchschnittliche Anzahl von Dienstpartitionen	Durchschnittliche Anzahl der Partitionen, die für alle Web-Dienste im Web Services Hub zugewiesen wurden
% verwendeter Partitionen	Prozentuale Angabe der Web-Dienst-Partitionen, die für alle Web-Dienste im Web Services Hub benutzt werden.
Durchschnittliche Anzahl der Ausführungsinstanzen	Durchschnittliche Anzahl der für alle Web-Dienste ausgeführten Instanzen im Web Services Hub.

Historienstatistik-Tabelle für Web Services

Um die Historienstatistik für die Web-Dienste im Web Services Hub anzuzeigen, wählen Sie die Ansicht Eigenschaften im Inhaltsbereich. Der Detailbereich zeigt die Daten aus der Historiendatei des Web Services Hub für das Datum an, das Sie angegeben haben.

Die folgende Tabelle beschreibt die Historienstatistik:

Eigenschaft	Beschreibung
Uhrzeit	Zeitpunkt des Ereignisses
Web-Dienst	Name des Web-Dienstes, für den die Informationen angezeigt werden. Wenn Sie den Namen eines Web-Dienstes anklicken, zeigt der Web-Dienst-Bericht das Fenster Dienststatistiken an.
Erfolgreiche Anfragen	Anzahl der Anfragen, die erfolgreich vom Web-Dienst verarbeitet wurden.
Antwort vom Typ 'Fault'	Anzahl der fehlerhaften Anfragen, die vom Web-Dienst verarbeitet wurden.
Dienstzeit (Durchschnitt)	Durchschnittliche Zeit, die zur Verarbeitung einer Dienstanfrage vom Web-Dienst erforderlich war.
Maximale Dienstzeit	Maximale Zeit, die zur Verarbeitung einer Dienstanfrage vom Web-Dienst erforderlich war.
Minimale Dienstzeit	Minimale Zeit, die zur Verarbeitung einer Dienstanfrage vom Web-Dienst erforderlich war.
DTM-Zeit (Durchschnitt)	Durchschnittliche Anzahl von Sekunden, die der PowerCenter Integration Service benötigte, um eine Anfrage vom Web Services Hub zu verarbeiten.
Dienstpartitionen (Durchschnitt)	Durchschnittliche Anzahl der Sitzungspartitionen, die dem Web-Dienst zugeteilt wurden.
% verwendete Partitionen	Prozentualer Anteil der vom Web-Dienst benutzten Partitionen.
Ausführungsinstanzen (Durchschnitt)	Durchschnittliche Anzahl der für den Web-Dienst ausgeführten Instanzen.

Laufzeitstatistiken für Web Services

Um die Laufzeitstatistiken für die Web-Dienste im Web Services Hub anzuzeigen, wählen Sie die Ansicht Web-Dienste im Inhaltsbereich. Die Ansicht Web-Dienste für die Statistiken für jeden Web-Dienst auf.

Der Bericht enthält folgende Informationen für jeden Web-Dienst innerhalb des gewählten Zeitintervalls:

Eigenschaft	Beschreibung
Dienstname	Name des Web-Dienstes, für den die Informationen angezeigt werden.
Erfolgreiche Anfragen	Anzahl der Anfragen, die der Web-Dienst erhalten hat und die der Web Services Hub erfolgreich verarbeiten konnte.
Antwort vom Typ 'Fault'	Anzahl der fehlerhaften Antworten, die von den Web-Diensten im Web Services Hub generiert wurden.

Eigenschaft	Beschreibung
Dienstzeit (Durchschnitt)	Durchschnittliche Zeit, die zur Verarbeitung einer Dienstanfrage vom Web-Dienst erforderlich war.
Dienstpartitionen (Durchschnitt)	Durchschnittliche Anzahl der Sitzungspartitionen, die dem Web-Dienst zugeteilt wurden.
Ausführungsinstanzen (Durchschnitt)	Durchschnittliche Anzahl von Instanzen des Web-Dienstes, die während des Intervalls ausgeführt wurden.

Web-Dienst-Eigenschaften

Um die Eigenschaften eines Web-Dienstes anzuzeigen, wählen Sie den Web-Dienst in der Ansicht Web-Dienste des Inhaltsbereichs aus. Im Detailsbereich zeigt die Ansicht Eigenschaften die Eigenschaften für den aktuell gewählten Web-Dienst an.

Der Bericht stellt die folgenden Informationen zum ausgewählten Web-Dienst bereit:

Eigenschaft	Beschreibung
Anzahl von erfolgreichen Anfragen	Anzahl der Anfragen, die der Web-Dienst erhalten hat und die der Web Services Hub erfolgreich verarbeiten konnte.
Anzahl von Antworten vom Typ 'Fault'	Anzahl der fehlerhaften Antworten, die von den Web-Diensten im Web Services Hub generiert wurden.
Nachrichten gesamt	Anzahl der gesamten Anfragen, die der Web Services Hub erhalten hat.
Letzter Serverneustart - Uhrzeit	Datum und Uhrzeit des letzten Starts des Web Services Hub.
Letzte Dienstzeit	Anzahl in Sekunden, die die letzte Dienstanfrage für die Verarbeitung benötigte
Durchschnittliche Dienstzeit	Durchschnittliche Zeit, die zur Verarbeitung einer Dienstanfrage vom Web-Dienst erforderlich war.
Durchschnittliche Anzahl von Dienstpartitionen	Durchschnittliche Anzahl der Sitzungspartitionen, die dem Web-Dienst zugeteilt wurden.
Durchschnittliche Anzahl von Ausführungsinstanzen	Durchschnittliche Anzahl von Instanzen des Web-Dienstes, die während des Intervalls ausgeführt wurden.

Top IP-Adressen des Web-Dienstes

Um die wichtigsten IP-Adressen für einen Web-Dienst anzuzeigen, wählen Sie die Ansicht Web-Dienste im Inhaltsbereich und wählen im Detailbereich die Ansicht "Top IP-Adressen". In dieser Ansicht werden die am

häufigsten aktiven IP-Adressen für den Web-Dienst angezeigt und in der Reihenfolge der am längsten bis zu den kürzesten beanspruchten Dienstzeiten aufgelistet.

Der Bericht stellt folgende Information für jede der am meisten aktiven IP-Adressen bereit:

Eigenschaft	Beschreibung
Top 10 Client-IP-Adressen	Die Liste der Client-IP-Adressen und die längste Zeit, die ein Web-Dienst benötigt hat, um die Anfrage eines Client zu verarbeiten. Die Client-IP-Adressen werden in der Reihenfolge von längster bis kürzester Dienstzeit aufgeführt. Verwenden Sie den Link <i>Hier klicken</i> , um die Liste der IP-Adressen und Dienstzeiten anzuzeigen.

Historienstatistik-Tabelle für Web-Dienst

Um die Tabelle der Historienstatistik für einen Web-Dienst anzuzeigen, wählen Sie in der Ansicht Web-Dienst im Inhaltsbereich einen Web-Dienst aus und aktivieren im Detailbereich die Tabellenansicht. Der Detailsbereich zeigt eine Tabelle der Historienstatistik für den Web-Dienst an.

Die Tabelle stellt die folgenden Informationen zum ausgewählten Web-Dienst bereit.

Eigenschaft	Beschreibung
Uhrzeit	Zeitpunkt des Ereignisses
Web-Dienst	Name des Web-Dienstes, für den die Informationen angezeigt werden.
Erfolgreiche Anfragen	Anzahl der Anfragen, die erfolgreich vom Web-Dienst verarbeitet wurden.
Antwort vom Typ 'Fault'	Anzahl der Anfragen, die vom Web-Dienst empfangen, aber nicht erfolgreich verarbeitet wurden, sondern Fehlerantworten generierten.
Dienstzeit (Durchschnitt)	Durchschnittliche Zeit, die zur Verarbeitung einer Dienstanfrage vom Web-Dienst erforderlich war.
Min. Dienstzeit	Minimale Zeit, die zur Verarbeitung einer Dienstanfrage vom Web-Dienst erforderlich war.
Max. Dienstzeit	Maximale Zeit, die zur Verarbeitung einer Dienstanfrage vom Web-Dienst erforderlich war.
DTM-Zeit (Durchschnitt)	Durchschnittliche Zeit, die der PowerCenter Integration Service benötigte, um eine Anfrage vom Web Services Hub zu verarbeiten.
Dienstpartitionen (Durchschnitt)	Durchschnittliche Anzahl der Sitzungspartitionen, die dem Web-Dienst zugeteilt wurden.
% verwendete Partitionen	Prozentualer Anteil der vom Web-Dienst benutzten Partitionen.
Ausführungsinstanzen (Durchschnitt)	Durchschnittliche Anzahl der für den Web-Dienst ausgeführten Instanzen.

Ausführen des Web Services Report

Führen Sie den Web-Dienst-Bericht von der Registerkarte Berichte im Administrator Tool aus.

Bevor Sie den Web-Dienst-Bericht für ein Web-Dienste-Hub ausführen, stellen Sie sicher, dass das Web-Dienste-Hub aktiviert ist. Bevor Sie den Web-Dienst-Bericht nicht für ein deaktiviertes Web-Dienste-Hub ausführen.

1. Klicken Sie im Administrator Tool auf die Registerkarte Sicherheit.
2. Klicken Sie auf "Web-Dienste".
3. Im Navigator wählen Sie das Web-Dienste-Hub, für das Sie den Bericht auszuführen möchten.
Im Inhaltsbereich zeigt die Ansicht Eigenschaften die Eigenschaften für das aktuell gewählte Web-Dienste-Hub an. Die Detailansicht zeigt historische Statistiken zu den Diensten im Web-Dienste-Hub.
4. Um ein Datum für die historischen Statistiken anzugeben, klicken Sie auf das Datumsfilter-Symbol im Detailbereich und wählen das Datum aus.
5. Um die Eigenschaften eines Web-Dienstes anzuzeigen, wählen Sie den Web-Dienst in der Ansicht Web-Dienste des Inhaltsbereichs aus.
Die Ansicht Web-Dienste zeigt Übersichtsstatistiken zu den einzelnen Diensten im Web-Dienste-Hub.
6. Um weitere Informationen zu einem Dienst anzuzeigen, wählen Sie den Dienst aus der Liste.
Im Detailbereich zeigt die Ansicht Eigenschaften die Eigenschaften des Dienstes an.
7. Zur Anzeige der wichtigsten IP-Adressen für den Dienst wählen Sie im Detailbereich die Ansicht "Top IP-Adressen".
8. Zur Anzeige der Tabellenattribute für den Dienst wählen Sie im Detailbereich die Ansicht "Tabelle".

Web Services Report für einen sicheren Web Services Hub ausführen

Um einen Web-Dienste-Hub auf HTTPS auszuführen, müssen Sie über eine SSL-Zertifikatsdatei für die Authentifizierung der Nachrichtenübertragungen verfügen. Wenn Sie einen Web-Dienste-Hub erstellen, der auf HTTPS ausgeführt werden soll, müssen Sie den Speicherort der Schlüsselspeicherdatei angeben, die das Zertifikat für den Web-Dienste-Hub enthält. Um die den Web-Dienste-Bericht im Administrator Tool für einen sicheren Web-Dienste-Hub ausführen zu können, müssen Sie das SSL-Zertifikat in das Java-Zertifikat importieren. Die Java-Zertifikatsdatei hat den Namen *cacerts* und befindet sich im Verzeichnis */lib/security* unter dem Java-Verzeichnis. Das Administrator Tool verwendet die *cacerts*-Zertifikatsdatei, um festzustellen, ob ein SSL-Zertifikat vertrauenswürdig ist.

In einer Domäne mit mehreren Knoten beeinflusst der Knoten, auf dem Sie das SSL-Zertifikat generieren, wie Sie auf den Web-Dienste-Bericht für einen sicheren Web-Dienste-Hub zugreifen können.

Beachten Sie die folgenden Regeln und Richtlinien bei der Ausführung des Web-Dienste-Berichts für einen sicheren Web-Dienste-Hub in einer Domäne mit mehreren Knoten:

- Generieren Sie für jeden sicheren Web-Dienste-Hub, der in einer Domäne läuft, ein SSL-Zertifikat und importieren Sie es in eine Java-Zertifikatsdatei.
- Das Administrator Tool sucht nach SSL-Zertifikaten in der Zertifikatsdatei eines Gateway-Knotens. Das SSL-Zertifikat für einen Web-Dienste-Hub, der auf einem Worker-Knoten läuft, muss auf einem Gateway-Knoten erzeugt werden und in die Zertifikatsdatei mit dem gleichen Gateway-Knoten importiert werden.
- Zur Anzeige des Web-Dienste-Berichts für einen sicheren Web-Dienste-Hub melden Sie sich beim Administrator Tool von dem Gateway-Knoten aus an, auf dem sich die Zertifikatsdatei mit dem SSL-Zertifikat des Web-Dienste-Hubs befindet, für den Sie Berichte anzeigen möchten.
- Wenn ein sicherer Web-Dienste-Hub auf einem Worker-Knoten läuft, muss das SSL-Zertifikat erzeugt und in die Zertifikatsdatei des Gateway-Knotens importiert werden. Wenn ein sicherer Web-Dienste-Hub auf einem Gateway- und einem Worker-Knoten läuft, muss das SSL-Zertifikat erzeugt und in die

Zertifikatsdatei des Gateway-Knotens importiert werden. Um Berichte für den sicheren Web-Dienste-Hub anzuzeigen, melden Sie sich beim Administrator Tool vom Gateway-Knoten aus an.

- Wenn die Domäne über zwei Gateway-Knoten verfügt und einen sicheren Web-Dienste-Hub auf jedem der Gateway-Knoten läuft, hängt der Zugriff auf die Web-Dienste-Bereich davon ab, wo sich das SSL-Zertifikat befindet.

Zum Beispiel: Auf dem Gateway-Knoten GWN01 läuft der Web-Dienste-Hub WSH01 und auf dem Gateway-Knoten GWN02 läuft der Web-Dienste-Hub WSH02. Sie können die Berichte für die Web-Dienste-Hubs abhängig vom Standort der SSL-Zertifikate anzeigen:

- Wenn das SSL-Zertifikat für WSH01 in der Zertifikatsdatei von GWN01, aber nicht von GWN02, steht, können Sie die Berichte für WSH01 anzeigen, wenn Sie sich über GWN01 beim Administrator Tool anmelden. Sie können die Berichte für WSH01 nicht anzeigen, wenn Sie sich über GWN02 beim Administrator Tool anmelden. Wenn GWN01 ausfällt, können Sie keine Berichte für WSH01 anzeigen.
 - Wenn das SSL-Zertifikat für WSH01 in den Zertifikatsdatei von GWN01 und GWN02 steht, können Sie die Berichte für WSH01 anzeigen, wenn Sie sich über GWN01 oder GWN02 beim Administrator Tool anmelden. Wenn GWN01 fehlschlägt, können Sie die Berichte für WSH01 anzeigen, wenn Sie sich über GWN02 beim Administrator Tool anmelden.
- Um ein erfolgreiches Failover zu gewährleisten, wenn ein Gateway-Knoten ausfällt, erzeugen und importieren Sie die SSL-Zertifikate von allen Web-Dienste-Hubs in der Domäne in die Zertifikatsdateien aller Gateway-Knoten in der Domäne.

KAPITEL 13

Knotendiagnostiken

Dieses Kapitel umfasst die folgenden Themen:

- [Knotendiagnostiken - Übersicht, 248](#)
- [Anmeldung beim Informatica MySupport-Portal, 249](#)
- [Generieren der Knotendiagnostik, 250](#)
- [Knotendiagnostiken herunterladen, 251](#)
- [Knotendiagnostiken hochladen, 251](#)
- [Knotendiagnostik analysieren, 252](#)

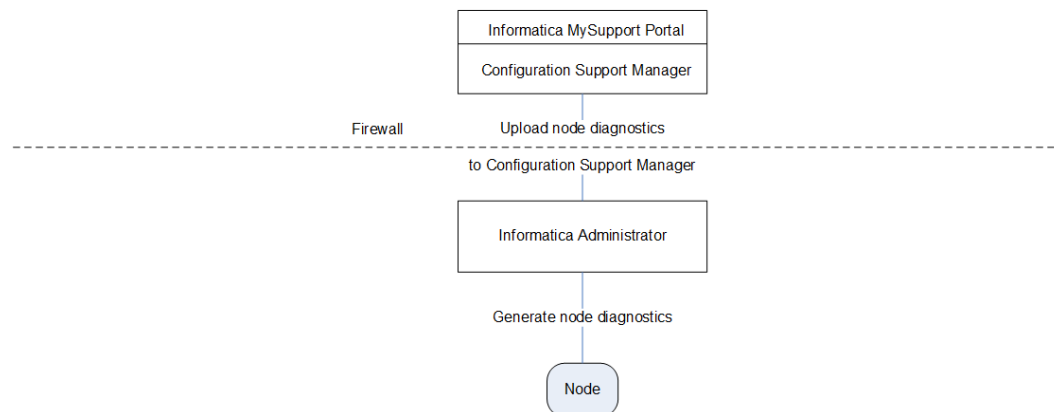
Knotendiagnostiken - Übersicht

Beim Configuration Support Manager handelt es sich um eine webbasierte Anwendung, mit der Sie Informatica-Updates verfolgen und Probleme in Ihrer Umgebung diagnostizieren können.

Sie können umfassende Informationen über Ihre technische Umgebung einsehen und Probleme diagnostizieren, bevor sie kritisch werden.

Generieren Sie aus dem Informatica Administrator heraus eine Knotendiagnose und laden Sie sie im Informatica MySupport-Portal in den Configuration Support Manager. Überprüfen Sie dann im Configuration Support Manager die Knotendiagnose gegen Geschäftsregeln und Empfehlungen.

Die folgende Abbildung zeigt den Arbeitsablauf zum Generieren und Hochladen von Knotendiagnosen:



Führen Sie die folgenden Schritte aus, um die Diagnose zu erstellen und hochzuladen:

1. Melden Sie sich beim Informatica MySupport-Portal an.

2. Generieren Sie eine Knotendiagnose. Der Dienstmanager analysiert die Dienste des Knotens und Knoten erzeugt Knotendiagnosen, die Informationen wie Details zu Betriebssystem, CPU, Datenbank und Patches enthalten.
3. Wahlweise können Sie die Knotendiagnose auf Ihre lokale Festplatte herunterladen.
4. Laden Sie Knotendiagnose in den Configuration Support Manager (ein Web-Anwendung zur Diagnose außerhalb der Firewall). Der Configuration Support Manager ist ein Bestandteil des Informatica MySupport-Portals. Der Dienstmanager stellt die Verbindung zum Configuration Support Manager über das HTTPS-Protokoll her und lädt die Knotendiagnose hoch.
5. Überprüfen Sie die Knotendiagnose im Configuration Support Manager, um Informationen zur Fehlerbehebung für Ihre Umgebung zu finden.

Anmeldung beim Informatica MySupport-Portal

Um die Knotendiagnostik zum Configuration Support Manager hochzuladen, müssen Sie sich beim Kundenportal anmelden. Die Anmeldedaten sind nicht benutzerspezifisch festgelegt. Für alle Benutzer, die auf das Administrator-Tool Zugriff haben, gelten dieselben Anmeldedaten. Registrieren Sie sich bei <http://communities.informatica.com>, wenn Sie die Anmeldedaten für das Kundenportal nicht haben. Die müssen die Anmeldedaten für das Kundenportal eingeben und diese Daten dann speichern. Alternativ können Sie die Daten des Kundenportals auch jedes Mal beim Hochladen von Knotendiagnostik in den Configuration Support Manager eingeben. Die Knotendiagnostik können Sie konfigurieren, ohne die Anmeldedaten einzugeben.

Zur Gewährleistung der Anmeldesicherheit müssen Sie sich vom Configuration Support Manager und von der Seite zum Hochladen der Knotendiagnostik im Administrator-Tool abmelden.

- Klicken Sie auf den Link zum Abmelden, um sich beim Configuration Support Manager abzumelden.
- Zum Abmelden von der Seite zum Hochladen, klicken Sie auf **Fenster schließen**.

Hinweis: Wenn Sie diese Fenster über die Schließen-Schaltfläche des Webbrowsers schließen, bleiben Sie beim Configuration Support Manager angemeldet. Weitere Benutzer können ohne gültige Anmeldedaten auf den Configuration Support Manager zugreifen.

Anmelden beim Informatica MySupport-Portal

Ehe Sie Knotendiagnostiken generieren und hochladen, müssen Sie sich im Informatica MySupport-Portal angemeldet haben.

1. Klicken Sie im Administrator-Tool auf die Registerkarte **Domäne**.
2. Wählen Sie die Domäne im Navigator aus.
3. Klicken Sie im Inhaltsbereich auf die Ansicht **Diagnostiken**
Eine Liste aller Knoten in der Domäne erscheint.
4. Klicken Sie auf **Anmeldedaten für Kundenportal bearbeiten**.
Das Dialogfeld **Anmeldedaten für Kundenportal bearbeiten** erscheint.

Hinweis: Sie können die Anmeldedaten für das Kundenportal auch im Menü **Aktionen** auf der Registerkarte **Diagnostiken** bearbeiten.

5. Geben Sie die folgenden Anmeldedaten ein:

Feld	Beschreibung
E-Mail-Adresse	Jene E-Mail-Adresse, mit der Sie Ihr Benutzerkonto beim Kundenportal angemeldet haben.
Passwort	Das Passwort für Ihr Benutzerkonto beim Kundenportal.
Projekt-ID	Einmalige ID, die Ihrem Supportprojekt zugewiesen wurde.

6. Klicken Sie auf **OK**.

Generieren der Knotendiagnostik

Wenn Sie Knotendiagnostik generieren, generiert das Administrator Tool die Knotendiagnostik in einer XML-Datei.

Die XML-Datei enthält Details zu den Diensten, Logs, Umgebungsvariablen, Betriebssystemparametern, Systeminformationen und Datenbank-Clients. Worker-Knotendiagnosen enthalten nur Knotenmetadaten. Sie umfassen keine Domänenmetadaten.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten** > Ansicht **Dienste und Knoten**.
2. Wählen Sie im Domänen-Navigator die Domäne aus.
3. Klicken Sie im Inhaltsbereich auf die Ansicht **Diagnostiken**
Eine Liste aller Knoten in der Domäne erscheint.
4. Wählen Sie den Knoten aus.
5. Klicken Sie auf **Diagnostikdatei generieren**.

6. Zur Bestätigung, dass Sie Knotendiagnostik generieren möchten, klicken Sie auf **Ja**.

Hinweis: Sie können auch aus dem Menü **Aktionen** auf der Registerkarte **Diagnostik** heraus Diagnostik generieren.

Die Datei `csmagent<Hostname>.xml`, die die Knotendiagnostik enthält, wird unter `INFA_HOME/server/csm/output` erstellt. Die Knotendiagnostik und der Zeitstempel der generierten Datei werden eingeblendet.

7. Um Diagnostik für Ihre Umgebung auszuführen, laden Sie die Datei `csmagent<Hostname>.xml` auf den Configuration Support Manager hoch.

Alternativ können Sie die XML-Datei auch auf Ihr lokales Laufwerk hochladen.

Nachdem Sie erstmals Knotendiagnostik erstellt haben, können Sie sie erneut generieren oder hochladen.

Knotendiagnostiken herunterladen

Nachdem Sie Knotendiagnostiken generiert haben, können Sie die Datei auf Ihr lokales Laufwerk herunterladen.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten** > Ansicht **Dienste und Knoten**.
2. Wählen Sie im Domänen-Navigator die Domäne aus.
3. Klicken Sie im Inhaltsbereich auf die Ansicht **Diagnostiken**
Eine Liste aller Knoten in der Domäne erscheint.
4. Klicken Sie auf den Diagnostikdateinamen des Knotens.
Die Datei wird in einem eigenen Browserfenster angezeigt.
5. Klicken Sie auf **Datei** > **Speichern unter**. Geben Sie dann den Speicherort der Datei an.
6. Klicken Sie auf **Speichern**.
Die XML-Datei ist auf Ihrem lokalen Laufwerk gesichert.

Knotendiagnostiken hochladen

Sie können die Knotendiagnostik über das Administrator Tool in den Configuration Support Manager hochladen. Sie müssen die Anmeldedaten für das Kundenportal eingeben, bevor Sie die Knotendiagnostik hochladen.

Beim Hochladen der Knotendiagnostik können Sie eine Konfiguration im Configuration Support Manager aktualisieren oder erstellen. Erstellen Sie eine Konfiguration, wenn Sie die Knotendiagnostik zum ersten Mal hochladen. Aktualisieren Sie eine Konfiguration, um die aktuellste Diagnose der Konfiguration anzuzeigen. Um aktuellen und vorherigen Knotenkonfigurationen einer bestehenden Konfiguration zu vergleichen, laden Sie die aktuelle Knotendiagnostik als neue Konfiguration hoch.

Hinweis: Wenn Sie keinen Zugang zum Internet haben, können Sie die Datei herunterladen und sie zu einem späteren Zeitpunkt hochladen. Außerdem können Sie die Datei in einer E-Mail an den Informatica Global Customer Support für eine Fehlerbehebung oder ein Upload senden.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten** > Ansicht **Dienste und Knoten**.
2. Wählen Sie im Domänen-Navigator die Domäne aus.
3. Klicken Sie im Inhaltsbereich auf die Ansicht **Diagnostiken**
Eine Liste aller Knoten in der Domäne erscheint.
4. Wählen Sie den Knoten aus.
5. Generieren Sie eine Knotendiagnose.
6. Klicken Sie auf **Diagnostikdatei auf CSM hochladen**.
Sie können die Knotendiagnose als eine neue Konfiguration oder als Aktualisierung einer bestehenden Konfiguration hochladen.
7. Um eine neue Konfiguration hochzuladen, fahren Sie mit Schritt [10](#) fort.
Um eine Konfiguration zu aktualisieren, wählen Sie **Vorhandene Konfiguration aktualisieren**.
8. Wählen Sie die zu aktualisierende Konfiguration aus der Liste der Konfigurationen aus.
9. Fahren Sie mit Schritt [12](#) fort.

10. Wählen Sie **Als neue Konfiguration hochladen**.
11. Geben Sie die folgenden Konfigurationsdetails ein:

Feld	Beschreibung
Name	Konfigurationsname.
Beschreibung	Konfigurationsbeschreibung.
Typ	Typ des Knotens, wobei es sich um einen der folgenden Typen handeln kann: <ul style="list-style-type: none"> - Produktion - Entwicklung - Test/QA

12. Klicken Sie auf **Jetzt hochladen**.
Nachdem Sie die Knotendiagnostik hochgeladen haben, wechseln Sie zum Configuration Support Manager, um die Knotendiagnostik zu analysieren.
13. Klicken Sie auf **Fenster schließen**
Hinweis: Wenn Sie das Fenster mit der Schaltfläche "Schließen" im Browser schließen, endet die Benutzerauthentifizierungssitzung nicht, und Sie können die Knotendiagnostik nicht mit einem anderen Satz von Anmeldeinformationen im Kundenportal zum Configuration Support Manager hochladen.

Knotendiagnostik analysieren

Zur Analyse der Knotendiagnostik verwenden Sie den Configuration Support Manager.

Verwenden Sie den Configuration Support Manager, um folgende Tasks auszuführen:

- Probleme diagnostizieren, ehe diese kritisch werden.
- Fehlerbehebungsmöglichkeiten erkennen.
- Empfehlungen erkennen, die das Risiko ungeplanter Ausfälle minimieren können.
- Anzeigen der Details zu Ihrer technischen Umgebung.
- Ihre Konfigurationen effizient verwalten.
- Proaktive Alarme per E-Mail und RSS abonnieren.
- Erweiterte Diagnostiken mit einer Vergleichskonfiguration ausführen.

Fehlerbehebungsmöglichkeiten erkennen

Sie können den Configuration Support Manager dazu benutzen, Probleme zu beheben, die während der Operationen aufgetreten sind. Um die Lösung von Supportthemen zu beschleunigen, können Sie Knotendiagnostiken generieren und in den Configuration Support Manager hochladen. Die Knotendiagnostiken lassen sich im Configuration Support Manager analysieren und liefern eine Lösung für Ihr Problem.

Angenommen, Sie führen eine Sorter-Sitzung aus, die große Datenmengen verarbeitet, und Sie bemerken, dass es zu einem Datenverlust kommt. Generieren Sie Knotendiagnostiken und laden Sie diese in den Configuration Support Manager hoch. Wenn Sie die Knotendiagnostiken nach Fehlerbehebungsalarmen

durchsuchen, stoßen Sie auf die Fehlerbehebung EBF178626, die für diesen Fall verfügbar ist. Wenden Sie EBF178626 an und führen Sie die Sitzung erneut aus. Alle Daten werden erfolgreich geladen.

Identifizieren von Empfehlungen

Der Configuration Support Manager hilft Ihnen, Probleme in Ihrem Umfeld zu vermeiden. Bei Problemen, die entstehen, nachdem Sie Änderungen an den Knoteneigenschaften vorgenommen haben, können Sie anhand des Vergleichs der verschiedenen Knotendiagnostiken im Configuration Support Manager eine Fehlersuche durchführen. Der Configuration Support Manager hilft Ihnen außerdem, Empfehlungen oder Aktualisierungen zu finden, mit denen Sie die Knotenleistung verbessern können.

So können Sie zum Beispiel den Knotenspeicher auf die Kapazität für ein größeres Datenvolumen upgraden. Sie generieren Knotendiagnostik und laden sie auf den Configuration Support Manager hoch. Wenn Sie die Diagnostik auf Betriebssystemwarnungen überprüfen, finden Sie die Empfehlungen zum Steigern der Gesamt-Swap-Speicherkapazität des Knotens auf die doppelte Menge des Knotenspeichers, die Sie zur Leistungsoptimierung verwenden können. Erhöhen Sie nach der Empfehlung des Configuration Support Manager die Swap-Speicherkapazität und verhindern Sie auf diese Weise die Verschlechterung der Leistung.

Tipp: Laden Sie regelmäßig Knotendiagnostik auf den Configuration Support Manager hoch und überprüfen Sie die Knotendiagnostik, um die Effizienz Ihrer Umgebung zu gewährleisten.

KAPITEL 14

Informationen zur Globalisierung

Dieses Kapitel umfasst die folgenden Themen:

- [Globalisierung - Übersicht, 254](#)
- [Gebietsschemata, 256](#)
- [Datenverschiebungsmodi, 257](#)
- [Codepages - Übersicht, 259](#)
- [Codepage-Kompatibilität, 261](#)
- [Codepage-Validierung, 269](#)
- [Entspannte Codepage-Validierung, 270](#)
- [PowerCenter Codepage-Umwandlung, 272](#)
- [Fallstudie: ISO 8859-1 Datenverarbeitung, 273](#)
- [Fallstudie: Verarbeiten von Unicode UTF-16LE Daten, 276](#)

Globalisierung - Übersicht

Informatica ist in der Lage, Daten in verschiedenen Sprachen zu verarbeiten. Einige Sprachen erfordern Einzelbytedaten, während andere Mehrbytedaten benötigen. Für die korrekte Datenverarbeitung in Informatica müssen Sie folgende Parameter einrichten:

- **Gebietsschema** Bei Informatica müssen die Einstellungen für das Gebietsschema auf Computern, die auf Informatica-Anwendungen zugreifen, mit den Codepages in der Domäne kompatibel sein. Es kann vorkommen, dass Sie die Einstellungen für das Gebietsschema ändern müssen. Das Gebietsschema gibt die Sprache an, das Territorium, die Zeichensatz-Verschlüsselung und die Sortierreihenfolge.
- **Datenverschiebungsmodus** Der PowerCenter Integration Service kann Einzelbyte- oder Multibyte-Daten verarbeiten und sie in Targets hineinschreiben. Zur Verarbeitung von Einzelbyte-Daten ist der ASCII-Datenverschiebungsmodus vorgesehen. Mehrbytedaten erfordern den Unicode-Datenverschiebungsmodus.
- **Codepages** Codepages enthalten die Verschlüsselung für die Angabe von Zeichen in einem Set aus einer oder mehreren Sprachen. Sie wählen eine Codepage basierend auf dem Typ der Zeichendaten, die Sie verarbeiten möchten. Um die präzise Datenverschiebung zu gewährleisten, müssen Sie dafür sorgen, dass die Codepages untereinander für die Informatica- und die Umgebungskomponenten kompatibel sind. Anhand der Codepages wird zwischen US-ASCII (7-Bit-ASCII-), ISO 8859-1 (8-Bit-ASCII-) und Multibyte-Zeichen unterschieden.

Damit die Daten Ihre Umgebung präzise passieren, müssen folgende Komponenten aufeinander abgestimmt sein:

- Codepage der Domänenkonfigurationsdatenbank
- Die Gebietsschema-Einstellungen und die Codepage des Administrator Tools
- Der Datenverschiebungsmodus für den PowerCenter Integration Service
- Die Codepage für jeden PowerCenter Integration Service Prozess
- Codepage des PowerCenter Client
- PowerCenter Repository Codepage
- Die Codepages der Quell- und der Target-Datenbank
- Codepage für Metadata Manager-Repository.

Sie können den PowerCenter Integration Service für RELAX-Validierung der Codepages konfigurieren. Bei Relax-Validierung sind die Einschränkungen für Quell- und Target-Codepages aufgehoben.

Unicode

Der Unicode-Standard ist die Arbeit des Unicode-Konsortiums, einem internationalen Gremium, das den Austausch von Daten in allen Sprachen fördert. Der Unicode-Standard wurde entwickelt, um jede beliebige Sprache zu unterstützen, gleich wie viele Bytes jedes Zeichen in dieser Sprache benötigen mag. Derzeit unterstützt er alle gängigen Sprachen und bietet eingeschränkte Unterstützung für andere, weniger verbreitete Sprachen. Das Unicode-Konsortium erweitert den Unicode-Standard kontinuierlich mit neuen Zeichencodierungen. Weitere Informationen zum Unicode-Standard finden Sie unter <http://www.unicode.org>.

Der Unicode-Standard umfasst mehrere Zeichensätze. Informatica nutzt die folgenden Unicode-Standards:

- UCS-2 (Universal Character Set, double-byte). Ein Zeichensatz, bei dem jedes verwendete Zeichen zwei Byte nutzt.
- UTF-16LE (Unicode Transformation Format) Ein Codierungsformat, bei dem jedes Zeichen zwischen einem und vier Byte nutzen kann.
- UTF-16 (Unicode Transformation Format) Ein Codierungsformat, bei dem jedes Zeichen zwischen zwei und vier Byte nutzen kann.
- UTF-32 (Unicode Transformation Format) Ein Codierungsformat, bei dem jedes Zeichen vier Byte verwendet.
- GB18030 Ein Unicode-Codierungsformat, das von der chinesischen Regierung definiert wurde, bei dem jedes Zeichen zwischen einem und vier Byte nutzen kann.

Informatica ist eine Unicode-Anwendung. PowerCenter Client, PowerCenter Integration Service und Data Integration Service nutzen intern UCS-2. Der PowerCenter Client konvertiert Benutzereingaben von einer beliebigen Sprache in UCS-2 und wandelt sie vor dem Schreiben in das PowerCenter-Repository von UCS-2 um. Der PowerCenter Integration Service und der Data Integration Service konvertieren die Quelldaten vor der Verarbeitung in UCS-2 und wandelt sie nach der Verarbeitung von UCS-2 um. PowerCenter Client, Model Repository, PowerCenter Integration Service und Data Integration Service unterstützen UTF-16LE. Sie können mit Informatica Daten in einer beliebigen Sprache verarbeiten.

Mit einem Unicode PowerCenter Repository arbeiten

Die PowerCenter Repository-Codepage ist die Codepage der Daten im PowerCenter Repository. Sie wählen die PowerCenter Repository-Codepage aus, wenn Sie ein PowerCenter Repository erstellen oder aktualisieren. Wenn die PowerCenter Repository-Codepage UTF-16LE ist, können Sie ein PowerCenter Repository erstellen, das die Codepage UTF-16LE verwendet.

Die Domänenkonfigurationsdatenbank verwendet die Codepage UTF-16LE. Wenn Sie Metadaten in mehreren Sprachen, wie Chinesisch, Japanisch und Arabisch speichern möchten, müssen Sie die Codepage UTF-16LE für alle Dienste in dieser Domäne verwenden.

Der Service Manager synchronisiert die Liste der Benutzer in der Domäne mit der Liste der Benutzer und Gruppen in allen Anwendungsdiensten. Wenn ein Benutzername in der Domäne Zeichen enthält, die die Codeseite des Anwendungsdienstes nicht erkennt, werden diese Zeichen nicht ordnungsgemäß umgewandelt, was zu Inkonsistenzen führt.

Verwenden Sie die folgenden Richtlinien, wenn Sie UTF-16LE als PowerCenter Repository-Codepage benutzen:

- Die Datenbankcodepage des PowerCenter Repository muss ebenfalls UTF-16LE sein.
- Die PowerCenter Repository-Codepage muss eine Obermenge der Codepages des PowerCenter Client und des PowerCenter Integration Service-Prozesses sein.
- In den UCS-2-Zeichensatz können Sie jedes beliebige Zeichen eingeben. Zum Beispiel: Sie können deutsche, chinesische und englische Metadaten in einem UTF-16LE-fähigen PowerCenter Repository speichern.
- Installieren Sie die Sprachen und Schriftarten auf der Maschine des PowerCenter Client. Wenn Sie ein UTF-16LE PowerCenter Repository verwenden, möchten Sie die Maschinen des PowerCenter Client eventuell befähigen, mehrere Sprachen anzuzeigen. Standardmäßig zeigen die PowerCenter Clients den Text in dem Sprachsatz der Gebietsschemaeinstellungen an. Verwenden Sie in der Systemsteuerung von Windows die Einstellungen unter "Region und Sprache", um den Maschinen der PowerCenter Clients Sprachgruppen hinzuzufügen.
- Sie können den Windows Input Method Editor (IME) dazu verwenden, Multibyte-Zeichen aus jeder beliebigen Sprache einzugeben, ohne jeweils eine Windows-Version für diese spezielle Sprache ausführen zu müssen.
- Wählen Sie für den Prozess des PowerCenter Integration Service eine Codepage aus, die alle Metadaten des PowerCenter Repository korrekt verarbeiten kann. Die Codepage des Prozesses des PowerCenter Integration Service muss eine Untermenge der PowerCenter Repository-Codepage sein. Wenn der PowerCenter Integration Service mehrere Dienstprozesse hat, stellen Sie sicher, dass die Codepages für alle Prozesse des PowerCenter Integration Service eine Untermenge der PowerCenter Repository-Codepage sind. Wenn Sie den Prozess des PowerCenter Integration Service unter Windows ausführen, muss die Codepage des Prozesses des PowerCenter Integration Service dieselbe sein wie die Codepage für die Gebietsschemaeinstellungen des Systems oder des Benutzer. Wenn Sie den Prozess des PowerCenter Integration Service unter UNIX ausführen, verwenden Sie die Codepage UTF-16LE für den Prozess des PowerCenter Integration Service.

Gebietsschemata

Jede Maschine hat ein Gebietsschema. Ein Gebietsschema ist eine Zusammenfassung von Voreinstellungen, die zur Benutzerumgebung gehört, z. B. die Eingabesprache, das Tastaturlayout, die Art der Datensortierung und das Währungs- bzw. Datumsformat. Informatica verwendet auf jeder Maschine Gebietsschemaeinstellungen.

Unter Windows können Sie folgende Gebietsschemaeinstellungen vornehmen:

- Systemschema. Hierzu gehören die Sprache, die Codepages und die erforderlichen Bitmap Font-Dateien, die als Standard für das System verwendet werden.
- Benutzerschema. Hierzu gehören die Standardformate für die Anzeige des Datums, der Uhrzeit, der Währung und des Zahlenformats.

- Eingabeschema. Hierzu gehört die Eingabemethode, z. B. Tastatur, der Systemsprache.

Weitere Informationen zum Konfigurieren der Gebietsschemaeinstellungen unter Windows finden Sie in der Dokumentation zu Windows.

Systemgebietsschema

Das Systemgebietsschema wird auch als das Systemstandardgebietsschema bezeichnet. Es legt fest, welche ANSI- und OEM-Codepages sowie Bitmap-Font-Dateien als Standardwerte für das System verwendet werden. Das Systemgebietsschema enthält die Einstellung der Sprache, was auch festlegt, in welcher Sprache Text auf der Benutzeroberfläche, einschließlich in Dialogfeldern und Fehlermeldungen angezeigt wird. Eine Meldungskatalogdatei definiert die Sprache, in der Meldungen angezeigt werden. Standardmäßig verwendet das Gerät die für das Systemgebietsschema festgelegte Sprache für alle Prozesse, sofern Sie die Sprache nicht für einen bestimmten Prozess überschreiben.

Das Systemgebietsschema ist auf Ihrem System bereits festgelegt und Sie brauchen die Einstellungen eventuell nicht zu ändern, um Informatica auszuführen. Wenn Sie das Systemgebietsschema konfigurieren müssen, konfigurieren Sie das Gebietsschema auf einem Windows-Rechner im Dialogfeld "Regionale Einstellungen". Unter UNIX geben Sie das Gebietsschema in der Umgebungsvariable LANG an.

Benutzerschema

Das Benutzerschema zeigt Datum, Uhrzeit, Währung und Zahlenformate für jeden Benutzer an. Sie können verschiedene Benutzerschemata auf einer einzigen Maschine angeben. Erstellen Sie ein Benutzerschema, wenn Sie auf einer Maschine mit Daten arbeiten, die eine andere Sprache als das Betriebssystem verwenden. Zum Beispiel: Sie sind ein englischer Benutzer, der in Hongkong auf einem chinesischen Betriebssystem arbeitet. Stellen Sie Englisch als Benutzerschema ein, um englische Standards bei Ihrer Arbeit in Hongkong zu verwenden. Wenn Sie ein neues Benutzerkonto erstellen, verwendet die Maschine ein Standardbenutzerschema.. Sie können diese Standardeinstellung ändern, wenn das Konto erstellt ist.

Eingabe-Gebietsschema

Ein Eingabe-Gebietsschema gibt das Tastatur-Layout einer bestimmten Sprache an. Sie haben die Möglichkeit, auf einem Windows-Computer ein Eingabe-Gebietsschema für die Darstellung von Zeichen einer bestimmten Sprache einzustellen.

Mit dem Windows Input Method Editor (IME) können Sie Multibyte-Zeichen einer beliebigen Sprache eingeben, ohne die spezielle Windows-Version für diese Sprache ausführen zu müssen. Beispiel: Sie arbeiten auf einem englischen Betriebssystem und müssen Text in Chinesisch eingeben. In diesem Fall können Sie mit dem IME das Eingabe-Gebietsschema auf Chinesisch einstellen und brauchen die chinesische Windows-Version nicht zu installieren. Möglicherweise möchten Sie einen IME verwenden, um Multibyte-Zeichen in ein PowerCenter-Repository einzugeben, das mit UTF-16LE arbeitet.

Datenverschiebungsmodi

Der Datenverschiebungsmodus ist eine Option des PowerCenter Integration Service, die auf der Basis der Daten gewählt wird, die verschoben werden sollen: Single-Byte oder Multibyte-Daten. Welchen Datenverschiebungsmodus Sie wählen, hängt von folgenden Faktoren ab:

- Den Anforderungen, die Single-Byte oder Multibyte-Metadaten im PowerCenter Repository zu speichern.

- Den Anforderungen, auf die Quelldaten zuzugreifen, die die Single-Byte oder Multibyte-Zeichendaten enthalten.
- Künftige Notwendigkeiten für Single-Byte oder Multibyte-Daten.

Der gewählte Datenverschiebungsmodus hat darauf Einfluss, wie der PowerCenter Integration Service die Beziehungen zur Sitzungs-Codepage und die Codepage-Validierung erzwingt. Er kann auch die Performance beeinflussen. Anwendungen können Single-Byte-Zeichen schneller als Multibyte-Zeichen verarbeiten.

Zeichendatenverschiebungs-Modus

Der PowerCenter Integration Service läuft in den folgenden Modus.

- ASCII (American Standard Code for Information Interchange). Die US-ASCII Codeseite enthält einen Satz von 7-Bit-ASCII-Zeichen und ist ein Subset von anderen Zeichen-Sets. Wenn der PowerCenter Integration Service im ASCII-Datenverschiebungsmodus läuft, erfordert jedes Zeichen ein Byte.
- Unicode. Der Universal-Zeichenverschlüsselungsstandard, der alle Sprachen unterstützt. Wenn der PowerCenter Integration Service im Unicode-Datenverschiebungs-Modus läuft, ordnet er bis zu zwei Byte pro Zeichen zu. Führen Sie den PowerCenter Integration Service im Unicode-Modus aus, wenn die Quelle Multibyte-Daten enthält.

Tipp: Sie können auch den ASCII- oder den Unicode-Datenverschiebungs-Modus nutzen, wenn die Quelle 8-Bit-ASCII-Daten enthält. Beim Verarbeiten von Daten im Unicode-Datenverschiebungs-Modus ordnet der PowerCenter Integration Service ein zusätzliches Byte zu. Zur Leistungssteigerung nutzen Sie den ASCII-Datenverschiebungs-Modus. Wenn die Quelle zum Beispiel Zeichen der ISO 8859-1 Codeseite enthält, verwenden Sie die ASCII-Datenverarbeitung.

Die von Ihnen gewählte Datenverschiebung beeinflusst die Anforderungen der Codeseite. Vergewissern Sie sich, dass die Codeseiten kompatibel sind.

ASCII-Datenverschiebungsmodus

Im ASCII-Modus verarbeitet der PowerCenter Integration Service Single-Byte Zeichen und führt keine Codepage-Konvertierungen durch. Wenn Sie den PowerCenter Integration Service im ASCII-Modus ausführen, erzwingt er keine Sitzungscodepage-Beziehungen.

Unicode-Datenverschiebungsmodus

Im Unicode-Modus erkennt der PowerCenter Integration Service die Multibyte-Zeichendaten und weist jedem Zeichen bis zu zwei Bytes zu. Der PowerCenter Integration Service führt eine Codepage-Konvertierung von Quellen und Targets durch. Wenn Sie für den PowerCenter Integration Service den Unicode-Datenverschiebungsmodus einstellen, verwendet er einen Unicode-Zeichensatz, um die Zeichen in einer angegebenen Codepage zu verarbeiten, zum Beispiel Shift-JIS oder UTF-16LE.

Wenn Sie den PowerCenter Integration Service im Unicode-Modus ausführen, erzwingt er Sitzungscodepage-Beziehungen.

Ändern der Datenverschiebungsmodi

Den Datenverschiebungsmodus können Sie in den Eigenschaften des PowerCenter Integration Service im Administrator Tool ändern. Nachdem Sie den Datenverschiebungsmodus geändert haben, wird der PowerCenter Integration Service im neuen Datenverschiebungsmodus ausgeführt, wenn Sie ihn das nächste Mal starten. Ändert sich der Datenverschiebungsmodus, ändert sich auch die Bearbeitung von Zeichendaten durch den PowerCenter Integration Service. Um die Entstehung von Dateninkonsistenzen in Ihren Target-Tabellen zu vermeiden, führt der PowerCenter Integration Service zusätzliche Prüfungen auf Sitzungen durch, die Sitzungs-Cachespeicher und -Dateien wiederverwenden.

Die folgende Tabelle beschreibt, wie der PowerCenter Integration Service Sitzungsdateien und Cachespeicher behandelt, nachdem Sie den Datenverschiebungsmodus geändert haben:

Sitzungsdatei oder - Cachespeicher	Zeit der Erstellung oder Nutzung	Verhalten des PowerCenter Integration Service nach Änderung des Datenverschiebungsmodus
Sitzungs-Logdatei (*.log)	Bei jeder Sitzung.	Keine Verhaltensänderung. Erstellt ein neues Sitzungs-Log für jede Sitzung mit der Codepage des PowerCenter Integration Service Prozesses.
Arbeitsablauf-Log	Bei jedem Arbeitsablauf.	Keine Verhaltensänderung. Erstellt für jeden Arbeitsablauf anhand der Codepage des PowerCenter Integration Service Prozesses eine neue Arbeitsablauf-Logdatei.
Abgelehnte Datei (*.bad)	Bei jeder Sitzung.	Keine Verhaltensänderung. Hängt mittels der Codepage des PowerCenter Integration Service Prozesses abgelehnte Daten an die vorhandene Ablehnungsdatei an.
Ausgabedatei (*.out)	Bei Sitzungen, die in eine Einfachdatei schreiben.	Keine Verhaltensänderung. Erstellt anhand der Target-Codepage eine neue Ausgabedatei für jede Sitzung.
Indikatordatei (*.in)	Bei Sitzungen, die in eine Einfachdatei schreiben.	Keine Verhaltensänderung. Erstellt für jede Sitzung eine neue Indikatordatei.
Inkrementelle Aggregationsdateien (*.idx, *.dat)	Sitzungen, bei denen inkrementelle Aggregation aktiviert ist.	<p>Wenn Dateien entfernt oder gelöscht werden, erstellt der PowerCenter Integration Service neue Dateien.</p> <p>Werden Dateien nicht verschoben oder gelöscht, schlägt die Sitzung des PowerCenter Integration Service fehl und es wird folgende Fehlermeldung ausgegeben.</p> <pre>SM_7038 Aggregate Error: ServerMode: [server data movement mode] and CachedMode: [data movement mode that created the files] mismatch.</pre> <p>Verschieben oder Löschen von Dateien, die mit einer anderen Codepage erstellt wurden.</p>
Unbenannte persistente Lookup-Dateien (*.idx, *.dat)	Sitzungen mit einer Lookup-Umwandlung, die für einen unbenannten persistenten Lookup-Cachespeicher konfiguriert wurden.	Baut den persistenten Lookup-Cachespeicher neu auf.
Mit Namen versehene persistente Lookup-Dateien (*.idx, *.dat)	Sitzungen mit einer Lookup-Umwandlung, die für einen mit Namen versehenen persistenten Lookup-Cachespeicher konfiguriert wurden.	<p>Wenn Dateien entfernt oder gelöscht werden, erstellt der PowerCenter Integration Service neue Dateien.</p> <p>Werden keine Dateien verschoben oder gelöscht, lässt der PowerCenter Integration Service die Sitzung fehlschlagen.</p> <p>Verschieben oder Löschen von Dateien, die mit einer anderen Codepage erstellt wurden.</p>

Codepages - Übersicht

Eine Codepage enthält die Kodierung zur Angabe von Zeichen in einer oder mehreren Sprachen. Eine Kodierung ist die Zuordnung einer Zahl zu einem Zeichen im Zeichensatz. Codepages dienen der Erkennung

von Daten in unterschiedlichen Sprachen. Beispiel: Wenn Sie ein Mapping für die Verarbeitung japanischer Daten anlegen, müssen Sie eine japanische Codepage für die Quelldaten auswählen.

Wenn Sie eine Codepage auswählen, bezieht sich das Programm oder die Anwendung, für das Sie die Codepage festlegen, auf einen bestimmten Datensatz, der die von der Anwendung erkannten Zeichen beschreibt. Dies hat Auswirkungen auf die Art und Weise, in der die Anwendung Zeichendaten speichert, empfängt und sendet.

Die meisten Computer verwenden eine der folgenden Codepages:

- US-ASCII (7-Bit ASCII)
- MS Latin1 (MS 1252) für Windows-Betriebssysteme
- Latin1 (ISO 8859-1) für UNIX-Betriebssysteme
- IBM EBCDIC US English (IBM037) für Mainframe-Systeme

Die US-ASCII-Codepage enthält alle 7-Bit-ASCII-Zeichen und ist die grundlegendste aller Codepages mit Unterstützung für US-Englisch. Die US-ASCII-Codepage ist nicht mit anderen Codepages kompatibel. Wenn Sie den PowerCenter Client, den PowerCenter Integration Service oder ein PowerCenter-Repository auf einem US-ASCII-System installieren, müssen Sie alle Komponenten auf US-ASCII-Systemen installieren und den PowerCenter Integration Service im ASCII-Modus ausführen.

MS Latin1 und Latin1 unterstützen beide Englisch und die meisten westeuropäischen Sprachen und sind miteinander kompatibel. Wenn Sie den PowerCenter Client, den PowerCenter Integration Service oder ein PowerCenter-Repository auf einem System installieren, das eine dieser Codepages verwendet, können Sie die übrigen Komponenten auf einem beliebigen Computer mit MS Latin1 oder Latin1 Codepages installieren.

Die IBM EBCDIC-Codepage können Sie für den PowerCenter Integration Service Prozess verwenden, wenn Sie ihn auf einem Mainframe-System installieren. Den PowerCenter Client oder das PowerCenter-Repository können Sie nicht auf Mainframe-Systemen installieren. Daher können Sie die Codepage IBM EBCDIC nicht für Installationen mit PowerCenter Client oder PowerCenter Repository nutzen.

UNIX Codepages

In den Vereinigten Staaten haben die meisten UNIX-Betriebssystemen mehr als eine Codepage installiert und verwenden die ASCII-Codepage standardmäßig. Wenn Sie PowerCenter in einer reinen ASCII-Umgebung ausführen möchten, können Sie die ASCII-Codepage verwenden und den PowerCenter Integration Service im ASCII-Modus ausführen.

UNIX-Systeme ermöglichen es Ihnen, die Codepage zu ändern, indem Sie die LANG, LC_CTYPE oder LC_ALL Umgebungsvariable ändern. Angenommen, Sie möchten die Codepage ändern, die ein AIX-Computer benutzt. Verwenden Sie den folgenden Befehl in der C-Shell, um Ihre Umgebung anzuzeigen:

```
locale
```

Daraus ergibt sich die folgende Ausgabe, wobei "C" "ASCII" bedeutet:

```
LANG="C"
LC_CTYPE="C"
LC_NUMERIC="C"
LC_TIME="C"
LC_ALL="C"
```

Um die Sprache in Englisch zu ändern und das System die Latin1-Codepage verwenden zu lassen, können Sie den folgenden Befehl verwenden:

```
setenv LANG en_US.iso88591
```

Wenn Sie das Gebietsschema erneut überprüfen, wurde es so geändert, dass nun Latin1 (ISO 8859-1) verwendet wird:

```
LANG="en_US.iso88591"
LC_CTYPE="en_US.iso88591"
```

```
LC_NUMERIC="en_US.iso88591"  
LC_TIME="en_US.iso88591"  
LC_ALL="en_US.iso88591"
```

Weitere Informationen über das Ändern des Gebietsschemas oder der Codepage in einem UNIX-System, finden Sie in der UNIX-Dokumentation.

Windows Codepages

Das Betriebssystem Windows basiert auf Unicode, aber es zeigt nicht die Codepage an, die vom Betriebssystem in den Umgebungseinstellungen verwendet wird. Sie können jedoch eine fundierte Vermutung anstellen, denn die Codepage basiert meist auf dem Land, in dem Sie das System erworben haben und dem dort üblichen Sprachsystem.

Wenn Sie Windows in den Vereinigten Staaten erworben haben und Englisch als Eingabe- und Anzeigesprache verwenden, nutzt Ihr Betriebssystem standardmäßig die Codepage MS Latin1 (MS1252). Wenn Sie jedoch weitere Anzeige- oder Eingabesprachen von der Windows-Installations-CD installiert haben und diese Sprachen benutzen, verwendet das Betriebssystem eventuell eine andere Codepage.

Um weitere Informationen zu der Standardcodepage für Ihr Windows-Betriebssystem zu erhalten, kontaktieren Sie bitte Microsoft.

Auswählen einer Codepage

Wählen Sie die Codeseiten basierend auf den Zeichendaten, die Sie in Mappings verwenden. Zeichendaten können durch Zeichenmodi dargestellt werden, die auf der Zeichengröße basieren. Die Zeichengröße gibt den Speicherplatz an, den ein Zeichen in der Datenbank benötigt. Die verschiedenen Zeichengrößen sind folgendermaßen definiert:

- Einfaches Byte. Ein Zeichen, das als eindeutige Zahl zwischen 0 und 255 dargestellt wird. Ein Byte entspricht acht Bit. ASCII-Zeichen sind aus einem Byte bestehende Zeichen.
- Doppeltes Byte. Ein Zeichen bestehend aus zwei Byte bzw. 16 Bit, dargestellt als eine eindeutige Zahl größer als 256. Viele asiatische Sprachen, wie Chinesisch, haben Zeichen, die aus doppelten Bytes bestehen.
- Multibyte. Ein Zeichen bestehend aus zwei oder mehr Byte, dargestellt als eindeutige Zahl größer als 256. Viele asiatische Sprachen, wie Chinesisch, haben Multibyte-Zeichen.

Codepage-Kompatibilität

Die Kompatibilität der Codepage ist unabdingbar für das präzise Verschieben, wenn der PowerCenter Integration Service im Unicode-Datenverschiebungsmodus ausgeführt wird.

Eine Codepage kann mit einer anderen Codepage kompatibel oder eine Teilmenge bzw. eine einer anderen Codepage übergeordnete Menge sein:

- Kompatibel. Zwei Codepages sind kompatibel, wenn die Zeichen der beiden Codepages virtuell identisch sind. Beispiel: Die Codepages JapanEUC und JIPSE enthalten identische Zeichen und sind miteinander kompatibel. Das PowerCenter Repository und der PowerCenter Integration Service Prozess können jeweils eine dieser Codepages nutzen und ohne Datenverlust Daten hin- und her schieben.
- Übergeordnete Menge. Eine Codepage ist eine übergeordnete Menge einer anderen Codepage, wenn Sie alle in der anderen Codepage verschlüsselten Zeichen und weitere Zeichen enthält, die nicht auf der

anderen Codepage verschlüsselt sind. Beispiel: MS Latin1 ist eine übergeordnete Menge von US-ASCII, weil es alle Zeichen der US-ASCII-Codepage enthält.

Hinweis: Bei Informatica ist eine Codepage eine sich selbst und allen anderen kompatiblen Codepages übergeordnete Menge.

- Teilmenge. Eine Codepage ist eine Teilmenge einer anderen Codepage, wenn alle Zeichen auf der Codepage ebenfalls auf der anderen Codepage verschlüsselt sind. Beispiel: US-ASCII ist eine Teilmenge von MS Latin1, weil alle Zeichen auf der US-ASCII-Codepage auch auf der MS Latin1 Codepage verschlüsselt sind.

Um die präzise Datenverschiebung zu gewährleisten, muss die Target-Codepage eine übergeordnete Menge der Quell-Codepage sein. Ist die Target-Codepage keine der Quell-Codepage übergeordnete Menge, kann der PowerCenter Integration Service möglicherweise nicht alle Zeichen verarbeiten. Dies führt zu fehlerhaften oder fehlenden Daten. Beispiel: Latin1 ist eine übergeordnete Menge von US-ASCII. Wenn Sie Latin1 als Quell-Codepage und US-ASCII als Target-Codepage auswählen, könnten Sie Zeichendaten verlieren, sofern die Quelle Zeichen enthält, die nicht in US-ASCII enthalten sind.

Beim Installieren oder Upgraden eines PowerCenter Integration Service zum Ausführen im Unicode-Modus müssen Sie die Kompatibilität der Codepages zwischen Domänenkonfigurations-Datenbank, Administrator Tool, PowerCenter Clients, PowerCenter Integration Service Prozessknoten, PowerCenter-Repository, Metadata Manager Repository und den Host-Computern von *pmrep* und *pmcmd* gewährleisten. Im Unicode-Modus erzwingt der PowerCenter Integration Service die Codepage-Kompatibilität zwischen PowerCenter Client und PowerCenter Repository sowie zwischen PowerCenter Integration Service Prozess und PowerCenter-Repository. Beim Ausführen des PowerCenter Integration Service im Unicode-Modus müssen die den Sitzungen zugeordneten Codepages außerdem die richtigen Beziehungen aufweisen:

- Für jede Quelle in der Sitzung muss die Quell-Codepage eine Teilmenge der Target-Codepage sein. Der PowerCenter Integration Service erfordert keine Codepage-Kompatibilität zwischen Quelle und PowerCenter Integration Service Prozess oder zwischen PowerCenter Integration Service Prozess und Target.
- Enthält die Sitzung eine Lookup- oder gespeicherte Prozedurumwandlung, muss die Datenbank oder Datei-Codepage eine Teilmenge des Target, das Daten aus der Lookup- oder gespeicherten Prozedurumwandlung aufnimmt und eine übergeordnete Menge der Quelle sein, die Daten an die Lookup- oder gespeicherte Prozedurumwandlung übergibt.
- Enthält die Sitzung eine externe Prozedur oder benutzerdefinierte Umwandlung, muss die Prozedur Daten in einer Codepage übergeben, die eine Teilmenge der Target-Codepage für Targets ist, die Daten von der externen Prozedur oder benutzerdefinierten Umwandlungen entgegennehmen.

Informatica nutzt Codepages für folgende Komponenten:

- Domänenkonfigurationsdatenbank. Die Domänenkonfigurations-Datenbank muss mit den Codepages von PowerCenter Repository und Metadata Manager Repository kompatibel sein.
- Administrator Tool. Die Dateneingabe in das Administrator Tool ist in einer beliebigen Sprache möglich.
- PowerCenter Client. Die Eingabe von Metadaten in den PowerCenter-Client ist in einer beliebigen Sprache möglich.
- PowerCenter Integration Service-Prozess. Der PowerCenter Integration Service kann Daten in ASCII-Modus oder Unicode-Modus verschieben. Als Datenverschiebungsmodus voreingestellt ist ASCII, wobei 7-Bit-ASCII- bzw. 8-Bit-ASCII-Zeichendaten übergeben werden. Zum Übergeben von Mehrbyte-Zeichendaten aus Quellen in Targets muss der Unicode-Datenverschiebungsmodus eingesetzt werden. Beim Ausführen des PowerCenter Integration Service im Unicode-Modus nutzt dieser bis zu drei Byte für jedes zu verschiebende Zeichen und führt zur Gewährleistung der Datenintegrität zusätzliche Prüfungen auf Sitzungsebene durch.

- PowerCenter Repository. Das PowerCenter Repository kann Daten in beliebigen Sprachen speichern. Zum Speichern von Mehrbyte-Daten im PowerCenter-Repository können Sie die UTF-16LE-Codepage nutzen. Die Codepage für das PowerCenter-Repository ist dieselbe wie die Datenbank-Codepage.
- Metadata Manager Repository. Im Metadata Manager Repository können Daten in beliebiger Sprache gespeichert werden. Zum Speichern von Mehrbyte-Daten im Repository können Sie die UTF-16LE-Codepage für das Metadata Manager Repository verwenden. Die Codepage für das Repository ist dieselbe wie für die Datenbank-Codepage.
- Quellen und Targets. Die Quellen und Targets speichern Daten in einer oder mehreren Sprachen. Sie benutzen die Codepages für die Angabe der Zeichenarten in den Quellen und Targets.
- PowerCenter-Befehlszeilenprogramme. Sie müssen gewährleisten, dass die Codepage für *pmrep* eine Teilmenge der PowerCenter Repository Codepage und die Codepage für *pmcmd* eine Teilmenge der PowerCenter Integration Service Prozess Codepage ist.

Die meisten Datenbankserver nutzen zwei Codepages: eine Client-Codepage für die Aufnahme von Daten von Client-Anwendungen und eine Server-Codepage zum Speichern der Daten. Wenn der Datenbankserver läuft, konvertiert er Daten zwischen den beiden Codepages, wenn diese unterschiedlich sind. Bei dieser Datenbankkonfiguration interagiert der PowerCenter Integration Service Prozess mit der Datenbank-Client-Codepage. Daher müssen Codepages, die der PowerCenter Integration Service Prozess verwendet, wie die Codepages für PowerCenter-Repository, Quelle oder Target, identisch mit der Codepage des Datenbank-Client sein. Die Datenbank-Client-Codepage ist normalerweise identisch mit der Codepage des Betriebssystems, auf dem der PowerCenter Integration Service Prozess ausgeführt wird. Die Datenbank-Client-Codepage ist eine Teilmenge der Datenbankserver-Codepage.

Ausführliche Informationen über bestimmte Datenbank-Client- und Server-Codepages finden Sie in Ihrer Datenbank-Dokumentation.

Hinweis: Der Reporting Service erfordert keine Angabe einer Codepage für die im Data Analyzer Repository gespeicherten Daten.. Das Administrator Tool schreibt Domänen-, Benutzer- und Gruppeninformationen in den Reporting Service. DataDirect-Treiber führen die erforderlichen Datenumwandlungen jedoch durch.

Codepage der Domänenkonfigurationsdatenbank

Die Domänen-Konfigurationsdatenbank muss mit den Codepages des PowerCenter Repository, des Metadata Manager Repository und des Model Repository, kompatibel sein.

Der Service Manager synchronisiert die Liste der Benutzer in der Domäne mit der Liste der Benutzer und Gruppen in allen Anwendungsdiensten.. Wenn ein Benutzername in der Domäne Zeichen enthält, die die Codeseite des Anwendungsdienstes nicht erkennt, werden diese Zeichen nicht ordnungsgemäß umgewandelt, was zu Inkonsistenzen führt.

Codepage des Administrator Tools

Das Administrator Tool kann auf jedem Knoten in einer Informatica-Domäne ausgeführt werden. Als Codepage für das Administrator Tool wird die Codepage des Betriebssystems des Knotens verwendet. Jeder Knoten in der Domäne muss dieselbe Codepage verwenden.

Die Codepage des Administrator Tools muss folgende Kriterien erfüllen:

- Sie muss eine Untermenge der Codepage des PowerCenter Repository sein.
- Sie muss eine Untermenge der Codepage des Metadata Manager Repository sein.
- Sie muss eine Untermenge der Codepage des Model Repository sein.

Codepage des PowerCenter Client

Die Codepage des PowerCenter Client entspricht der Codepage des Betriebssystems des PowerCenter Client. Zur Kommunikation mit dem PowerCenter Repository muss die Codepage des PowerCenter Client eine Untermenge der Codepage des PowerCenter Repository sein.

Codepage des PowerCenter Integration Service-Prozesses

Die Codepage eines PowerCenter Integration Service-Prozesses ist die Codepage des Knotens, auf dem der PowerCenter Integration Service-Prozess ausgeführt wird. Definieren Sie die Codepage für jeden PowerCenter Integration Service-Prozess im Administrator Tool auf der Registerkarte "Prozesse".

Unter UNIX können Sie jedoch die Codepage des PowerCenter Integration Service-Prozesses ändern, indem Sie die Umgebungsvariable LANG, LC_CTYPE oder LC_ALL für den Benutzer ändern, erden Prozess startet.

Die Codepage des PowerCenter Integration Service Prozesses muss:

- Eine Untermenge der Codepage des PowerCenter Repository sein.
- Eine Obermenge des Computers sein, der *pmcmd* hostet, oder eine Obermenge der Codepage sein, die in der Umgebungsvariablen INFA_CODEPAGENAME angegeben ist

Die Codepages aller PowerCenter Integration Service-Prozesse müssen miteinander kompatibel sein. Sie können z. B. MS Windows Latin1 für einen Knoten unter Windows und ISO-8859-1 für einen Knoten unter UNIX verwenden.

PowerCenter Integration Services, die für den Unicode-Modus konfiguriert sind, validieren Codepages beim Start einer Sitzung, um genaue Datenbewegungen zu gewährleisten. Dabei wird die Sitzungscodepage zur Konvertierung der Zeichendaten herangezogen. Wenn Sie den PowerCenter Integration Service im ASCII-Modus ausführen, validiert er die Sitzungscodepages nicht. Er liest alle Zeichendaten als ASCII-Zeichen und führt keine Codepage-Konvertierung durch.

Mit jeder Codepage ist eine Sortierreihenfolge verknüpft. Wenn Sie eine Sitzung konfigurieren, können Sie eine der Sortierreihenfolgen wählen, die mit der Codepage der PowerCenter Integration Service-Prozesses verbunden sind. Wenn Sie den PowerCenter Integration Service im Unicode-Modus ausführen, nutzt er die ausgewählte Sitzungssortierreihenfolge zur Sortierung der Zeichendaten. Wenn Sie den PowerCenter Integration Service im ASCII-Modus ausführen, sortiert er alle Zeichendaten in binärer Sortierreihenfolge.

Wenn Sie dem PowerCenter Integration Service in den Vereinigten Staaten unter Windows ausführen, sollten Sie MS Windows Latin1 (ANSI) als Codepage des PowerCenter Integration Service-Prozesses verwenden.

Wenn Sie dem PowerCenter Integration Service in den Vereinigten Staaten unter UNIX ausführen, sollten Sie ISO 8859-1 als Codepage des PowerCenter Integration Service-Prozesses verwenden.

Wenn Sie *pmcmd* für die Kommunikation mit dem PowerCenter Integration Service nutzen, muss die Codepage des Betriebssystems, das *pmcmd* hostet, mit der Codepage des PowerCenter Integration Service-Prozesses identisch sein.

Der PowerCenter Integration Service generiert die Namen der Sitzungsprotokolldateien, Ablehnungsdateien, Caches bzw. Cache-Dateien und Leistungsdetaildateien auf der Basis der Codepage des PowerCenter Integration Service-Prozesses.

PowerCenter Repository-Codepage

Die Codepage des PowerCenter-Repository ist die Codepage der Daten im Repository. Der PowerCenter Repository Service verwendet die PowerCenter Repository-Codepage, um Metadaten in der PowerCenter Repository-Datenbank zu speichern und daraus abzurufen. Wählen Sie die PowerCenter Repository-Codepage beim Erstellen oder Aktualisieren eines PowerCenter-Repository aus. Wenn die Codepage der PowerCenter

Repository-Datenbank UTF-16LE ist, können Sie ein PowerCenter-Repository mit UTF-16LE als Codepage erstellen.

Die Codepage des PowerCenter-Repository muss folgende Bedingungen erfüllen:

- Mit der Codepage der Domänenkonfigurationsdatenbank kompatibel sein
- Eine Obermenge der Codepage des Administrator Tools sein
- Eine Obermenge der Codepage des PowerCenter Clients sein
- Eine Obermenge der Codepage für den PowerCenter Integration Service-Prozess sein
- Eine Obermenge des Computers sein, der *pmrep* hostet, oder eine Obermenge der Codepage sein, die in der Umgebungsvariablen INFA_CODEPAGENAME angegeben ist

Eine globale PowerCenter Repository-Codepage muss eine Teilmenge der lokalen PowerCenter Repository-Codepage sein, wenn Sie Verknüpfungen im lokalen PowerCenter-Repository erstellen möchten, die auf ein Objekt in einem globalen PowerCenter-Repository verweisen.

Wenn Sie Objekte von einem PowerCenter-Repository zu einem anderen PowerCenter-Repository kopieren, muss die Codepage für das Target-Repository eine Obermenge der Codepage des Quell-Repositorys sein.

Codepage für Metadaten Manager-Repository.

Die Codepage des Metadata Manager-Repository ist die Codepage der Daten im Repository. Der Metadata Manager Service verwendet die Metadata Manager-Repository-Codepage, um Metadaten in der Repository-Datenbank zu speichern und daraus abzurufen. Das Administrator Tool schreibt Benutzer- und Gruppen-Informationen in den Metadata Manager Service. Außerdem schreibt das Administrator Tool Domäneninformationen in die Repository-Datenbank. Der PowerCenter Repository Service-Prozess schreibt Metadaten in die Repository-Datenbank. Wählen Sie die Repository-Codepage beim Erstellen oder Aktualisieren eines Metadata Manager-Repository aus. Wenn die Codepage der Repository-Datenbank UTF-16LE ist, können Sie ein Repository mit UTF-16LE als Codepage erstellen.

Die Codepage des Metadata Manager-Repository muss folgende Bedingungen erfüllen:

- Mit der Codepage der Domänenkonfigurationsdatenbank kompatibel sein
- Eine Obermenge der Codepage des Administrator Tools sein
- Eine Untermenge der Codepage des PowerCenter Repository sein.
- Eine Obermenge der Codepage für den PowerCenter Integration Service-Prozess sein

PowerCenter-Quell-Codepage

Die Quell-Codepage ist vom Typ der Quelle abhängig:

- Flatfiles und VSAM-Dateien. Die Codepage der Daten in der Datei. Wählen Sie bei der Konfiguration der Flatfile- oder COBOL-Quelldefinition eine Codepage, die mit der Codepage der Daten in der Datei übereinstimmt.
- XML-Dateien Der PowerCenter Integration Service konvertiert XML in Unicode, wenn er eine XML-Quelle analysiert. Wenn Sie eine XML-Quelldefinition erstellen, weist der PowerCenter Designer eine Standard-Codepage zu. Sie können die Codepage nicht ändern.
- Relationale Datenbanken. Die Codepage des Datenbank-Client. Wählen Sie bei der Konfiguration der relationale Verbindung im PowerCenter Workflow Manager eine Codepage, die mit der Codepage des Datenbank-Client kompatibel ist. Wenn Sie eine Datenbank-Umgebungsvariable zur Angabe der Sprache für die Datenbank festlegen, stellen Sie sicher, dass die Codepage für die Verbindung mit der für die Variable festgelegten Sprache kompatibel ist. Zum Beispiel: Wenn Sie die Umgebungsvariable NLS_LANG für eine Oracle-Datenbank festgelegt haben, müssen Sie sicherstellen, dass die Codepage der Oracle-

Verbindung mit dem festgelegten Wert in der Variable `NLS_LANG` identisch ist. Wenn Sie keine kompatiblen Codepages verwenden, können die Sitzungen hängen, Daten können inkonsistent werden, oder Sie können einen Datenbankfehler erhalten, wie z. B.:

```
ORA-00911: Invalid character specified.
```

Unabhängig vom Typ der Quelle muss die Quell-Codepage eine Teilmenge der Codepage der Umwandlungen und Targets sein, die Daten von der Quelle empfangen. Die Quell-Codepage braucht keine Teilmenge der Umwandlungen oder Targets zu sein, die keine Daten aus der Quelle empfangen.

Hinweis: Wählen Sie IBM EBCDIC nur dann als Codepage für Ihre Quelldatenbankverbindung, wenn Sie auf EBCDIC-Daten zugreifen, wie beispielsweise Daten aus einer extrahierten Großrechnerdatei zugreifen.

PowerCenter-Target-Codepage

Die Target-Codepage ist vom Typ des Targets abhängig:

- **Einfachdateien** Wählen Sie bei der Konfiguration der Einfachdatei-Target-Definition eine Codepage, die mit der Codepage der Daten in der Einfachdatei übereinstimmt.
- **XML-Dateien** Konfigurieren Sie die XML-Target-Codepage, nachdem Sie die XML-Target-Definition erstellt haben. Der XML-Assistent ordnet dem XML-Target eine Standard-Codepage zu. Der PowerCenter Designer wendet nicht die Codepage an, die im XML-Schema steht.
- **Relationale Datenbanken.** Wählen Sie bei der Konfiguration der relationale Verbindung im PowerCenter Workflow Manager eine Codepage, die mit der Codepage des Datenbank-Client kompatibel ist. Wenn Sie eine Datenbank-Umgebungsvariable zur Angabe der Sprache für die Datenbank festlegen, stellen Sie sicher, dass die Codepage für die Verbindung mit der für die Variable festgelegten Sprache kompatibel ist. Zum Beispiel: Wenn Sie die Umgebungsvariable `NLS_LANG` für eine Oracle-Datenbank festgelegt haben, müssen Sie sicherstellen, dass die Codepage der Oracle-Verbindung mit dem festgelegten Wert in der Variable `NLS_LANG` kompatibel sein. Wenn Sie keine kompatiblen Codepages verwenden, können die Sitzungen hängen oder Sie können einen Datenbankfehler erhalten, wie z. B.:

```
ORA-00911: Invalid character specified.
```

Die Target-Codepage muss eine Obermenge der Codepage der Umwandlungen und Quellen sein, die Daten an das Target liefern. Die Target-Codepage braucht keine Obermenge der Umwandlungen oder Quellen zu sein, die keine Daten an das Target liefern.

Der Integration Service erstellt Sitzungsindikatordateien, Sitzungsausgabedateien sowie Steuerungsdateien für externen Ladevorgang und Datendateien unter Verwendung der Codepage der Target-Einfachdatei.

Hinweis: Wählen Sie IBM EBCDIC nur dann als Codepage für Ihre Target-Datenbankverbindung, wenn Sie auf EBCDIC-Daten zugreifen, wie beispielsweise Daten aus einer extrahierten Großrechnerdatei zugreifen.

Befehlszeilenprogramm-Codepages

Die Befehlszeilenprogramme *pmcmd* und *pmrep* erfordern Codepage-Kompatibilität. *pmcmd* und *pmrep* nutzen Codepages zum Senden von Befehlen in Unicode. Andere Befehlszeilenprogramme erfordern keine Codepages.

Die Codepage-Kompatibilität für *pmcmd* und *pmrep* ist davon abhängig, ob Sie die Codepage-Umgebungsvariable `INFA_CODEPAGENAME` für *pmcmd* oder *pmrep* konfiguriert haben. Sie können diese Variable entweder für ein Befehlszeilenprogramm oder für beide angeben.

Falls Sie diese Variable für ein Befehlszeilenprogramm nicht konfiguriert haben, vergewissern Sie sich bitte, dass folgende Anforderungen erfüllt sind:

- Haben Sie die Variable nicht für *pmcmd* konfiguriert, muss die Codepage des *pmcmd* für das Computer-Hosting eine Teilmenge der Codepage für den PowerCenter Integration Service Prozess sein.

- Sollten Sie die Variable nicht für *pmrep* konfiguriert haben, muss die Codepage des *pmrep* für das Computer-Hosting eine Teilmenge der PowerCenter Repository Codepage sein.

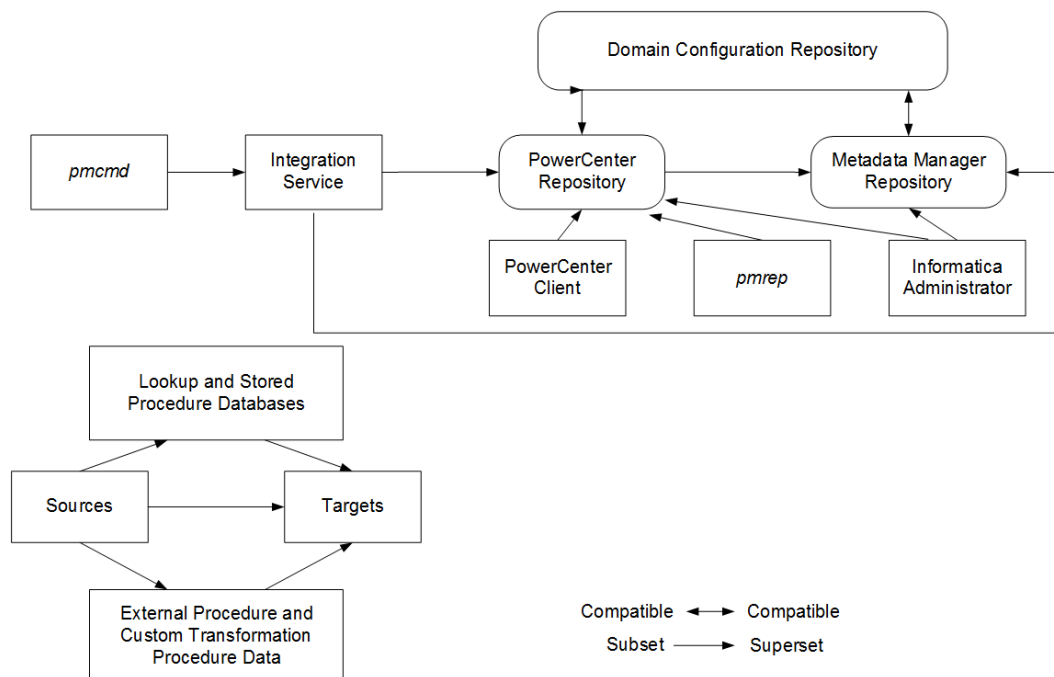
Wenn Sie die Codepage-Umgebungsvariable INFA_CODEPAGE_NAME für *pmcmd* oder *pmrep* konfigurieren, vergewissern Sie sich bitte, dass folgende Anforderungen erfüllt sind:

- Konfigurieren Sie INFA_CODEPAGE_NAME für *pmcmd*, muss die für die Variable definierte Codepage eine Teilmenge der Codepage für den PowerCenter Integration Service Prozess sein.
- Falls Sie INFA_CODEPAGE_NAME für *pmrep* konfigurieren, muss die für die Variable definierte Codepage eine Teilmenge der PowerCenter Repository Codepage sein.
- Führen Sie *pmcmd* und *pmrep* auf ein- und demselben Computer aus und konfigurieren Sie die Variable INFA_CODEPAGE_NAME, muss die für die Variable definierte Codepage Teilmengen der Codepages für den PowerCenter Integration Service Prozess und das PowerCenter Repository darstellen.

Sofern die Codepages nicht kompatibel sind, wird der PowerCenter Integration Service Prozess den Arbeitsablauf, die Sitzung oder die Task möglicherweise nicht vom PowerCenter Repository abfragen.

Codepage-Kompatibilität - Zusammenfassung

Die folgende Abbildung zeigt die Codepage-Kompatibilität in der Informatica-Umgebung:



Die folgende Tabelle enthält eine Zusammenfassung der Codepage-Kompatibilität zwischen Quellen, Zielen, Repositorys, dem Informatica Administrator, dem PowerCenter Client und dem PowerCenter-Integrationsdienst-Prozess:

Komponenten-Codepage	Codepage-Kompatibilität
Quelle (inklusive relationale, Einfachdatei und XML-Datei)	Ziel-Teilmenge. Teilmenge der Lookup-Daten. Teilmenge gespeicherter Prozeduren. Teilmenge der Codepage einer externen Prozedur oder einer benutzerdefinierten Umwandlungsprozedur.
Ziel (inklusive relationale, XML-Dateien und Einfachdateien)	Übergeordnete Menge der Quelle. Übergeordnete Menge für Lookup-Daten. Übergeordnete Menge gespeicherter Prozeduren. Übergeordnete Menge der Codepage für eine externe Prozedur oder eine benutzerdefinierte Umwandlungsprozedur. Der Integrationsdienst-Prozess erstellt mit der Codepage der Ziel-Einfachdatei externe Ladedaten und Steuerungsdateien.
Datenbank für Lookup- und gespeicherte Prozeduren	Ziel-Teilmenge. Übergeordnete Menge der Quelle.
Externe Prozedur und benutzerdefinierte Umwandlungsprozeduren	Ziel-Teilmenge. Übergeordnete Menge der Quelle.
Domänen-Konfigurationsdatenbank	Kompatibel mit dem PowerCenter-Repository-Dienst. Kompatibel mit dem Metadata Manager Repository.
PowerCenter-Integrationsdienst-Prozess	Kompatibel mit dessen Betriebssystem Teilmenge des PowerCenter-Repository. Teilmenge des Metadata Manager Repository. Übergeordnete Menge für Computer-Hosting <i>pmcmd</i> . Identisch mit anderen Knoten, auf denen die PowerCenter-Integrationsdienst-Prozesse ausgeführt werden.
PowerCenter-Repository	Kompatibel mit der Domänen-Konfigurationsdatenbank. Übergeordnete Menge des PowerCenter Client. Übergeordnete Menge der Knoten, auf denen der PowerCenter-Integrationsdienst-Prozess ausgeführt wird. Übergeordnete Menge des Metadata Manager Repository. Eine globale PowerCenter-Repository Codepage muss eine Teilmenge eines lokalen PowerCenter-Repository sein.
PowerCenter Client	Teilmenge des PowerCenter-Repository.
Computer, auf dem <i>pmcmd</i> ausgeführt wird	Teilmenge des PowerCenter-Integrationsdienst-Prozesses.
Computer, auf dem <i>pmrep</i> ausgeführt wird	Teilmenge des PowerCenter-Repository.

Komponenten-Codepage	Codepage-Kompatibilität
Administrator-Tool	Teilmenge des PowerCenter-Repository. Teilmenge des Metadata Manager Repository.
Metadata Manager Repository	Kompatibel mit der Domänen-Konfigurationsdatenbank. Teilmenge des PowerCenter-Repository. Übergeordnete Menge des Administrator-Tool. Übergeordnete Menge des PowerCenter-Integrationsdienst-Prozesses.

Codepage-Validierung

Die Computer, die den PowerCenter Client, den PowerCenter Integration Service Prozess und die PowerCenter Repository-Datenbank hosten, müssen die entsprechenden Codepages verwenden. So lassen sich Daten- oder Repository-Inkonsistenzen vermeiden. Wenn der PowerCenter Integration Service im Unicode-Datenverschiebungsmodus ausgeführt wird, erzwingt er Sitzungs-Codepage-Beziehungen. Wird der PowerCenter Integration Service im ASCII-Modus ausgeführt, erzwingt er keine Sitzungs-Codepage-Beziehungen.

Um die Kompatibilität zu gewährleisten, führen PowerCenter Client und PowerCenter Integration Service folgende Codepage-Validierungen durch:

- PowerCenter schränkt die Verwendung EBCDIC-basierter Codepages für Repositories ein. Da Sie weder den PowerCenter-Client noch das PowerCenter-Repository auf Mainframe-Systemen installieren können, ist es nicht möglich, EBCDIC-basierte Codepages wie IBM EBCDIC als PowerCenter-Repository Codepage zu wählen.
- Der PowerCenter Client kann keine Verbindung zum PowerCenter-Repository herstellen, wenn seine Codepage eine Teilmenge der PowerCenter-Repository-Codepage ist. Ist die PowerCenter-Client-Codepage keine Teilmenge der PowerCenter-Repository-Codepage, kann der PowerCenter-Client aufgrund des folgenden Fehlers keine Verbindung zur PowerCenter-Repository-Codepage herstellen:

```
REP_61082 <PowerCenter Client>'s code page <PowerCenter Client code page> is not one-way compatible to repository <PowerCenter repository name>'s code page <PowerCenter repository code page>.
```

- Nachdem Sie die PowerCenter-Repository-Codepage eingerichtet haben, können Sie sie ändern. Nachdem Sie ein PowerCenter-Repository erstellt oder geupgradet haben, dürfen Sie die PowerCenter-Repository-Codepage nicht ändern. So vermeiden Sie Datenverluste und Inkonsistenzen im PowerCenter-Repository.
- Der PowerCenter Integration Service Prozess kann starten, wenn seine Codepage eine Untermenge der PowerCenter-Repository-Codepage ist. Die Codepage des PowerCenter Integration Service Prozesses muss eine Teilmenge der PowerCenter-Repository-Codepage sein, um Datenverlust oder Inkonsistenzen zu vermeiden. Ist er keine Teilmenge der PowerCenter-Repository-Codepage, schreibt der PowerCenter Integration Service folgende Meldung in die Log-Dateien:

```
REP_61082 <PowerCenter Integration Service>'s code page <PowerCenter Integration Service code page> is not one-way compatible to repository <PowerCenter repository name>'s code page <PowerCenter repository code page>.
```

- Im Unicode-Datenverschiebungsmodus startet der PowerCenter Integration Service Arbeitsabläufe mit den entsprechenden Quell- und Target-Codepage-Beziehungen für jede Sitzung. Wird der PowerCenter Integration Service im Unicode-Modus ausgeführt, muss die Codepage für jede Quelle in einer Sitzung eine Teilmenge der Target-Codepage sein. So wird Datenverlust während einer Sitzung vermieden.

Stehen Quell- und Target-Codepage nicht im richtigen Verhältnis zueinander schlägt die PowerCenter Integration Service Sitzung fehl und ins Sitzungs-Log wird folgende Meldung geschrieben:

```
TM_6227 Error: Code page incompatible in session <session name>. <Additional details>.
```

- Der PowerCenter Workflow Manager validiert die Quell-, Target-, Lookup- und gespeicherten Prozedur-Codepage-Beziehungen für jede Sitzung. Beim Speichern der Sitzung prüft der PowerCenter Workflow Manager die Codepage-Beziehungen unabhängig vom Datenverschiebungsmodus des PowerCenter Integration Service. Konfigurieren Sie eine Sitzung mit ungültigen Quell-, Target-, Lookup- oder gespeicherten Prozedur-Codepage-Beziehungen, generiert der PowerCenter Workflow Manager beim Speichern der Sitzung eine Warnmeldung wie die folgende:

```
CMN_1933 Code page <code page name> for data from file or connection associated with transformation <name of source, target, or transformation> needs to be one-way compatible with code page <code page name> for transformation <source or target or transformation name>.
```

Wenn Sie die Sitzung im ASCII-Modus ausführen möchten, können Sie die Sitzung speichern wie konfiguriert. Um die Sitzung im Unicode-Modus auszuführen, müssen Sie die Sitzung so bearbeiten, dass sie die richtigen Codepages verwendet.

Entspannte Codepage-Validierung

In Ihrer Umgebung kann es notwendig sein, dass Sie Daten aus unterschiedlichen Quellen mit Zeichensätzen aus verschiedenen Sprachen verarbeiten. Zum Beispiel könnten Sie Daten aus englischen und japanischen Quellen unter Verwendung desselben PowerCenter-Repository verarbeiten müssen oder Quelldaten extrahieren wollen, die in einer Unicode-Codierung wie UTF-16LE codiert sind. Sie können den PowerCenter Integration Service für eine entspannte Codepage-Validierung konfigurieren. Mit der entspannten Codepage-Validierung können Sie Daten mit Quellen und Targets verarbeiten, die inkompatible Codepages haben.

Auch wenn die entspannte Codepage-Validierung Codepage-Einschränkungen bei Quellen und Targets entfernt, erzwingt sie dennoch die Codepage-Kompatibilität zwischen dem PowerCenter Integration Service und dem PowerCenter-Repository.

Hinweis: Die entspannte Codepage-Validierung ist kein Schutz vor möglichen Dateninkonsistenzen, wenn Sie Daten zwischen inkompatiblen Codepages verschieben. Sie müssen sicherstellen, dass die Zeichen, die der PowerCenter Integration Service aus der Quelle liest, in der Target-Codepage enthalten sind.

Informatica hebt die folgenden Einschränkungen auf, wenn Sie die entspannte Codepage-Validierung einsetzen:

- Quell- und Target-Codepages. Sie können jede beliebige Codepage verwenden, die von Informatica für Ihre Quell- und Targetdaten unterstützt wird.
- Sitzungs-Sortier-Reihenfolge. Sie können beim Konfigurieren von Sitzungen jede beliebige Sortierreihenfolge verwenden, die von Informatica unterstützt wird.

Wenn Sie eine Sitzung mit entspannter Codepage-Validierung starten, schreibt der PowerCenter Integration Service die folgende Meldung in das Sitzungs-Log:

```
TM_6185 WARNING! Data code page validation is disabled in this session.
```

Wenn Sie die entspannte Codepage-Validierung verwenden, schreibt der PowerCenter Integration Service Beschreibungen der Datenbankverbindungs-Codepages in das Sitzungs-Log.

Der folgende Text zeigt ein Beispiel für eine Codepage-Meldung im Sitzungs-Log:

```
TM_6187 Repository code page: [MS Windows Latin 1 (ANSI), superset of Latin 1]  
WRT_8222 Target file [$PMTARGETFileDir\passthru.out] code page: [MS Windows Traditional Chinese, superset of Big 5]
```

```

WRT_8221 Target database connection [Japanese Oracle] code page: [MS Windows Japanese,
superset of Shift-JIS]
TM_6189 Source database connection [Japanese Oracle] code page: [MS Windows Japanese,
superset of Shift-JIS]
CMN_1716 Lookup [LKP_sjis_lookup] uses database connection [Japanese Oracle] in code
page [MS Windows Japanese, superset of Shift-JIS]
CMN_1717 Stored procedure [J_SP_INCREMENT] uses database connection [Japanese Oracle] in
code page [MS Windows Japanese, superset of Shift-JIS]

```

Wenn der PowerCenter Integration Service Daten nicht richtig konvertieren kann, schreibt er eine Fehlermeldung in das Sitzungs-Log.

Konfigurieren des PowerCenter Integration Service

Um den PowerCenter Integration Service auf Codepage Relaxation zu konfigurieren, müssen folgende Tasks im Administrator Tool durchgeführt werden:

- Codepage-Validierung deaktivieren. Deaktivieren Sie die Option ValidateDataCodePages in den Eigenschaften des PowerCenter Integration Service.
- Konfigurieren Sie den PowerCenter Integration Service auf Unicode-Datenverschiebungsmodus. Wählen Sie in den Eigenschaften des PowerCenter Integration Service Unicode als Datenverschiebungsmodus.
- Konfigurieren Sie den PowerCenter Integration Service so, dass er zum Schreiben in den Logs den Zeichensatz UTF-16LE verwendet. Aktivieren Sie beim Konfigurieren von Sitzungen oder Arbeitsabläufen zum Schreiben in Log-Dateien die Option LogInUTF8 in den Eigenschaften für den PowerCenter Integration Service. Wenn Sie die Option LogInUTF8 aktivieren, schreibt der PowerCenter Integration Service alle Logs in UTF-16LE. Der PowerCenter Integration Service schreibt per Standard im Log-Manager in UTF-16LE.

Kompatible Quell- und Target-Codepages auswählen

Obwohl es das PowerCenter ermöglicht, jede unterstützte Codepage zu verwenden, gibt es Risiken mit inkompatiblen Codepages für Quellen und Targets. Wenn Ihre Target-Codepage keine Obermenge der Quell-Codepage ist, riskieren Sie Inkonsistenzen in den Target-Daten, denn die Quelldaten enthalten eventuell Zeichen, die nicht in der Target-Codepage codiert sind.

Wenn der PowerCenter Integration Service Zeichen liest, die nicht in der Target-Codepage enthalten sind, riskieren Sie Umwandlungsfehler, inkonsistente Daten oder fehlgeschlagene Sitzungen.

Hinweis: Wenn Sie die Codepage-Validierung lockern, liegt es in Ihrer Verantwortung, dass die Datenkonvertierung von der Quelle in das Target korrekt funktioniert.

Fehlerbehebung für Codepage-Lockerung

Der PowerCenter Integration Service hat einen Fehler in einer Sitzung begangen und schreibt folgende Meldung in das Sitzungs-Log:

```

TM_6188 The specified sort order is incompatible with the PowerCenter Integration
Service code page.

```

Wählen Sie zum Validieren von Codepages eine Sortierreihenfolge aus, die mit der PowerCenter Integration Service-Codepage kompatibel ist. Um die Codepage-Validierung zu lockern, legen Sie im PowerCenter Integration Service fest, dass die Codepage-Validierung im Unicode-Datenverschiebungsmodus gelockert wird.

Ich habe versucht, den Sitzungs- und Arbeitsablauf-Log anzuzeigen, aber sie enthalten nur unlesbare Zeichen.

Der PowerCenter Integration Service ist nicht für das Schreiben von Sitzungs- und Arbeitsablauf-Logs mit dem UTF-16LE Zeichensatz konfiguriert.

Aktivieren Sie die Option `LogInUTF8` in den Eigenschaften des PowerCenter Integration Service.

PowerCenter Codepage-Umwandlung

Wenn im Datenverschiebungsmodus Unicode festgelegt ist, akzeptiert der PowerCenter-Client Eingaben in jeder Sprache und wandelt sie in UCS-2 um. Der PowerCenter Integration Service konvertiert Quelldaten vor der Verarbeitung in UCS-2 und wandelt die verarbeiteten Daten vor dem Laden von UCS-2 in die Target-Codepage um.

In einer Sitzung wandelt der PowerCenter Integration Service Quell-, Target- und Lookup-Abfragen von der PowerCenter-Repository-Codepage in die Quell-, Target- oder Lookup-Codepage um. Der PowerCenter Integration Service konvertiert auch den Namen und den Aufrufstext gespeicherter Prozeduren von der PowerCenter-Repository-Codepage in die Codepage der Datenbank der gespeicherten Prozedur um.

Zur Laufzeit überprüft der PowerCenter Integration Service, ob er die folgenden Abfragen und Prozedurentexte von der PowerCenter-Repository-Codepage ohne Datenverlust konvertieren kann:

- Quellabfrage. Muss in Quelldatenbank-Codepage konvertieren.
- Lookup-Abfrage. Muss in Lookup-Datenbank-Codepage konvertieren.
- Target-SQL-Abfrage. Muss in Target-Datenbank-Codepage konvertieren.
- Name und Aufrufstext gespeicherter Prozeduren. Muss in Codepage der Datenbank der gespeicherten Prozedur konvertieren.

Auswählen von Zeichen für PowerCenter Repository Metadaten

Bei der Eingabe von Metadaten ins PowerCenter-Repository können Sie beliebige Zeichen der PowerCenter-Repository-Codepage verwenden. Nutzt das PowerCenter-Repository UTF-16LE, können beliebige Unicode-Zeichen eingegeben werden. In einem für UTF-16LE aktivierten PowerCenter-Repository können Sie beispielsweise deutsche, japanische und englische Metadaten speichern. Es muss jedoch gewährleistet sein, dass der PowerCenter Integration Service erfolgreich SQL-Transaktionen mit Quell-, Target-, Lookup- und gespeicherten Prozedurdatenbanken abwickeln kann. Außerdem müssen Sie sicherstellen, dass der PowerCenter Integration Service aus Quell- und Lookup-Dateien lesen und in Target- und Lookup-Dateien schreiben kann. Daher müssen Sie beim Ausführen einer Sitzung darauf achten, dass die Zeichen der PowerCenter-Repository-Metadaten in den Quell-, Target-, Lookup- und gespeicherten Prozedur-Codepages kodiert sind.

Beispiel

PowerCenter Integration Service, PowerCenter-Repository und PowerCenter-Client nutzen die ISO 8859-1 Latin1 Codepage und die Quelldatenbank enthält anhand der Shift-JIS-Codepage kodierte japanische Daten. Jede Codepage enthält Zeichen, die nicht in einer anderen kodiert sind. Werden andere Zeichen als 7-Bit-

ASCII für PowerCenter-Repository und Quelldatenbank-Metadaten verwendet, kann die Sitzung in folgenden Situationen fehlschlagen oder dazu führen, dass keine Zeilen in das Target geladen werden:

- Sie erstellen ein Mapping, das ein String-Literal mit speziellen Zeichen des deutschen Sprachbereichs nach ISO 8859-1 in einer Abfrage enthält. Die Quelldatenbank kann die Abfrage zurückweisen oder inkonsistente Ergebnisse zurückgeben.
- Sie erstellen mit dem PowerCenter-Client SQL-Abfragen mit speziellen Zeichen des deutschen Sprachbereichs nach ISO 8859-1. Die Quelldatenbank kann die spezifisch deutschen Zeichen der ISO 8859-1 Codepage nicht in die Shift-JIS-Codepage konvertieren.
- Die Quelldatenbank hat einen Tabellennamen, der japanische Zeichen enthält. Der PowerCenter-Designer kann die japanischen Zeichen der Quelldatenbank-Codepage nicht in diejenigen der Codepage des PowerCenter-Client konvertieren. Stattdessen importiert der PowerCenter-Designer die japanischen Zeichen als Fragezeichen (?) und ändert so den Namen der Tabelle. Der PowerCenter Repository Service speichert den Namen der Quelltable als Fragezeichen im PowerCenter-Repository. Sendet der PowerCenter Integration Service eine Abfrage an die Quelldatenbank mit dem geänderten Tabellennamen, kann die Quelldatenbank die richtige Tabelle nicht finden und gibt keine Zeilen oder einen Fehler an den PowerCenter Integration Service zurück, so dass die Sitzung fehlschlägt.

Da die US-ASCII-Codepage eine Teilmenge der Codepages ISO 8859-1 und Shift-JIS ist, können Sie diese Dateninkonsistenzen vermeiden, indem Sie für Ihre sämtlichen Metadaten 7-Bit-ASCII-Zeichen verwenden.

Fallstudie: ISO 8859-1 Datenverarbeitung

Diese Fallstudie beschreibt, wie Sie eine Umgebung zur Verarbeitung von ISO 8859-1 Multibyte-Daten einrichten können. So können Sie Ihre Umgebung konfigurieren, wenn Sie Daten verschiedener westeuropäischer Sprachen mit Zeichensätzen der ISO 8859-1 Codepage verarbeiten müssen. Dieses Beispiel beschreibt eine Umgebung zur Verarbeitung von Daten in englischer und deutscher Sprache.

In dieser Fallstudie umfasst die ISO 8859-1 Umgebung folgende Elemente:

- PowerCenter Integration Service auf einem UNIX-System
- PowerCenter Client auf einem Windows-System, erworben in den Vereinigten Staaten
- PowerCenter Repository gespeichert in einer Oracle-Datenbank unter UNIX
- Quelldatenbank mit Daten in englischer Sprache
- Weitere Quelldatenbank mit Daten in deutscher und englischer Sprache
- Target-Datenbank mit Daten in deutscher und englischer Sprache
- Lookup-Datenbank mit englischsprachigen Daten

Die Datenumgebung muss englische und deutsche Zeichendaten verarbeiten.

Die ISO 8859-1-Umgebung

Die Datenumgebung muss englische und deutsche Zeichendaten verarbeiten.

ISO 8859-1 Umgebung konfigurieren

Verwenden Sie die folgenden Richtlinien, wenn Sie eine Umgebung ähnlich wie in diesem Beispiel für die ISO 8859-1 Datenverarbeitung konfigurieren möchten:

1. Stellen Sie die Codepage-Kompatibilität zwischen dem PowerCenter Repository Datenbank-Client und dem Datenbankserver sicher.
2. Stellen Sie die Codepage-Kompatibilität zwischen dem PowerCenter Client und dem PowerCenter Repository sicher sowie zwischen dem PowerCenter Integration Dienstprozess und dem PowerCenter Repository.
3. Setzen Sie den Datenverschiebungsmodus des PowerCenter Integration Service auf ASCII.
4. Überprüfen Sie die Kompatibilität der Sitzungs-Codepage.
5. Prüfen Sie die Codepage-Kompatibilität für die Lookup- und Gespeicherte-Prozeduren-Datenbank.
6. Stellen Sie die Codepage-Kompatibilität externer Prozeduren oder benutzerdefinierter Transformationsprozeduren sicher.
7. Konfigurieren Sie die Sortierreihenfolge einer Sitzung.

Schritt 1. Verifizieren der Kompatibilität von PowerCenter Repository Database Client und Server

Der Datenbank-Client und Server, die das PowerCenter Repository hosten, müssen in der Lage sein, ohne Datenverlust zu kommunizieren.

Das PowerCenter Repository befindet sich in einer Oracle-Datenbank. Benutzen Sie die Umgebungsvariable `NLS_LANG`, um das Gebietsschema (Sprache, Region und Zeichensatz) festzulegen, das der Datenbank-Client und -Server bei der Anmeldung verwenden sollen:

```
NLS_LANG = LANGUAGE_TERRITORY.CHARACTERSET
```

Standardmäßig konfiguriert Oracle `NLS_LANG` für US-Englisch, das US-Territorium, und den 7-Bit ASCII-Zeichensatz:

```
NLS_LANG = AMERICAN_AMERICA.US7ASCII
```

Ändern Sie die Standard-Konfiguration, um ISO 8859-1-Daten mit der Oracle `WE8ISO8859P1` Codepage in das PowerCenter Repository zu schreiben. Beispiel:

```
NLS_LANG = AMERICAN_AMERICA.WE8ISO8859P1
```

Weitere Informationen zum Überprüfen und Ändern der PowerCenter Repository Database-Codepage finden Sie in Ihrer Datenbank-Dokumentation.

Schritt 2. Stellen Sie die PowerCenter Codepage-Kompatibilität sicher

PowerCenter Integration Service und PowerCenter-Client-Codepages müssen Teilmengen der PowerCenter Repository Codepage sein. Da der PowerCenter-Client und PowerCenter Integration Service jeweils die System-Codepages des Computers verwenden, auf denen sie installiert sind, müssen Sie überprüfen, ob die System-Codepages Teilmengen der PowerCenter Repository Codepage sind.

In diesem Fall wurde der PowerCenter-Client auf Windows-Systemen in den Vereinigten Staaten gekauft. Daher sind die System-Codepages für die PowerCenter-Client-Computer auf MS Windows Latin1 eingestellt. Um System- und Bildschirmsprachen zu überprüfen, öffnen Sie das Dialogfeld "Regionale Einstellungen" in der Windows-Systemsteuerung. Für Systeme, die in den Vereinigten Staaten erworben wurden, müssen die Ländereinstellungen und Eingabegebietsschemata für Englisch (USA) konfiguriert werden.

Der PowerCenter Integration Service ist auf einem UNIX-Rechner installiert. Die Standard-Codepage für das UNIX-Betriebssysteme ist ASCII. In dieser Umgebung ändern Sie die UNIX-System-Codepage auf ISO 8859-1 Western European, sodass sie eine Teilmenge der PowerCenter Repository-Codepage ist.

Schritt 3. Konfigurieren des PowerCenter Integration Service für den ASCII-Datenverschiebungsmodus

Konfigurieren Sie den PowerCenter Integration Service für die Verarbeitung von ISO 8859-1 Daten. Im Administrator Tool setzen Sie den Datenverschiebungsmodus für den PowerCenter Integration Service auf ASCII.

Schritt 4. Stellen Sie die Sitzungs-Codepage-Kompatibilität sicher

Wenn Sie einen Arbeitsablauf im ASCII-Datenverschiebungsmodus ausführen, erzwingt der PowerCenter Integration Service Quell- und Target-Codepage-Beziehungen. Um genaue Datenumwandlungen zu gewährleisten, muss die Quell-Codepage eine Teilmenge der Target-Codepage sein.

In diesem Fall enthält die Umgebung eine Quelldatenbank mit deutschen und englischen Daten. Wenn Sie eine Quelldatenbank-Verbindung im PowerCenter Workflow Manager konfigurieren, muss die Codepage für die Verbindung mit der Quelldatenbank-Codepage identisch und eine Teilmenge der Target-Codepage sein. Da sowohl die Codepage MS Windows Latin1 und die Codepage ISO 8859-1 Western European deutsche Umlaute enthalten, würden Sie wahrscheinlich eine dieser Codepages für die Quelldatenbank-Verbindungen verwenden.

Da die Target-Codepage eine Obermenge der Quell-Codepages sein muss, müssen Sie für die Targetdatenbank-Verbindungen entweder MS Windows Latin1, ISO-8859-1 Western European oder UTF-16LE oder flache Dateien verwenden. Um Datenkonsistenz zu gewährleisten, muss die konfigurierte Target-Codepage der Targetdatenbank oder Einfachdatei-System-Codepage entsprechen.

Wenn Sie den PowerCenter Integration Service für entspannte Codepage-Validierung konfigurieren, entfernt der PowerCenter Integration Service Einschränkungen bei der Kompatibilität von Quell- und Target-Codepages. Sie können für Quell- und Targetdaten eine beliebige unterstützte Codepage auswählen. Sie müssen jedoch sicherstellen, dass die Targets nur Zeichendaten erhalten, die in der Target-Codepage codiert wurden.

Schritt 5. Verifizieren der Codepage-Kompatibilität für Lookup-Datenbank und Datenbank der gespeicherten Prozedur

Die Codepages der Lookup-Datenbank und der Datenbank für die gespeicherten Prozeduren müssen eine Obermenge der Quell-Codepages und eine Untermenge der Target-Codepages sein. In diesem Fall müssen alle Verbindungen zu Lookup- und Gespeicherte-Prozeduren-Datenbanken eine Codepage verwenden, die mit den Codepages ISO 8859-1 Western European oder MS Windows Latin1 kompatibel ist.

Schritt 6. Kompatibilität externer Prozedur oder benutzerdefinierter Umwandlungsprozedur prüfen

Die externen Prozedur und die benutzerdefinierten Umwandlungsprozeduren müssen die Zeichendaten aus den Quell-Codepages verarbeiten können, und sie müssen die Zeichen übergeben, die in den Target-Codepages kompatibel sind. In diesem Fall müssen alle Daten, die von externen Prozeduren oder benutzerdefinierten Umwandlungsprozeduren verarbeitet werden, den Codepages ISO 8859-1 Western European oder MS Windows Latin1 entsprechen.

Schritt 7. Konfigurieren der Sitzungs-Sortierreihenfolge

Wenn Sie den PowerCenter Integration Service im ASCII-Modus ausführen, verwendet er für alle Sitzungen eine binäre Sortierreihenfolge. In den Sitzungseigenschaften listet der PowerCenter Workflow Manager alle Sortierreihenfolgen auf, die zur Codepage des PowerCenter Integration Service gehören. Sie können eine Sortierreihenfolge für die Sitzung auswählen.

Fallstudie: Verarbeiten von Unicode UTF-16LE Daten

Diese Fallstudie beschreibt, wie Sie eine Umgebung zur Verarbeitung von Unicode UTF-16LE Multibyte-Daten einrichten können. Wenn Sie Daten westeuropäischer Sprachen, Sprachen aus dem mittleren Osten oder Asien bzw. anderer im UTF-16LE Zeichensatz verschlüsselter Sprachen zu verarbeiten haben, werden Sie Ihre Umgebung möglicherweise so konfigurieren. In diesem Beispiel wird eine Umgebung beschrieben, die Daten in deutscher und japanischer Sprache verarbeitet.

In dieser Fallstudie besteht die UTF-16LE Umgebung aus folgenden Elementen:

- PowerCenter Integration Service auf einem UNIX-Computer
- PowerCenter Clients auf Windows-Systemen
- PowerCenter Repository, gespeichert in einer Oracle-Datenbank auf UNIX
- Eine Quelldatenbank mit Daten in deutscher Sprache
- Eine Quelldatenbank mit Daten in deutscher und japanischer Sprache
- Eine Target-Datenbank mit Daten in deutscher und japanischer Sprache
- Eine Lookup-Datenbank mit deutschsprachigen Daten

Die Datenumgebung muss Daten bestehend aus deutschen und japanischen Schriftzeichen verarbeiten können.

Die UTF-8-Umgebung

Die Datenumgebung muss Daten bestehend aus deutschen und japanischen Schriftzeichen verarbeiten können.

UTF-16LE Umgebung konfigurieren

Verwenden Sie die folgenden Richtlinien, wenn Sie eine Umgebung ähnlich wie in diesem Beispiel für die UTF-16LE Datenverarbeitung konfigurieren möchten:

1. Stellen Sie die Codepage-Kompatibilität zwischen dem PowerCenter Repository Datenbank-Client und dem Datenbankserver sicher.
2. Stellen Sie die Codepage-Kompatibilität zwischen dem PowerCenter Client und dem PowerCenter Repository sicher sowie zwischen dem PowerCenter Integration Service und dem PowerCenter Repository.
3. Konfigurieren Sie den PowerCenter Integration Service für Unicode-Datenverschiebungsmodus.
4. Überprüfen Sie die Kompatibilität der Sitzungs-Codepage.
5. Prüfen Sie die Codepage-Kompatibilität für die Lookup- und Gespeicherte-Prozeduren-Datenbank.
6. Stellen Sie die Codepage-Kompatibilität externer Prozeduren oder benutzerdefinierter Transformationsprozeduren sicher.

7. Konfigurieren Sie die Sortierreihenfolge einer Sitzung.

Schritt 1. Stellen Sie die Kompatibilität von PowerCenter Repository Database Client und Server sicher

Der Datenbank-Client und Server, die das PowerCenter Repository hosten, müssen in der Lage sein, ohne Datenverlust zu kommunizieren.

Das PowerCenter Repository befindet sich in einer Oracle-Datenbank. Stellen Sie die Umgebungsvariable NLS_LANG auf das Gebietsschema (Sprache, Region und Zeichensatz) ein, das Datenbank-Client und Server bei der Anmeldung verwenden sollen.

```
NLS_LANG = LANGUAGE_TERRITORY.CHARACTERSET
```

Standardmäßig konfiguriert Oracle NLS_LANG für US-Englisch, das US-Territorium, und den 7-Bit ASCII-Zeichensatz:

```
NLS_LANG = AMERICAN_AMERICA.US7ASCII
```

Ändern Sie die Standard-Konfiguration, um UTF-16LE Daten mit dem Oracle UTF8-Zeichensatz in das PowerCenter Repository zu schreiben. Beispiel:

```
NLS_LANG = AMERICAN_AMERICA.UTF8
```

Weitere Informationen zum Überprüfen und Ändern der PowerCenter Repository Database-Codepage finden Sie in Ihrer Datenbank-Dokumentation.

Schritt 2. Stellen Sie die PowerCenter Codepage-Kompatibilität sicher

PowerCenter Integration Service und PowerCenter-Client-Codepages müssen Teilmengen der PowerCenter Repository Codepage sein. Da der PowerCenter-Client und PowerCenter Integration Service jeweils die System-Codepages des Computers verwenden, auf denen sie installiert sind, müssen Sie überprüfen, ob die System-Codepages Teilmengen der PowerCenter Repository Codepage sind.

In diesem Fall wurden der PowerCenter-Client auf Windows-Systemen in der Schweiz gekauft. Daher sind die System-Codepages für die PowerCenter-Client-Computer auf MS Windows Latin1 eingestellt. Um System- und Bildschirmsprachen zu überprüfen, öffnen Sie das Dialogfeld "Regionale Einstellungen" in der Windows-Systemsteuerung.

Der PowerCenter Integration Service ist auf einem UNIX-Rechner installiert. Die Standard-Codepage für das UNIX-Betriebssysteme ist ASCII. In dieser Umgebung muss der UNIX-System-Zeichensatz auf UTF-16LE geändert werden.

Schritt 3. Konfigurieren des PowerCenter Integration Service für den Unicode-Datenverschiebungsmodus

Sie müssen den PowerCenter Integration Service für die Verarbeitung von UTF-16LE Daten konfigurieren. Im Administrator Tool setzen Sie den Datenverschiebungsmodus für den PowerCenter Integration Service auf Unicode. Der PowerCenter Integration Service ordnet bei der Verarbeitung von Multibyte-Zeichen jedem Zeichen ein zusätzliches Byte zu.

Schritt 4. Stellen Sie die Sitzungs-Codepage-Kompatibilität sicher

Wenn Sie einen PowerCenter-Arbeitsablauf im Unicode-Datenverschiebungsmodus ausführen, erzwingt der PowerCenter Integration Service Quell- und Target-Codepage-Beziehungen. Um genaue Datenumwandlungen zu gewährleisten, muss die Quell-Codepage eine Teilmenge der Target-Codepage sein.

In diesem Fall enthält die Umgebung eine Quelldatenbank mit deutschen und japanischen Daten. Wenn Sie eine Quelldatenbank-Verbindung im PowerCenter Workflow Manager konfigurieren, muss die Codepage für die Verbindung mit der Quelldatenbank-Codepage identisch sein. Sie können jede Codepage für die Quelldatenbank verwenden.

Da die Target-Codepage eine Obermenge der Quell-Codepages sein muss, müssen Sie für die Target-Datenbank-Verbindungen UTF-16LE oder Einfachdateien verwenden. Um Datenkonsistenz zu gewährleisten, muss die konfigurierte Target-Codepage der Target-Datenbank oder Einfachdatei-Systemcodepage entsprechen.

Wenn Sie den PowerCenter Integration Service für entspannte Codepage-Validierung konfigurieren, entfernt der PowerCenter Integration Service Einschränkungen bei der Kompatibilität von Quell- und Target-Codepages. Sie können für Quell- und Targetdaten eine beliebige unterstützte Codepage auswählen. Sie müssen jedoch sicherstellen, dass die Targets nur Zeichendaten erhalten, die in der Target-Codepage codiert wurden.

Schritt 5. Verifizieren der Codepage-Kompatibilität für Lookup-Datenbank und Datenbank der gespeicherten Prozedur

Die Codepages der Lookup-Datenbank und der Datenbank für die gespeicherten Prozeduren müssen eine Obermenge der Quell-Codepages und eine Untermenge der Target-Codepages sein. In diesem Fall müssen alle Verbindungen zu Lookup- und Gespeicherte-Prozeduren-Datenbanken eine Codepage verwenden, die mit UTF-16LE kompatibel ist.

Schritt 6. Kompatibilität externer Prozedur oder benutzerdefinierter Umwandlungsprozedur prüfen

Die externen Prozedur und die benutzerdefinierten Umwandlungsprozeduren müssen die Zeichendaten aus den Quell-Codepages verarbeiten können, und sie müssen die Zeichen übergeben, die in den Target-Codepages kompatibel sind.

In diesem Fall müssen die externe Prozedur und die benutzerdefinierten Umwandlungen die deutschen und japanischen Daten aus den Quellen verarbeiten können. Der PowerCenter Integration Service übergibt die Daten an Prozeduren jedoch in UCS-2. Aus diesem Grund müssen alle Daten, die von einer externen Prozedur oder von benutzerdefinierten Umwandlungen verarbeitet werden, dem Zeichensatz UCS-2 entsprechen.

Schritt 7. Konfigurieren der Sitzungs-Sortierreihenfolge

Wenn Sie den PowerCenter Integration Service im Unicode-Modus ausführen, verwendet er für alle Sitzungen die festgelegte Sortierreihenfolge. Standardmäßig sind die Sitzungen für eine binäre Sortierreihenfolge konfiguriert.

Um deutsche und japanische Daten zu sortieren, wenn der PowerCenter Integration Service UTF-16LE verwendet, empfiehlt es sich die binäre Sortierreihenfolge beizubehalten.

KAPITEL 15

Informatica Cloud-Verwaltung

Dieses Kapitel umfasst die folgenden Themen:

- [Informatica Cloud-Verwaltung - Übersicht , 279](#)
- [Informatica Cloud-Organisationen , 279](#)
- [Informatica Cloud-Sicherheitsagent, 281](#)
- [Informatica Cloud-Verbindungen, 281](#)

Informatica Cloud-Verwaltung - Übersicht

Wenn Sie Informatica Cloud verwenden, können Sie die Details Ihrer Informatica Cloud-Organisation im Administrator-Tool hinzufügen.

Sie können die Details der Organisationen auf der Registerkarte **Cloud** überprüfen. Sie müssen über ausreichende Berechtigungen zum Anzeigen der Registerkarte **Cloud** verfügen.

Sie können Organisationen im Administrator-Tool hinzufügen oder entfernen. Nachdem Sie eine Organisation hinzugefügt haben, können Sie die Sicherheitsagenten und Informatica Cloud-Verbindungen in der Organisation anzeigen. Ein Sicherheitsagent ist ein leichtes Programm, das alle Aufgaben ausführt und die sichere Kommunikation an der gesamten Firewall zwischen Ihrem Unternehmen und Informatica Cloud ermöglicht. Informatica Cloud-Verbindungen sind die Verbindungen, die Benutzer in der Organisation erstellen, um auf Daten in verschiedenen Datenquellen zuzugreifen.

Sie können den Status von Sicherheitsagenten überwachen und die Eigenschaften von Organisationen, Sicherheitsagenten und Verbindungen anzeigen. Im Administrator-Tool können Sie keine Änderungen an Organisationen, Sicherheitsagenten oder Verbindungen vornehmen.

Informatica Cloud-Organisationen

Eine Informatica Cloud-Organisation ist ein sicherer Bereich innerhalb des Informatica Cloud-Repository, in dem Sie Daten und Objekte speichern.

Ihr Unternehmen kann je nach Bedarf mehrere Organisationen erstellen. Beispiel: Der Informatica Cloud-Administrator könnte eine Sandbox-Organisation und eine Produktionsorganisation erstellen. Eine Organisation kann außerdem mehrere Unterorganisationen umfassen. Im Administrator-Tool können Sie Organisationen hinzufügen, um Eigenschaften der Organisationen, Sicherheitsagenten und Verbindungen anzuzeigen und den Status von Sicherheitsagenten zu überwachen.

Im Administrator-Tool können Sie keine Eigenschaften der Organisation ändern.

Hinweis: Wenn die Anmeldedaten der Organisation ablaufen oder wenn ein Problem mit der Konnektivität zu Informatica Cloud besteht, wird der Name der Organisation als „Nicht identifiziert“ angezeigt.

Eigenschaften der Informatica Cloud-Organisation

Im Administrator-Tool können Sie die Eigenschaften von Organisationen anzeigen.

Sie können die folgenden Details einer Organisation anzeigen:

Details zum Unternehmen

Angaben zur Organisation, wie z. B. Name und Adresse.

Unternehmenseigenschaften

Die mit der Organisation verbundenen Eigenschaften, wie z. B. Erstellungsdatum und Organisations-ID.

Standardmäßige E-Mail-Benachrichtigungsoptionen

Die Standard-E-Mail-Adressen für den Empfang von Job-Benachrichtigungen.

Authentifizierungsoptionen

Die von der Organisation verwendeten Authentifizierungsdetails.

Unterorganisationen

Die Liste der mit der Organisation verbundenen Unterorganisationen.

Hinzufügen einer Organisation

Zum Hinzufügen einer Organisation im Administrator-Tool müssen Sie über ausreichende Berechtigungen verfügen.

1. Klicken Sie auf die Registerkarte **Cloud**.
2. Wählen Sie im Menü **Aktionen** die Option **Unternehmen hinzufügen**.
3. Geben Sie den Benutzernamen und das Passwort der Informatica Cloud-Organisation ein.
Der Informatica Cloud-Benutzer muss über Administratorberechtigungen in der Organisation verfügen.
4. Klicken Sie auf **OK**.

Entfernen einer Organisation

Sie können eine Organisation entfernen, wenn Sie über ausreichende Berechtigungen verfügen.

1. Klicken Sie auf die Registerkarte **Cloud**.
2. Wählen Sie im Menü **Aktionen** die Option **Unternehmen hinzufügen**.
Das Dialogfeld **Organisation entfernen** wird angezeigt.
3. Klicken Sie auf **Ja**.

Bearbeiten von Informatica Cloud-Anmeldedaten

Sie können die Informatica Cloud-Anmeldedaten einer Organisation verwenden, um neue Anmeldedaten zu verwenden oder wenn die vorhandenen Anmeldedaten abgelaufen sind.

1. Klicken Sie auf die Registerkarte **Cloud**.
2. Wählen Sie die Organisation.

3. Wählen Sie im Menü **Aktionen** die Option **Anmeldung bearbeiten**.
Das Dialogfeld **Anmeldedaten bearbeiten** wird angezeigt.
4. Wählen Sie **Passwort ändern**, um das Passwort zu aktualisieren.
5. Geben Sie die neuen Anmeldedaten an.
6. Klicken Sie auf **OK**.

Informatica Cloud-Sicherheitsagent

Der Informatica Cloud-Sicherheitsagent ist ein Lightweight-Programm, das alle Aufgaben ausführt und die sichere Kommunikation in der Firewall zwischen Ihrer Organisation und Informatica Cloud ermöglicht.

Nach dem Hinzufügen einer Organisation im Administrator-Tool können Sie die mit der Organisation verbundenen Sicherheitsagenten anzeigen. Sie können den Status von Sicherheitsagenten über Informatica Cloud überwachen und dort entsprechende Aktionen ausführen. Sie können auch die Eigenschaften eines Sicherheitsagenten anzeigen.

Erweitern Sie im Navigator der Registerkarte **Cloud** eine Organisation und wählen Sie **Sicherheitsagenten**, um die Liste der Sicherheitsagenten anzuzeigen.

Sie können die folgenden Details eines Sicherheitsagenten im Administrator-Tool anzeigen:

- Details zum Sicherheitsagenten
- Versionsdetails zum Sicherheitsagenten
- Paketdetails
- Konfigurationsdetails zum Sicherheitsagenten
- Weitere Eigenschaften

Informatica Cloud-Verbindungen

Eine Informatica Cloud-Verbindung ist ein Informatica Cloud-Objekt, das Sie konfigurieren, um eine Verbindung zu Cloud- und lokalen Anwendungen, Plattformen, Datenbanken und Einfachdateien herzustellen.

Nach dem Hinzufügen einer Organisation im Administrator-Tool können Sie die Verbindungen, die Sie für die Organisation konfiguriert haben, in Informatica Cloud anzeigen.

Erweitern Sie im Navigator der Registerkarte **Cloud** eine Organisation und wählen Sie **Verbindungen**, um die Liste der Verbindungen im rechten Bereich anzuzeigen.

Sie können die folgenden Details einer Cloud-Verbindung im Administrator-Tool anzeigen:

- Verbindungsdetails
- Verbindungseigenschaften

ANHANG A

Codepages

Dieser Anhang umfasst die folgenden Themen:

- [Unterstützte Codepages für Anwendungsdienste, 282](#)
- [Unterstützte Codepages für Quellen und Ziele, 284](#)

Unterstützte Codepages für Anwendungsdienste

Informatica unterstützt die Codepages aus Gründen der Internationalisierung. Zum globalen Support verwendet Informatica die internationalen Komponenten für Unicode (ICU). Eine Liste der Codepage-Aliase in ICU finden Sie unter <http://demo.icu-project.org/icu-bin/convexp>.

Wenn Sie im Administrator-Tool eine Anwendungsdienst-Codepage zuweisen, wählen Sie die Codepage-Beschreibung aus.

Sie müssen mit UTF-8 kompatible Codepages für die Domäne, den Modellrepository-Dienst und für jeden Datenintegrationsdienst-Prozess verwenden.

Die nachstehende Tabelle gibt den Namen, eine Beschreibung und die ID für die unterstützten Codepages für PowerCenter-Repository-Dienst, Metadata Manager-Dienst und jeden PowerCenter-Integrationsdienst-Prozess an:

Name	Beschreibung	ID
IBM-037	IBM EBCDIC US Englisch	2028
IBM-1047	IBM EBCDIC US Englisch IBM1047	1047
IBM-273	IBM EBCDIC Deutsch	2030
IBM-280	IBM EBCDIC Italienisch	2035
IBM-285	IBM EBCDIC UK Englisch	2038
IBM-297	IBM EBCDIC Französisch	2040
IBM-500	IBM EBCDIC Internationales Lateinisch-1	2044
IBM-930	IBM EBCDIC Japanisch	930

Name	Beschreibung	ID
IBM-935	IBM EBCDIC Vereinfachtes Chinesisch	935
IBM-937	IBM EBCDIC Traditionelles Chinesisch	937
IBM-939	IBM EBCDIC Japanisch CP939	939
ISO-8859-10	ISO 8859-10 Lateinisch 6 (Nordisch)	13
ISO-8859-15	ISO 8859-15 Lateinisch 9 (Westeuropäisch)	201
ISO-8859-2	ISO 8859-2 Osteuropäisch	5
ISO-8859-3	ISO 8859-3 Süd-osteuropäisch	6
ISO-8859-4	ISO 8859-4 Baltisch	7
ISO-8859-5	ISO 8859-5 Kyrillisch	8
ISO-8859-6	ISO 8859-6 Arabisch	9
ISO-8859-7	ISO 8859-7 Griechisch	10
ISO-8859-8	ISO 8859-8 Hebräisch	11
ISO-8859-9	ISO 8859-9 Lateinisch 5 (Türkisch)	12
JapanEUC	Japanische erweiterte UNIX-Codierung (einschließlich JIS X 0212)	18
Latin-1	ISO 8859-1 Westeuropäisch	4
MS1250	MS Windows Lateinisch 2 (Zentraleuropa)	2250
MS1251	MS Windows Kyrillisch (Slawisch)	2251
MS1252	MS Windows Lateinisch 1 (ANSI), übergeordneter Zeichensatz von Lateinisch 1	2252
MS1253	MS Windows Griechisch	2253
MS1254	MS Windows Lateinisch 5 (Türkisch), übergeordneter Zeichensatz von ISO 8859-9	2254
MS1255	MS Windows Hebräisch	2255
MS1256	MS Windows Arabisch	2256
MS1257	MS Windows Ostseeanrainer	2257
MS1258	MS Windows Vietnamesisch	2258
MS1361	MS Windows Koreanisch (Johab)	1361
MS874	MS-DOS Thailändisch, übergeordneter Zeichensatz von TIS 620	874

Name	Beschreibung	ID
MS932	MS Windows Japanisch, Umsch-JIS	2024
MS936	MS Windows Vereinfachtes Chinesisch, übergeordneter Zeichensatz von GB 2312-80, EUC Codierung	936
MS949	MS Windows Koreanisch, übergeordneter Zeichensatz von KS C 5601-1992	949
MS950	MS Windows Traditionelles Chinesisch, übergeordneter Zeichensatz von Big 5	950
US-ASCII	7-Bit-ASCII	1
UTF-8	UTF 8-Kodierung von Unicode	106

Unterstützte Codepages für Quellen und Ziele

Informatica unterstützt die Codepages aus Gründen der Internationalisierung. Zum globalen Support verwendet Informatica die internationalen Komponenten für Unicode (ICU). Eine Liste der Codepages-Aliase in ICU finden Sie unter <http://demo.icu-project.org/icu-bin/convexp>

Wenn Sie im PowerCenter Client eine Quelle oder ein Ziel zuweisen, wählen Sie die Codepage-Beschreibung aus. Wenn Sie eine Codepage mit dem Befehl *pmrep* CreateConnection zuweisen oder die Codepage in einer Parameterdatei definieren, geben Sie den Codepage-Namen ein. Die nachstehende Tabelle gibt den Namen, eine Beschreibung und die ID für die unterstützten Codepages für Quellen und Ziele an:

Name	Beschreibung	ID
Adobe-Standard-Encoding	Adobe Standardcodierung	10073
BOCU-1	Binär geordnete Komprimierung für Unicode (BOCU-1)	10010
CESU-8	ICompatibility Codierungsschema für UTF-16 (CESU-8)	10011
cp1006	ISO Urdu	10075
cp1098	PC Farsi	10076
cp1124	ISO Kyrillisch Ukraine	10077
cp1125	PC Kyrillisch Ukraine	10078
cp1131	PC Kyrillisch Weißrussland	10080
cp1381	PC Chinesisch GB (S-Ch Mischdaten)	10082
cp850	PC Lateinisch1	10036

Name	Beschreibung	ID
cp851	PC DOS Griechisch (ohne Euro)	10037
cp856	PC Hebräisch (alt)	10040
cp857	PC Lateinisch5 (ohne Euroaktualisierung)	10041
cp858	PC Lateinisch1 (mit Euroaktualisierung)	10042
cp860	PC Portugal	10043
cp861	PC Island	10044
cp862	PC Hebräisch (ohne Euroaktualisierung)	10045
cp863	PC Kanadisches Französisch	10046
cp864	PC Arabisch (ohne Euroaktualisierung)	10047
cp865	PC Nordisch	10048
cp866	PC Russisch (ohne Euroaktualisierung)	10049
cp868	PC Urdu	10051
cp869	PC Griechisch (ohne Euroaktualisierung)	10052
cp922	IPC Estnisch (ohne Euroaktualisierung)	10056
cp949c	PC Koreanisch - KS	10028
ebcdic-xml-us	EBCDIC US (mit Euro) - Erweiterung für XML4C(Xerces)	10180
EUC-KR	EUC Koreanisch	10029
GB_2312-80	Vereinfachtes Chinesisch (GB2312-80)	10025
gb18030	GB 18030 MBCS Codepage	1392
GB2312	Chinesisches EUC	10024
HKSCS	Hongkong erweiterter Zeichensatz	9200
hp-roman8	HP Lateinisch1	10072
HZ-GB-2312	Vereinfachtes Chinesisch (HZ GB2312)	10092
IBM-037	IBM EBCDIC US Englisch	2028
IBM-1025	EBCDIC Kyrrillisch	10127
IBM-1026	EBCDIC Türkei	10128
IBM-1047	IBM EBCDIC US Englisch IBM1047	1047

Name	Beschreibung	ID
IBM-1047-s390	EBCDIC IBM-1047 für S/390 (LF und NL zwischengespeichert)	10167
IBM-1097	EBCDIC Farsi	10129
IBM-1112	EBCDIC Baltisch	10130
IBM-1122	EBCDIC Estland	10131
IBM-1123	EBCDIC Kyrillisch Ukraine	10132
IBM-1129	ISO Vietnamesisch	10079
IBM-1130	EBCDIC Vietnamesisch	10133
IBM-1132	EBCDIC Laotisch	10134
IBM-1133	ISO Laotisch	10081
IBM-1137	EBCDIC Devanagari	10163
IBM-1140	EBCDIC US (mit Euroaktualisierung)	10135
IBM-1140-s390	EBCDIC IBM-1140 für S/390 (LF und NL zwischengespeichert)	10168
IBM-1141	EBCDIC Deutschland, Österreich (mit Euroaktualisierung)	10136
IBM-1142	EBCDIC Dänemark, Norwegen (mit Euroaktualisierung)	10137
IBM-1142-s390	EBCDIC IBM-1142 für S/390 (LF und NL zwischengespeichert)	10169
IBM-1143	EBCDIC Finnland, Schweden (mit Euroaktualisierung)	10138
IBM-1143-s390	EBCDIC IBM-1143 für S/390 (LF und NL zwischengespeichert)	10170
IBM-1144	EBCDIC Italien (mit Euroaktualisierung)	10139
IBM-1144-s390	EBCDIC IBM-1144 für S/390 (LF und NL zwischengespeichert)	10171
IBM-1145	EBCDIC Spanien, Lateinamerika (mit Euroaktualisierung)	10140
IBM-1145-s390	EBCDIC IBM-1145 für S/390 (LF und NL zwischengespeichert)	10172
IBM-1146	EBCDIC Großbritannien, Irland (mit Euroaktualisierung)	10141
IBM-1146-s390	EBCDIC IBM-1146 für S/390 (LF und NL zwischengespeichert)	10173
IBM-1147	EBCDIC Frankreich (mit Euroaktualisierung)	10142
IBM-1147-s390	EBCDIC IBM-1147 für S/390 (LF und NL zwischengespeichert)	10174
IBM-1147-s390	EBCDIC IBM-1147 für S/390 (LF und NL zwischengespeichert)	10174
IBM-1148	EBCDIC Internationales Lateinisch1 (mit Euroaktualisierung)	10143

Name	Beschreibung	ID
IBM-1148-s390	EBCDIC IBM-1148 für S/390 (LF und NL zwischengespeichert)	10175
IBM-1149	EBCDIC Island (mit Euroaktualisierung)	10144
IBM-1149-s390	IEBCDIC IBM-1149 für S/390 (LF und NL zwischengespeichert)	10176
IBM-1153	EBCDIC Lateinisch2 (mit Euroaktualisierung)	10145
IBM-1153-s390	EBCDIC IBM-1153 für S/390 (LF und NL zwischengespeichert)	10177
IBM-1154	EBCDIC Mehrsprachiges Kyrillisch (mit Euroaktualisierung)	10146
IBM-1155	EBCDIC Türkei (mit Euroaktualisierung)	10147
IBM-1156	EBCDIC Mehrsprachiges Baltisch (mit Euroaktualisierung)	10148
IBM-1157	EBCDIC Estnisch (mit Euroaktualisierung)	10149
IBM-1158	EBCDIC Kyrillisch Ukraine (mit Euroaktualisierung)	10150
IBM-1159	IBM EBCDIC Taiwan, traditionelles Chinesisch	11001
IBM-1160	EBCDIC Thailändisch (mit Euroaktualisierung)	10151
IBM-1162	Thailändisch (mit Euroaktualisierung)	10033
IBM-1164	EBCDIC Vietnamesisch (mit Euroaktualisierung)	10152
IBM-1250	MS Windows Lateinisch2 (ohne Euroaktualisierung)	10058
IBM-1251	MS Windows Kyrillisch (ohne Euroaktualisierung)	10059
IBM-1255	MS Windows Hebräisch (ohne Euroaktualisierung)	10060
IBM-1256	MS Windows Arabisch (ohne Euroaktualisierung)	10062
IBM-1257	MS Windows Baltisch (ohne Euroaktualisierung)	10064
IBM-1258	MS Windows Vietnamesisch (ohne Euroaktualisierung)	10066
IBM-12712	EBCDIC Hebräisch (aktualisiert für Euro und neuen Shekel, Steuerzeichen)	10161
IBM-12712-s390	EBCDIC IBM-12712 für S/390 (LF und NL zwischengespeichert)	10178
IBM-1277	Adobe Lateinisch1-Codierung	10074
IBM-13121	IBM EBCDIC Erweitertes Koreanisch CP13121	11002
IBM-13124	IBM EBCDIC Vereinfachtes Chinesisch CP13124	11003
IBM-1363	PC Koreanisch KSC MBCS erweitert (mit \ <-> Won-Zuordnung)	10032

Name	Beschreibung	ID
IBM-1364	EBCDIC Erweitertes Koreanisch (SBCS IBM-13121 kombiniert mit DBCS IBM-4930)	10153
IBM-1371	EBCDIC Erweitertes Taiwanesisch (SBCS IBM-1159 kombiniert mit DBCS IBM-9027)	10154
IBM-1373	Taiwan Big-5 (mit Euroaktualisierung)	10019
IBM-1375	MS Taiwan Big-5 mit HKSCS-Erweiterungen	10022
IBM-1386	PC Chinesisch GBK (IBM-1386)	10023
IBM-1388	EBCDIC Chinesisch GB (S-Ch DBCS-Hostdaten)	10155
IBM-1390	EBCDIC Japanisches Katakana (mit Euroaktualisierung)	10156
IBM-1399	EBCDIC Japanisches Lateinisches-Kanji (mit Euroaktualisierung)	10157
IBM-16684	EBCDIC Erweitertes Japanisch (DBCS IBM-1390 kombiniert mit DBCS IBM-1399)	10158
IBM-16804	EBCDIC Arabisch (mit Euroaktualisierung)	10162
IBM-16804-s390	EBCDIC IBM-16804 für S/390 (LF und NL zwischengespeichert)	10179
IBM-25546	ISO-2022 Codierung für Koreanisch (Erweiterung 1)	10089
IBM-273	IBM EBCDIC Deutsch	2030
IBM-277	EBCDIC Dänemark, Norwegen	10115
IBM-278	EBCDIC Finnland, Schweden	10116
IBM-280	IBM EBCDIC Italienisch	2035
IBM-284	EBCDIC Spanien, Lateinamerika	10117
IBM-285	IBM EBCDIC UK Englisch	2038
IBM-290	EBCDIC Japanisches Katakana SBCS	10118
IBM-297	IBM EBCDIC Französisch	2040
IBM-33722	Japanisches EUC (mit \ <-> Yen-Zuordnung)	10017
IBM-367	IBM-367	10012
IBM-37-s390	EBCDIC IBM-37 für S/390 (LF und NL zwischengespeichert)	10166
IBM-420	EBCDIC Arabisch	10119
IBM-424	EBCDIC Hebräisch (aktualisiert für neuen Shekel, Steuerzeichen)	10120

Name	Beschreibung	ID
IBM-437	PC USA	10035
IBM-4899	EBCDIC Hebräisch (mit Euroaktualisierung)	10159
IBM-4909	ISO Griechisch (mit Euroaktualisierung)	10057
IBM-4933	IBM Vereinfachtes Chinesisch CP4933	11004
IBM-4971	EBCDIC Griechisch (mit Euroaktualisierung)	10160
IBM-500	IBM EBCDIC Internationales Lateinisch-1	2044
IBM-5050	Japanisches EUC (gepacktes Format)	10018
IBM-5123	EBCDIC Japanisches Lateinisch (mit Euroaktualisierung)	10164
IBM-5351	MS Windows Hebräisch (frühere Version)	10061
IBM-5352	MS Windows Arabisch (frühere Version)	10063
IBM-5353	MS Windows Baltisch (frühere Version)	10065
IBM-803	EBCDIC Hebräisch	10121
IBM-833	IBM EBCDIC Koreanisch CP833	833
IBM-834	IBM EBCDIC Koreanisch CP834	834
IBM-835	IBM Taiwan, traditionelles Chinesisch CP835	11005
IBM-836	IBM EBCDIC Vereinfachtes Chinesisch	11006
IBM-837	IBM Vereinfachtes Chinesisch CP837	11007
IBM-838	EBCDIC Thailändisch	10122
IBM-8482	EBCDIC Japanisches Katakana SBCS (mit Euroaktualisierung)	10165
IBM-852	PC Lateinisch2 (ohne Euroaktualisierung)	10038
IBM-855	PC Kyrillisch (ohne Euroaktualisierung)	10039
IBM-867	PC Hebräisch (mit Euroaktualisierung)	10050
IBM-870	EBCDIC Lateinisch2	10123
IBM-871	EBCDIC Island	10124
IBM-874	PC Thailand (ohne Euroaktualisierung)	10034
IBM-875	EBCDIC Griechisch	10125
IBM-901	PC Baltisch (mit Euroaktualisierung)	10054

Name	Beschreibung	ID
IBM-902	PC Estnisch (mit Euroaktualisierung)	10055
IBM-918	EBCDIC Urdu	10126
IBM-930	IBM EBCDIC Japanisch	930
IBM-933	IBM EBCDIC Koreanisch CP933	933
IBM-935	IBM EBCDIC Vereinfachtes Chinesisch	935
IBM-937	IBM EBCDIC Traditionelles Chinesisch	937
IBM-939	IBM EBCDIC Japanisch CP939	939
IBM-942	PC Japanisch SJIS-78 Syntax (IBM-942)	10015
IBM-943	PC Japanisch SJIS-90 (IBM-943)	10016
IBM-949	PC Koreanisch - KS (Standard)	10027
IBM-950	Taiwan Big-5 (ohne Euroaktualisierung)	10020
IBM-964	EUC Taiwan	10026
IBM-971	EUC Koreanisch (nur DBCS)	10030
IMAP-Mailboxname	IMAP-Mailboxname	10008
is-960	Israelischer Standard 960 (7-Bit Hebräisch-Codierung)	11000
ISO-2022-CN	ISO-2022 Codierung für Chinesisch	10090
ISO-2022-CN-EXT	ISO-2022 Codierung für Chinesisch (Erweiterung 1)	10091
ISO-2022-JP	ISO-2022 Codierung für Japanisch	10083
ISO-2022-JP-2	ISO-2022 Codierung für Japanisch (Erweiterung 2)	10085
ISO-2022-KR	ISO-2022 Codierung für Koreanisch	10088
ISO-8859-10	ISO 8859-10 Lateinisch 6 (Nordisch)	13
ISO-8859-13	ISO 8859-13 PC Baltisch (ohne Euroaktualisierung)	10014
ISO-8859-15	ISO 8859-15 Lateinisch 9 (Westeuropäisch)	201
ISO-8859-2	ISO 8859-2 Osteuropäisch	5
ISO-8859-3	ISO 8859-3 Süd-osteuropäisch	6
ISO-8859-4	ISO 8859-4 Baltisch	7
ISO-8859-5	ISO 8859-5 Kyrillisch	8

Name	Beschreibung	ID
ISO-8859-6	ISO 8859-6 Arabisch	9
ISO-8859-7	ISO 8859-7 Griechisch	10
ISO-8859-8	ISO 8859-8 Hebräisch	11
ISO-8859-9	ISO 8859-9 Lateinisch 5 (Türkisch)	12
JapanEUC	Japanische erweiterte UNIX-Codierung (einschließlich JIS X 0212)	18
JEF	Japanisch EBCDIC Fujitsu	9000
JEF-K	Japanisch EBCDIC-Kana Fujitsu	9005
JIPSE	NEC ACOS JIPSE Japanisch	9002
JIPSE-K	NEC ACOS JIPSE-Kana Japanisch	9007
JIS_Encoding	ISO-2022 Codierung für Japanisch (Erweiterung 1)	10084
JIS_X0201	ISO-2022 Codierung für Japanisch (JIS_X0201)	10093
JIS7	ISO-2022 Codierung für Japanisch (Erweiterung 3)	10086
JIS8	ISO-2022 Codierung für Japanisch (Erweiterung 4)	10087
JP-EBCDIC	EBCDIC Japanisch	9010
JP-EBCDIK	EBCDIK Japanisch	9011
KEIS	HITACHI KEIS Japanisch	9001
KEIS-K	HITACHI KEIS-Kana Japanisch	9006
KOI8-R	IRussisch Internet	10053
KSC_5601	PC Koreanisch KSC MBCS erweitert (KSC_5601)	10031
Latin-1	ISO 8859-1 Westeuropäisch	4
LMBCS-1	Lotus MBCS Codierung für PC Lateinisch1	10103
LMBCS-11	Lotus MBCS Codierung für MS-DOS Thailändisch	10110
LMBCS-16	Lotus MBCS Codierung für Windows Japanisch	10111
LMBCS-17	Lotus MBCS Codierung für Windows Koreanisch	10112
LMBCS-18	Lotus MBCS Codierung für Windows Chinesisch (Traditionell)	10113
LMBCS-19	Lotus MBCS Codierung für Windows Chinesisch (vereinfacht)	10114

Name	Beschreibung	ID
LMBCS-2	Lotus MBCS Codierung für PC DOS Griechisch	10104
LMBCS-3	Lotus MBCS Codierung für Windows Hebräisch	10105
LMBCS-4	Lotus MBCS Codierung für Windows Arabisch	10106
LMBCS-5	Lotus MBCS Codierung für Windows Kyrillisch	10107
LMBCS-6	Lotus MBCS Codierung für PC Lateinisch2	10108
LMBCS-8	Lotus MBCS Codierung für Windows Türkisch	10109
Macintosh	Apple Lateinisch 1	10067
MELCOM	MITSUBISHI MELCOM Japanisch	9004
MELCOM-K	MITSUBISHI MELCOM-Kana Japanisch	9009
MS1250	MS Windows Lateinisch 2 (Zentraleuropa)	2250
MS1251	MS Windows Kyrillisch (Slawisch)	2251
MS1252	MS Windows Lateinisch 1 (ANSI), übergeordneter Zeichensatz von Lateinisch 1	2252
MS1253	MS Windows Griechisch	2253
MS1254	MS Windows Lateinisch 5 (Türkisch), übergeordneter Zeichensatz von ISO 8859-9	2254
MS1255	MS Windows Hebräisch	2255
MS1256	MS Windows Arabisch	2256
MS1257	MS Windows Ostseeanrainer	2257
MS1258	MS Windows Vietnamesisch	2258
MS1361	MS Windows Koreanisch (Johab)	1361
MS874	MS-DOS Thailändisch, übergeordneter Zeichensatz von TIS 620	874
MS932	MS Windows Japanisch, Umsch-JIS	2024
MS936	MS Windows Vereinfachtes Chinesisch, übergeordneter Zeichensatz von GB 2312-80, EUC Codierung	936
MS949	MS Windows Koreanisch, übergeordneter Zeichensatz von KS C 5601-1992	949
MS950	MS Windows Traditionelles Chinesisch, übergeordneter Zeichensatz von Big 5	950
SCSU	Standardkomprimierungsschema für Unicode (SCSU)	10009

Name	Beschreibung	ID
UNISYS	UNISYS Japanisch	9003
UNISYS-K	UNISYS-Kana Japanisch	9008
US-ASCII	7-Bit-ASCII	1
UTF-16_OppositeEndian	UTF-16 Codierung von Unicode (entgegengesetztes Plattform-Endian)	10004
UTF-16_PlatformEndian	UTF-16 Codierung von Unicode (Plattform-Endian)	10003
UTF-16BE	UTF-16 Codierung von Unicode (Big Endian)	1200
UTF-16LE	UTF-16 Codierung von Unicode (Lower Endian)	1201
UTF-32_OppositeEndian	UTF-32 Codierung von Unicode (entgegengesetztes Plattform-Endian)	10006
UTF-32_PlatformEndian	UTF-32 Codierung von Unicode (Plattform-Endian)	10005
UTF-32BE	UTF-32 Codierung von Unicode (Plattform-Endian)	10001
UTF-32LE	UTF-32 Codierung von Unicode (Lower Endian)	10002
UTF-7	UTF-7-Kodierung von Unicode	10007
UTF-8	UTF 8-Kodierung von Unicode	106
windows-57002	Indischer Skriptcode zum Informationsaustausch - Devanagari	10094
windows-57003	Indischer Skriptcode zum Informationsaustausch - Bengalisch	10095
windows-57004	Indischer Skriptcode zum Informationsaustausch - Tamilisch	10099
windows-57005	Indischer Skriptcode zum Informationsaustausch - Telugu	10100
windows-57007	Indischer Skriptcode zum Informationsaustausch - Oriya	10098
windows-57008	Indischer Skriptcode zum Informationsaustausch - Kannada	10101
windows-57009	Indischer Skriptcode zum Informationsaustausch - Malayalam	10102
windows-57010	Indischer Skriptcode zum Informationsaustausch - Gujarati	10097
windows-57011	Indischer Skriptcode zum Informationsaustausch - Gurumukhi	10096
x-mac-centraleurroman	Apple Zentraleuropa	10070
x-mac-cyrillic	Apple Kyrillisch	10069

Name	Beschreibung	ID
x-mac-greek	Apple Griechisch	10068
x-mac-turkish	Apple Türkisch	10071

Einschränkungen für quell- und zielseitige Codepages

Beachten Sie bei der Zuweisung von Codepages in der Quelle oder im Ziel die folgenden Einschränkungen:

- Wählen Sie IBM EBCDIC als Code für Ihre Quelldatenbankverbindung nur dann, wenn Sie auf EBCDIC-Daten zugreifen, zum Beispiel auf Daten aus einer extrahierten Großrechnerdatei.
- Die folgenden Codepages werden nicht für Datenbank- oder relationale Verbindungen unterstützt:
 - UTF-16 Codierung von Unicode (entgegengesetztes Plattform-Endian)
 - UTF-16 Codierung von Unicode (Plattform-Endian)
 - UTF-16 Codierung von Unicode (Big Endian)
 - UTF-16 Codierung von Unicode (Lower Endian)

ANHANG B

Befehlszeilenberechtigungen

Dieser Anhang umfasst die folgenden Themen:

- [infacmd as Befehle, 295](#)
- [infacmd dis Befehle, 296](#)
- [infacmd ipc Befehlsprogramme, 298](#)
- [infacmd isp-Befehle, 298](#)
- [infacmd mrs Befehlsprogramme, 309](#)
- [infacmd ms Befehlsprogramme, 310](#)
- [infacmd oie Befehlsprogramme, 311](#)
- [infacmd ps Befehlsprogramme, 311](#)
- [infacmd pwx - Befehle, 312](#)
- [infacmd rtm Befehlsprogramme, 313](#)
- [infacmd sql - Befehle, 313](#)
- [infacmd rds Befehlsprogramme, 315](#)
- [infacmd wfs-Befehle, 315](#)
- [pmcmd-Befehle, 315](#)
- [pmrep Befehlsprogramme, 318](#)

infacmd as Befehle

Um *infacmd as* Befehle auszuführen, müssen die Benutzer über eines der gelisteten Sets von Domänenberechtigungen, Analyst-Dienst Berechtigungen und Domänenobjektberechtigungen verfügen.

Die folgende Tabelle enthält eine Auflistung der erforderlichen Berechtigungen für *infacmd as* Befehle:

infacmd as Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
CreateAuditTables	Domänen-Administration	Dienst verwalten	Domäne oder Knoten, auf der/dem der Analyst-Dienst ausgeführt wird
CreateService	Domänen-Administration	Dienst verwalten	Domäne oder Knoten, auf der/dem der Analyst-Dienst ausgeführt wird
DeleteAuditTables	Domänen-Administration	Dienst verwalten	Domäne oder Knoten, auf der/dem der Analyst-Dienst ausgeführt wird
ListServiceOptions	-	-	Analyst-Dienst
ListServiceProcessOptions	-	-	Analyst-Dienst
UpdateServiceOptions	Domänen-Administration	Dienst verwalten	Domäne oder Knoten, auf der/dem der Analyst-Dienst ausgeführt wird
UpdateServiceProcessOptions	Domänen-Administration	Dienst verwalten	Domäne oder Knoten, auf der/dem der Analyst-Dienst ausgeführt wird

infacmd dis Befehle

Um *infacmd dis*-Befehle ausführen zu können, benötigt der Benutzer eine der aufgeführten Gruppen von Domänenberechtigungen, Berechtigungen für Datenintegrationsdienste und Domänenobjektberechtigungen.

Aus der folgenden Tabelle gehen die erforderlichen Berechtigungen für *infacmd dis* Befehle hervor:

infacmd dis Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
BackupApplication	Anwendungsadministration	Anwendungen verwalten	-
CancelDataObjectCacheRefresh	-	-	-
CreateService	Domänen-Administration	Dienste verwalten	Domäne oder Knoten, auf der/dem der Datenintegrationsdienst ausgeführt wird

infacmd dis Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
DeployApplication	Anwendungsadministratio n	Anwendungen verwalten	-
ListApplicationObjects	-	-	-
ListApplications	-	-	-
ListDataObjectOptions	-	-	-
ListServiceOptions	-	Dienst verwalten	Domäne oder Knoten, auf der/dem der Datenintegrationsdienst ausgeführt wird
ListServiceProcessOptions	-	Dienst verwalten	Domäne oder Knoten, auf der/dem der Datenintegrationsdienst ausgeführt wird
PurgeDataObjectCache	-	-	-
RefreshDataObjectCache	-	-	-
RenameApplication	Anwendungsadministratio n	Anwendungen verwalten	-
RestoreApplication	Anwendungsadministratio n	Anwendungen verwalten	-
StartApplication	Anwendungsadministratio n	Anwendungen verwalten	-
StopApplication	Anwendungsadministratio n	Anwendungen verwalten	-
UndeployApplication	Anwendungsadministratio n	Anwendungen verwalten	-
UpdateApplication	Anwendungsadministratio n	Anwendungen verwalten	-
UpdateApplicationOptions	Anwendungsadministratio n	Anwendungen verwalten	-
UpdateDataObjectOptions	Anwendungsadministratio n	Anwendungen verwalten	-
UpdateServiceOptions	Domänen-Administration	Dienste verwalten	Domäne oder Knoten, auf der/dem der Datenintegrationsdienst ausgeführt wird
UpdateServiceProcessOpti ons	Domänen-Administration	Dienste verwalten	Domäne oder Knoten, auf der/dem der Datenintegrationsdienst ausgeführt wird

infacmd ipc Befehlsprogramme

Um ein *infacmd ipc*-Befehlsprogramm auszuführen, muss der Benutzer eine der aufgelisteten Berechtigungen für die Model Repository-Objekte besitzen.

Die nachstehende Tabelle für die erforderlichen Berechtigungen für die *infacmd isp* Befehlsprogramme auf:

infacmd ipc Befehlsprogramme	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
ExportToPC	-	-	Im Ordner zu lesen, in dem die Referenztabellen für den Export erstellt werden.

infacmd isp-Befehle

Um die *infacmd isp*-Befehle auszuführen, müssen die Benutzer eine der aufgeführten Zusammenstellungen für Domänenberechtigungen, Dienstberechtigungen, Domänenobjektberechtigungen und Verbindungsberechtigungen besitzen.

Einem Benutzer muss die Administratorrolle für die Domäne zugewiesen sein, damit er folgende Befehle ausführen kann:

- AddDomainLink
- AssignGroupPermission (in der Domäne)
- AssignGroupPermission (in den Betriebssystemprofilen)
- AddServiceLevel
- AssignUserPermission (in der Domäne)
- AssignUserPermission (in den Betriebssystemprofilen)
- CreateOSProfile
- PurgeLog
- RemoveDomainLink
- RemoveOSProfile
- RemoveServiceLevel
- SwitchToGatewayNode
- SwitchToWorkerNode
- UpdateDomainOptions
- UpdateDomainPassword
- UpdateGatewayInfo
- UpdateServiceLevel
- UpdateSMTPOptions

Benutzern muss die Administratorrolle für die Domäne zugewiesen sein, damit der UpdateGatewayInfo-Befehl ausgeführt werden kann:

Die nachstehende Tabelle für die erforderlichen Berechtigungen für die *infacmd isp*-Befehle auf:

infacmd isp-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
GetNodeName	-	-	Knoten
UpdateGatewayInfo	-	-	-

infacmd isp-Befehl	Berechtigungsgruppen	Name der Berechtigung	Berechtigung für
AddAlertUser (für Ihr Benutzerkonto)	-	-	-
AddAlertUser (für andere Benutzer)	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
AddConnectionPermissions	-	-	Verbindung zuweisen
AddDomainLink	-	-	-
AddDomainNode	Domänenverwaltung	Knoten und Gitter verwalten	Domäne und Knoten
AssignGroupPermission (in Anwendungsdiensten oder Lizenzobjekten)	Domänenverwaltung	Dienste verwalten	Anwendungsdienst oder Lizenzobjekt
AssignGroupPermission (in der Domäne)	-	-	-
AssignGroupPermission (in Ordnern)	Domänenverwaltung	Domänenordner verwalten	Ordner
AssignGroupPermission (auf Knoten und Gittern)	Domänenverwaltung	Knoten und Gitter verwalten	Knoten oder Gitter
AssignGroupPermission (in den Betriebssystemprofilen)	-	-	-
AddGroupPrivilege	Sicherheitsverwaltung	Berechtigungen und Rollen gewähren	Domäne, Metadata Manager-Dienst, Modellrepository-Dienst, PowerCenter-Repository-Dienst oder Berichterstellungsdienst
AddLicense	Domänenverwaltung	Dienste verwalten	Domäne oder übergeordneter Ordner
AddNodeResource	Domänenverwaltung	Knoten und Gitter verwalten	Knoten
AddRolePrivilege	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
AddServiceLevel	-	-	-

infacmd isp-Befehl	Berechtigungsgruppen	Name der Berechtigung	Berechtigung für
AssignGroupPermission (in Anwendungsdiensten oder Lizenzobjekten)	Domänenverwaltung	Dienste verwalten	Anwendungsdienst oder Lizenzobjekt
AssignUserPermission (in der Domäne)	-	-	-
AssignGroupPermission (in Ordnern)	Domänenverwaltung	Domänenordner verwalten	Ordner
AssignGroupPermission (auf Knoten und Gittern)	Domänenverwaltung	Knoten und Gitter verwalten	Knoten oder Gitter
AssignUserPermission (in den Betriebssystemprofilen)	-	-	-
AssignUserPrivilege	Sicherheitsverwaltung	Berechtigungen und Rollen gewähren	Domäne, Metadata Manager-Dienst, Modellrepository-Dienst, PowerCenter-Repository-Dienst oder Berichterstellungsdienst
AssignUserToGroup	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
AssignedToLicense	Domänenverwaltung	Dienste verwalten	Lizenzobjekt und Anwendungsdienst
AssignISTOMMService	Domänenverwaltung	Dienste verwalten	Metadata Manager-Dienst
AssignLicense	Domänenverwaltung	Dienste verwalten	Lizenzobjekt und Anwendungsdienst
AssignRoleToGroup	Sicherheitsverwaltung	Berechtigungen und Rollen gewähren	Domäne, Metadata Manager-Dienst, Modellrepository-Dienst, PowerCenter-Repository-Dienst oder Berichterstellungsdienst
AssignRoleToUser	Sicherheitsverwaltung	Berechtigungen und Rollen gewähren	Domäne, Metadata Manager-Dienst, Modellrepository-Dienst, PowerCenter-Repository-Dienst oder Berichterstellungsdienst
AssignRSToWSHubService	Domänenverwaltung	Dienste verwalten	PowerCenter-Repository-Dienst und Webdienst-Hub
BackupReportingServiceContents	Domänenverwaltung	Dienste verwalten	Berichterstellungsdienst

infacmd isp-Befehl	Berechtigungsgruppen	Name der Berechtigung	Berechtigung für
ConvertLogFile	-	-	Domäne oder Anwendungsdienst
CreateFolder	Domänenverwaltung	Domänenordner verwalten	Domäne oder übergeordneter Ordner
CreateConnection	-	-	-
CreateGrid	Domänenverwaltung	Knoten und Gitter verwalten	Domäne oder übergeordneter Ordner und Gittern zugewiesene Knoten
CreateGroup	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
CreateIntegrationService	Domänenverwaltung	Dienste verwalten	Domäne oder übergeordneter Ordner, Knoten oder Gitter, auf dem der PowerCenter-Integrationsdienst ausgeführt wird, Lizenzobjekt und zugehöriger PowerCenter-Repository-Dienst
CreateMMService	Domänenverwaltung	Dienste verwalten	Domäne oder übergeordneter Ordner, Knoten, auf dem der Metadata Manager-Dienst ausgeführt wird, Lizenzobjekt und zugehöriger PowerCenter-Integrationsdienst und PowerCenter-Repository-Dienst
CreateOSProfile	-	-	-
CreateReportingService	Domänenverwaltung	Dienste verwalten	Domäne oder übergeordneter Ordner, Knoten, auf dem der Berichterstellungsdienst ausgeführt wird, Lizenzobjekt und Anwendungsdienst, der für Bericht ausgewählt wurde
CreateReportingServiceContents	Domänenverwaltung	Dienste verwalten	Berichterstellungsdienst

infacmd isp-Befehl	Berechtigungsgruppen	Name der Berechtigung	Berechtigung für
CreateRepositoryService	Domänenverwaltung	Dienste verwalten	Domäne und übergeordneter Ordner, Knoten auf dem der PowerCenter-Repository-Dienst ausgeführt wird und Lizenzobjekt
CreateRole	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
CreateSAPBWService	Domänenverwaltung	Dienste verwalten	Domäne oder übergeordneter Ordner, Knoten oder Gitter, auf dem der SAP BW-Dienst ausgeführt wird, Lizenzobjekt und zugehöriger PowerCenter-Integrationsdienst
CreateUser	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
CreateWSHubService	Domänenverwaltung	Dienste verwalten	Domäne oder übergeordneter Ordner, Knoten oder Gitter, auf dem der Webdienst-Hub ausgeführt wird, Lizenzobjekt und zugehöriger PowerCenter-Repository-Dienst
DeleteSchemaReportingServiceContents	Domänenverwaltung	Dienste verwalten	Berichterstellungsdienst
DisableNodeResource	Domänenverwaltung	Knoten und Gitter verwalten	Knoten
DisableService (für Metadata Manager-Dienst)	Domänenverwaltung	Dienstausführung verwalten	Metadata Manager-Dienst und zugehöriger PowerCenter-Integrationsdienst und PowerCenter-Repository-Dienst
DisableService (für alle anderen Anwendungsdienste)	Domänenverwaltung	Dienstausführung verwalten	Anwendungsdienst
DisableServiceProcess	Domänenverwaltung	Dienstausführung verwalten	Anwendungsdienst
DisableUser	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-

infacmd isp-Befehl	Berechtigungsgruppen	Name der Berechtigung	Berechtigung für
EditUser	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
EnableNodeResource	Domänenverwaltung	Knoten und Gitter verwalten	Knoten
EnableService (für Metadata Manager-Dienst)	Domänenverwaltung	Dienstausführung verwalten	Metadata Manager-Dienst und zugehöriger PowerCenter-Integrationsdienst und PowerCenter-Repository-Dienst
EnableService (für alle anderen Dienste)	Domänenverwaltung	Dienstausführung verwalten	Anwendungsdienst
EnableServiceProcess	Domänenverwaltung	Dienstausführung verwalten	Anwendungsdienst
EnableUser	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
ExportDomainObjects (für Benutzer, Gruppen und Rollen)	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
ExportDomainObjects (für Verbindungen)	Domänenverwaltung	Verbindungen verwalten	Lesen in Verbindungen
ExportUsersAndGroups	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
GetFolderInfo	-	-	Ordner
GetLastError	-	-	Anwendungsdienst
GetLog	-	-	Domäne oder Anwendungsdienst
GetNodeName	-	-	Knoten
GetServiceOption	-	-	Anwendungsdienst
GetServiceProcessOption	-	-	Anwendungsdienst
GetServiceProcessStatus	-	-	Anwendungsdienst
GetServiceStatus	-	-	Anwendungsdienst
GetSessionLog	Laufzeitobjekte	Überwachen	Lesen im Repository-Ordner

infacmd isp-Befehl	Berechtigungsgruppen	Name der Berechtigung	Berechtigung für
GetWorkflowLog	Laufzeitobjekte	Überwachen	Lesen im Repository-Ordner
Hilfe	-	-	-
ImportDomainObjects (für Benutzer, Gruppen und Rollen)	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
ImportDomainObjects (für Verbindungen)	Domänenverwaltung	Verbindungen verwalten	Schreiben in Verbindungen
ImportUsersAndGroups	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
ListAlertUsers	-	-	Domäne
ListAllGroups	-	-	-
ListAllRoles	-	-	-
ListAllUsers	-	-	-
ListConnectionOptions	-	-	Lesen in Verbindung
ListConnections	-	-	-
ListConnectionPermissions	-	-	-
ListConnectionPermissions durch Gruppe	-	-	-
ListConnectionPermissions durch Benutzer	-	-	-
ListDomainLinks	-	-	Domäne
ListDomainOptions	-	-	Domäne
ListFolders	-	-	Ordner
ListGridNodes	-	-	-
ListGroupsForUser	-	-	Domäne
ListGroupPermissions	-	-	-
ListGroupPrivilege	Sicherheitsverwaltung	Berechtigungen und Rollen gewähren	Domäne, Metadata Manager-Dienst, Modellrepository-Dienst, PowerCenter-Repository-Dienst oder Berichterstellungsdienst

infacmd isp-Befehl	Berechtigungsgruppen	Name der Berechtigung	Berechtigung für
ListLDAPConnectivity	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
ListLicenses	-	-	Lizenzobjekte
ListNodeOptions	-	-	Knoten
ListNodes	-	-	-
ListNodeResources	-	-	Knoten
ListPlugins	-	-	-
ListRepositoryLDAPConfiguration	-	-	Domäne
ListRolePrivileges	-	-	-
ListSecurityDomains	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
ListServiceLevels	-	-	Domäne
ListServiceNodes	-	-	Anwendungsdienst
ListServicePrivileges	-	-	-
ListServices	-	-	-
ListSMTPOptions	-	-	Domäne
ListUserPermissions	-	-	-
ListUserPrivilege	Sicherheitsverwaltung	Berechtigungen und Rollen gewähren	Domäne, Metadata Manager-Dienst, Modellrepository-Dienst, PowerCenter-Repository-Dienst oder Berichterstellungsdienst
MigrateReportingServiceContents	Domänenverwaltung und Sicherheitsverwaltung	Verwalten von Diensten, Benutzern, Gruppen und Rollen	Domäne
MoveFolder	Domänenverwaltung	Domänenordner verwalten	Ursprungs- und Zielordner
MoveObject (für Anwendungsdienste und Lizenzobjekte)	Domänenverwaltung	Dienste verwalten	Ursprungs- und Zielordner

infacmd isp-Befehl	Berechtigungsgruppen	Name der Berechtigung	Berechtigung für
MoveObject (für Knoten und Gitter)	Domänenverwaltung	Knoten und Gitter verwalten	Ursprungs- und Zielordner
Ping	-	-	-
PurgeLog	-	-	-
RemoveAlertUser (für Ihr Benutzerkonto)	-	-	-
RemoveAlertUser (für andere Benutzer)	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
RemoveConnection	-	-	Schreiben in Verbindungen
RemoveConnectionPermissions	-	-	Verbindung zuweisen
RemoveDomainLink	-	-	-
RemoveFolder	Domänenverwaltung	Domänenordner verwalten	Domäne oder übergeordneter Ordner und Ordner werden entfernt
RemoveGrid	Domänenverwaltung	Knoten und Gitter verwalten	Domäne oder übergeordneter Ordner und Gitter
RemoveGroup	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
RemoveGroupPrivilege	Sicherheitsverwaltung	Berechtigungen und Rollen gewähren	Domäne, Metadata Manager-Dienst, Modellrepository-Dienst, PowerCenter-Repository-Dienst oder Berichterstellungsdienst
RemoveLicense	Domänenverwaltung	Dienste verwalten	Domäne oder übergeordneter Ordner und Lizenzobjekt
RemoveNode	Domänenverwaltung	Knoten und Gitter verwalten	Domäne oder übergeordneter Ordner und Knoten
RemoveNodeResource	Domänenverwaltung	Knoten und Gitter verwalten	Knoten
RemoveOSProfile	-	-	-

infacmd isp-Befehl	Berechtigungsgruppen	Name der Berechtigung	Berechtigung für
RemoveRole	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
RemoveRolePrivilege	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
RemoveService	Domänenverwaltung	Dienste verwalten	Domäne oder übergeordneter Ordner und Anwendungsdienst
RemoveServiceLevel	-	-	-
RemoveUser	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
RemoveUserFromGroup	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
RemoveUserPrivilege	Sicherheitsverwaltung	Berechtigungen und Rollen gewähren	Domäne, Metadata Manager-Dienst, Modellrepository-Dienst, PowerCenter-Repository-Dienst oder Berichterstellungsdienst
RenameConnection	-	-	Schreiben in Verbindungen
ResetPassword (für Ihr Benutzerkonto)	-	-	-
ResetPassword (für andere Benutzer)	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
RestoreReportingServiceContents	Domänenverwaltung	Dienste verwalten	Berichterstellungsdienst
RunCUPProfile	Domänenverwaltung	Knoten und Gitter verwalten	Knoten
SetConnectionPermission	-	-	Verbindung zuweisen
SetLDAPConnectivity	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
SetRepositoryLDAPConfiguration	-	-	Domäne
ShowLicense	-	-	Lizenzobjekt
ShutdownNode	Domänenverwaltung	Knoten und Gitter verwalten	Knoten

infacmd isp-Befehl	Berechtigungsgruppen	Name der Berechtigung	Berechtigung für
SwitchToGatewayNode	-	-	-
SwitchToWorkerNode	-	-	-
UnAssignISMMService	Domänenverwaltung	Dienste verwalten	PowerCenter-Integrationsdienst und Metadata Manager-Dienst.
UnassignLicense	Domänenverwaltung	Dienste verwalten	Lizenzobjekt und Anwendungsdienst
UnAssignRoleFromGroup	Sicherheitsverwaltung	Berechtigungen und Rollen gewähren	Domäne, Metadata Manager-Dienst, Modellrepository-Dienst, PowerCenter-Repository-Dienst oder Berichterstellungsdienst
UnAssignRoleFromUser	Sicherheitsverwaltung	Berechtigungen und Rollen gewähren	Domäne, Metadata Manager-Dienst, Modellrepository-Dienst, PowerCenter-Repository-Dienst oder Berichterstellungsdienst
UnassignRSWSHubService	Domänenverwaltung	Dienste verwalten	PowerCenter-Repository-Dienst und Webdienst-Hub
UnassociateDomainNode	Domänenverwaltung	Knoten und Gitter verwalten	Knoten
UpdateConnection	-	-	Schreiben in Verbindungen
UpdateDomainOptions	-	-	-
UpdateDomainPassword	-	-	-
UpdateFolder	Domänenverwaltung	Domänenordner verwalten	Ordner
UpdateGatewayInfo	-	-	-
UpdateGrid	Domänenverwaltung	Knoten und Gitter verwalten	Gitter und Knoten
UpdateIntegrationService	Domänenverwaltung	Dienste verwalten	PowerCenter-Integrationsdienst
UpdateLicense	Domänenverwaltung	Dienste verwalten	Lizenzobjekt
UpdateMMService	Domänenverwaltung	Dienste verwalten	Metadata Manager-Dienst

infacmd isp-Befehl	Berechtigungsgruppen	Name der Berechtigung	Berechtigung für
UpdateNodeOptions	Domänenverwaltung	Knoten und Gitter verwalten	Knoten
UpdateOSProfile	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	Betriebssystemprofil
UpdateReportingService	Domänenverwaltung	Dienste verwalten	Berichterstellungsdienst
UpdateRepositoryService	Domänenverwaltung	Dienste verwalten	PowerCenter-Repository-Dienst
UpdateSAPBWService	Domänenverwaltung	Dienste verwalten	SAP BW-Dienst
UpdateServiceLevel	-	-	-
UpdateServiceProcess	Domänenverwaltung	Dienste verwalten	PowerCenter-Integrationsdienst Jeder dem PowerCenter-Integrationsdienst hinzugefügte Knoten
UpdateSMTPOptions	-	-	-
UpdateWSHubService	Domänenverwaltung	Dienste verwalten	Webdienst-Hub
UpgradeReportingServiceContents	Domänenverwaltung	Dienste verwalten	Berichterstellungsdienst

infacmd mrs Befehlsprogramme

Um ein *infacmd mrs*-Befehlsprogramm ausführen zu können, muss der Benutzer über einen der aufgelisteten Sätze an Profil- und Domänenobjektberechtigungen verfügen.

Die nachstehende Tabelle führt die erforderlichen Berechtigungen für die *infacmd mrs* Befehlsprogramme auf:

Befehl infacmd mrs	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für...
BackupContents	Domänenverwaltung	Dienst verwalten	Domäne oder Knoten, auf dem der Modellrepository-Dienst ausgeführt wird
CreateContents	Domänenverwaltung	Dienst verwalten	Domäne oder Knoten, auf dem der Modellrepository-Dienst ausgeführt wird
CreateService	Domänenverwaltung	Dienst verwalten	Domäne oder Knoten, auf dem der Modellrepository-Dienst ausgeführt wird

Befehl <i>infacmd mrs</i>	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für...
DeleteContents	Domänenverwaltung	Dienst verwalten	Domäne oder Knoten, auf dem der Modellrepository-Dienst ausgeführt wird
ListBackupFiles	Domänenverwaltung	Dienst verwalten	Domäne oder Knoten, auf dem der Modellrepository-Dienst ausgeführt wird
ListProjects	Domänenverwaltung	Dienst verwalten	Domäne oder Knoten, auf dem der Modellrepository-Dienst ausgeführt wird
ListServiceOptions	-	-	Der Modellrepository-Dienst
ListServiceProcessOptions	-	-	Der Modellrepository-Dienst
RestoreContents	Domänenverwaltung	Dienst verwalten	Domäne oder Knoten, auf dem der Modellrepository-Dienst ausgeführt wird
UpgradeContents	Verwaltung des Modellrepository-Diensts	Erstellen, Bearbeiten und Löschen von Projekten	Schreiben in Projekten
UpdateServiceOptions	Domänenverwaltung	Dienst verwalten	Der Modellrepository-Dienst
UpdateServiceProcessOptions	Domänenverwaltung	Dienst verwalten	Der Modellrepository-Dienst

infacmd ms Befehlsprogramme

Um ein *infacmd ms*-Befehlsprogramm auszuführen, muss der Benutzer eine der aufgelisteten Berechtigungen für das Domänenobjekt besitzen.

Die nachstehende Tabelle führt die erforderlichen Berechtigungen für die *infacmd ms* Befehlsprogramme auf:

infacmd ms Befehlsprogramme	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
ListMappings	-	-	-
ListMappingParams	-	-	-
RunMapping	-	-	Ausführen auf Verbindungsobjekten, die von Mappings benutzt werden

infacmd oie Befehlsprogramme

Um ein *infacmd oie*-Befehlsprogramm auszuführen, muss der Benutzer eine der aufgelisteten Berechtigungen für die Model Repository-Objekte besitzen.

Die nachstehende Tabelle führt die erforderlichen Berechtigungen für die *infacmd oie* Befehlsprogramme auf:

infacmd oie Befehlsprogramme	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
ExportObjects	-	-	Lesen in Projekt
ImportObjects	-	-	In Projekt schreiben

infacmd ps Befehlsprogramme

Um *infacmd ps*-Befehle ausführen zu können, müssen Benutzer über einen der aufgeführten Sätze an Profilberechtigungen und Berechtigungen für Domänenobjekte verfügen.

Die nachstehende Tabelle führt die erforderlichen Berechtigungen für die *infacmd ps* Befehlsprogramme auf:

infacmd ps Befehlsprogramm	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
CreateWH	-	-	-
DropWH	-	-	-
Ausführen	-	-	Lesen in Projekt Quellverbindungsobjekt ausführen
Liste	-	-	Lesen in Projekt
Löschen	-	-	Lesen und Schreiben in Ordner

infacmd ps-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
CreateWH	-	-	-
DropWH	-	-	-

infacmd pwx - Befehle

Um *infacmd pwx*-Befehle auszuführen, müssen Benutzer einen der aufgeführten Sätze von PowerExchange-Anwendungsdienstberechtigungen besitzen.

Die nachstehende Tabelle führt die erforderlichen Berechtigungen für die *infacmd pwx* Befehlsprogramme auf:

infacmd pwx-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
CloseForceListener	Verwaltungsbefehle	closeforce	-
CloseListener	Verwaltungsbefehle	schließen	-
CondenseLogger	Verwaltungsbefehle	kondensieren	-
CreateListenerService	Domänen-Administration	Dienst verwalten	Domäne oder Knoten, auf dem/der der PowerExchange-Anwendungsdienst läuft
CreateLoggerService	Domänen-Administration	Dienst verwalten	Domäne oder Knoten, auf dem/der der PowerExchange-Anwendungsdienst läuft
DisplayAllLogger	Informationsbefehle	displayall	-
DisplayCheckpointsLogger	Informationsbefehle	displaycheckpoints	-
DisplayCPULogger	Informationsbefehle	displaycpu	-
DisplayEventsLogger	Informationsbefehle	displayevents	-
DisplayMemoryLogger	Informationsbefehle	displaymemory	-
DisplayRecordsLogger	Informationsbefehle	displayrecords	-
DisplayStatusLogger	Informationsbefehle	displaystatus	-
FileSwitchLogger	Verwaltungsbefehle	fileswitch	-
ListTaskListener	Informationsbefehle	listtask	-
ShutDownLogger	Verwaltungsbefehle	herunterfahren	-
StopTaskListener	Verwaltungsbefehle	stoptask	-

infacmd pwx-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
UpdateListenerService	Domänen-Administration	Dienst verwalten	Domäne oder Knoten, auf dem/der der PowerExchange-Anwendungsdienst läuft
UpdateLoggerService	Domänen-Administration	Dienst verwalten	Domäne oder Knoten, auf dem/der der PowerExchange-Anwendungsdienst läuft

infacmd rtm Befehlsprogramme

Um ein *infacmd rtm*-Befehlsprogramm auszuführen, muss der Benutzer eines der aufgelisteten Sets an Profil- und Domänenobjektberechtigungen des Modellrepository-Diensts besitzen.

Die nachstehende Tabelle führt die erforderlichen Berechtigungen für die *infacmd rtm* Befehlsprogramme auf:

infacmd rtm Befehlsprogramme	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
Deployimport	-	-	-
Exportieren	-	-	Lesen in Projekten, die Referenztabellen für den Export enthalten.
Importieren	-	-	Lesen und Schreiben in dem Projekt, in die die Referenztabellen importiert werden.

infacmd sql - Befehle

Um *infacmd sql*-Befehle ausführen zu können, müssen Benutzer über einen der aufgeführten Sätze an Domänenberechtigungen, Datenintegrationsdienst und Berechtigungen für Domänenobjekte verfügen.

Die folgende Tabelle listet die erforderlichen Berechtigungen für die *infacmd sql*-Befehle auf:

infacmd sql - Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
ExecuteSQL	-	-	Basierend auf Objekten, auf die Sie in Ihrer SQL-Anweisung zugreifen möchten
ListColumnPermissions	-	-	-
ListSQLDataServiceOptions	-	-	-
ListSQLDataServicePermissions	-	-	-
ListSQLDataServices	-	-	-
ListStoredProcedurePermissions	-	-	-
ListTableOptions	-	-	-
ListTablePermissions	-	-	-
PurgeTableCache	-	-	-
RefreshTableCache	-	-	-
RenameSQLDataService	Anwendungsadministration	Anwendungen verwalten	-
SetColumnPermissions	-	-	Gewähren für das Objekt
SetSQLDataServicePermissions	-	-	Gewähren für das Objekt
SetStoredProcedurePermissions	-	-	Gewähren für das Objekt
SetTablePermissions	-	-	Gewähren für das Objekt
StartSQLDataService	Anwendungsadministration	Anwendungen verwalten	-
StopSQLDataService	Anwendungsadministration	Anwendungen verwalten	-
UpdateColumnOptions	Anwendungsadministration	Anwendungen verwalten	-
UpdateSQLDataServiceOptions	Anwendungsadministration	Anwendungen verwalten	-
UpdateTableOptions	Anwendungsadministration	Anwendungen verwalten	-

infacmd rds Befehlsprogramme

Um ein infacmd rds-Befehlsprogramm auszuführen, muss der Benutzer eines der aufgelisteten Sets an Domänen-, Reporting and Dashboards Service-Berechtigungen sowie der Domänenobjektberechtigungen besitzen.

Die nachstehende Tabelle führt die erforderlichen Berechtigungen für die infacmd rds Befehlsprogramme auf:

infacmd rds Befehlsprogramm	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
CreateService	Domänen-Administration	Dienst verwalten	Domäne oder Knoten, auf dem der Reporting and Dashboards Service ausgeführt wird
ListServiceProcessOptions	-	-	Der Reporting and Dashboards Service

infacmd wfs-Befehle

Zum Ausführen von infacmd wfs-Befehlen benötigen Benutzer keine Berechtigungen.

pmcmd-Befehle

Um *pmcmd*-Befehle auszuführen zu können, müssen Benutzer über die aufgeführten Sätze an Berechtigungen für PowerCenter-Repository-Dienst und PowerCenter Repository-Objekte verfügen.

Wenn der PowerCenter-Integrationsdienst im abgesicherten Modus läuft, müssen die Benutzer über die Administrator-Rolle für den zugehörige PowerCenter-Repository-Dienst verfügen, um folgende Befehle ausführen zu können:

- aborttask
- abortworkflow
- getrunningsessionsdetails
- getservicedetails
- getsessionstatistics
- gettaskdetails
- getworkflowdetails
- recoverworkflow
- scheduleworkflow
- starttask
- startworkflow
- stoptask
- stopworkflow

- unscheduleworkflow

Die folgende Tabelle listet die erforderlichen Berechtigungen für die *pmcmd*-Befehle auf:

pmcmd-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung
aborttask (vom eigenen Benutzerkonto gestartet)	-	-	Lesen und Ausführen in Ordner
aborttask (von anderen Benutzern gestartet)	Laufzeitobjekte	Ausführung verwalten	Lesen und Ausführen in Ordner
abortworkflow (vom eigenen Benutzerkonto gestartet)	-	-	Lesen und Ausführen in Ordner
abortworkflow (von anderen Benutzern gestartet)	Laufzeitobjekte	Ausführung verwalten	Lesen und Ausführen in Ordner
Verbinden	-	-	-
Trennen	-	-	-
Beenden	-	-	-
getrunningsessionsdetails	Laufzeitobjekte	Überwachen	-
getservicedetails	Laufzeitobjekte	Überwachen	Lesen in Ordner
getserviceproperties	-	-	-
getsessionstatistics	Laufzeitobjekte	Überwachen	Lesen in Ordner
gettaskdetails	Laufzeitobjekte	Überwachen	Lesen in Ordner
getworkflowdetails	Laufzeitobjekte	Überwachen	Lesen in Ordner
Hilfe	-	-	-
pingservice	-	-	-
recoverworkflow (vom eigenen Benutzerkonto gestartet)	Laufzeitobjekte	Ausführen	Lesen und Ausführen in Ordner Lesen und Ausführen in Verbindungsobjekten Berechtigung für Betriebssystemprofil (falls zutreffend)
recoverworkflow (von anderen Benutzern gestartet)	Laufzeitobjekte	Ausführung verwalten	Lesen und Ausführen in Ordner Lesen und Ausführen in Verbindungsobjekten Berechtigung für Betriebssystemprofil (falls zutreffend)

pmcmd-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung
scheduleworkflow	Laufzeitobjekte	Ausführung verwalten	Lesen und Ausführen in Ordner Lesen und Ausführen in Verbindungsobjekten Berechtigung für Betriebssystemprofil (falls zutreffend)
setfolder	-	-	Lesen in Ordner
setnowait	-	-	-
setwait	-	-	-
showsettings	-	-	-
starttask	Laufzeitobjekte	Ausführen	Lesen und Ausführen in Ordner Lesen und Ausführen in Verbindungsobjekten Berechtigung für Betriebssystemprofil (falls zutreffend)
startworkflow	Laufzeitobjekte	Ausführen	Lesen und Ausführen in Ordner Lesen und Ausführen in Verbindungsobjekten Berechtigung für Betriebssystemprofil (falls zutreffend)
stoptask (vom eigenen Benutzerkonto gestartet)	-	-	Lesen und Ausführen in Ordner
stoptask (von anderen Benutzern gestartet)	Laufzeitobjekte	Ausführung verwalten	Lesen und Ausführen in Ordner
stopworkflow (vom eigenen Benutzerkonto gestartet)	-	-	Lesen und Ausführen in Ordner
stopworkflow (von anderen Benutzern gestartet)	Laufzeitobjekte	Ausführung verwalten	Lesen und Ausführen in Ordner
unscheduleworkflow	Laufzeitobjekte	Ausführung verwalten	Lesen und Ausführen in Ordner
unsetfolder	-	-	Lesen in Ordner
Version	-	-	-
waittask	Laufzeitobjekte	Überwachen	Lesen in Ordner
waitworkflow	Laufzeitobjekte	Überwachen	Lesen in Ordner

pmrep Befehlsprogramme

Benutzer müssen über die Berechtigung "Repository Manager öffnen" verfüge, um *pmrep*-Befehle ausführen zu können, mit Ausnahme der folgenden Befehle:

- Ausführen
- Erstellen
- Wiederherstellen
- Upgrade
- Version
- Hilfe

Um *pmrep*-Befehle auszuführen zu können, müssen Benutzer über einen der aufgeführten Sätze an Domänenberechtigungen und Berechtigungen für PowerCenter-Repository-Dienst, Domänenberechtigungen und Berechtigungen für Model Repository-Objekte verfügen.

Benutzer müssen Objekteigentümer sein oder über die Administrator-Rolle für den PowerCenter-Repository-Dienst verfügen, um die folgenden Befehle ausführen zu können:

- AssignPermission
- ChangeOwner
- DeleteConnection
- DeleteDeploymentGroup
- DeleteFolder
- DeleteLabel
- ModifyFolder (zum Ändern des Eigentümers, Konfigurieren von Berechtigungen, Freigeben des Ordners oder Bearbeiten von Ordernamen oder Beschreibung)

Die folgende Tabelle listet die erforderlichen Berechtigungen für die *pmrep*-Befehle auf:

pmrep-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung
AddToDeploymentGroup	Globale Objekte	Bereitstellungsgruppe n verwalten	Lesen in ursprünglichem Ordner Lesen und Schreiben in Bereitstellungsgruppe
ApplyLabel	-	-	Lesen in Ordner Lesen und Ausführen in Beschriftung
AssignPermission	-	-	-
BackUp	Domänen-Administration	Dienste verwalten	Berechtigung für PowerCenter-Repository-Dienst
ChangeOwner	-	-	-
CheckIn (für Ihre eigenen Auscheck-Vorgänge)	Designobjekte	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner

pmrep-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung
CheckIn (für Ihre eigenen Auscheck-Vorgänge)	Quellen und Ziele	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner
CheckIn (für Ihre eigenen Auscheck-Vorgänge)	Laufzeitobjekte	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner
CheckIn (für Auscheck-Vorgänge anderer)	Designobjekte	Versionen verwalten	Lesen und Schreiben in Ordner
CheckIn (für Auscheck-Vorgänge anderer)	Quellen und Ziele	Versionen verwalten	Lesen und Schreiben in Ordner
CheckIn (für Auscheck-Vorgänge anderer)	Laufzeitobjekte	Versionen verwalten	Lesen und Schreiben in Ordner
CleanUp	-	-	-
ClearDeploymentGroup	Globale Objekte	Bereitstellungsgruppen verwalten	Lesen und Schreiben in Bereitstellungsgruppe
Connect	-	-	-
Erstellen	Domänen-Administration	Dienste verwalten	Berechtigung für PowerCenter-Repository-Dienst
CreateConnection	Globale Objekte	Verbindungen erstellen	-
CreateDeploymentGroup	Globale Objekte	Bereitstellungsgruppen verwalten	-
CreateFolder	Ordner	Erstellen	-
CreateLabel	Globale Objekte	Beschriftungen erstellen	-
Löschen	Domänen-Administration	Dienste verwalten	Berechtigung für PowerCenter-Repository-Dienst
DeleteConnection	-	-	-
DeleteDeploymentGroup	-	-	-
DeleteFolder	-	-	-
DeleteLabel	-	-	-
DeleteObject	Designobjekte	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner
DeleteObject	Quellen und Ziele	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner

pmrep-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung
DeleteObject	Laufzeitobjekte	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner
BereitstellungsGruppeBereitstellen	Globale Objekte	Bereitstellungsgruppen verwalten	Lesen in ursprünglichem Ordner Lesen und Schreiben in Zielordner Lesen und Ausführen in Bereitstellungsgruppe
DeployFolder	Ordner	Kopieren bei Original-Repository Erstellen bei Ziel-Repository	Lesen in Ordner
ExecuteQuery	-	-	Lesen und Ausführen in Abfragen
Beenden	-	-	-
FindCheckout	-	-	Lesen in Ordner
GetConnectionDetails	-	-	Lesen in Verbindungsobjekten
Hilfe	-	-	-
KillUserConnection	Domänen-Administration	Dienste verwalten	Berechtigung für PowerCenter-Repository-Dienst
ListConnections	-	-	Lesen in Verbindungsobjekten
ListObjectDependencies	-	-	Lesen in Ordner
ListObjects	-	-	Lesen in Ordner
ListTablesBySess	-	-	Lesen in Ordner
ListUserConnections	Domänen-Administration	Dienste verwalten	Berechtigung für PowerCenter-Repository-Dienst
ModifyFolder (zum Ändern des Eigentümers, Konfigurieren von Berechtigungen, Freigeben des Ordners oder Bearbeiten von Ordernamen oder Beschreibung)	-	-	-
ModifyFolder (zum Ändern des Status)	Ordner	Versionen verwalten	Lesen und Schreiben in Ordner
Benachrichtigen	Domänen-Administration	Dienste verwalten	Berechtigung für PowerCenter-Repository-Dienst
ObjectExport	-	-	Lesen in Ordner

pmrep-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung
ObjectImport	Designobjekte	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner
ObjectImport	Quellen und Ziele	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner
ObjectImport	Laufzeitobjekte	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner
PurgeVersion	Designobjekte	Versionen verwalten	Lesen und Schreiben in Ordner Lesen, Schreiben und Ausführen von Abfragen, wenn Sie einen Abfragenamen angeben
PurgeVersion	Quellen und Ziele	Versionen verwalten	Lesen und Schreiben in Ordner Lesen, Schreiben und Ausführen von Abfragen, wenn Sie einen Abfragenamen angeben
PurgeVersion	Laufzeitobjekte	Versionen verwalten	Lesen und Schreiben in Ordner Lesen, Schreiben und Ausführen von Abfragen, wenn Sie einen Abfragenamen angeben
PurgeVersion (zum Löschen von Objekten auf Ordner Ebene)	Ordner	Versionen verwalten	Lesen und Schreiben in Ordner
PurgeVersion (zum Löschen von Objekten auf Repository-Ebene)	Domänen-Administration	Dienste verwalten	Berechtigung für PowerCenter-Repository-Dienst
Registrieren	Domänen-Administration	Dienste verwalten	Berechtigung für PowerCenter-Repository-Dienst
RegisterPlugin	Domänen-Administration	Dienste verwalten	Berechtigung für PowerCenter-Repository-Dienst
Wiederherstellen	Domänen-Administration	Dienste verwalten	Berechtigung für PowerCenter-Repository-Dienst
RollbackDeployment	Globale Objekte	Bereitstellungsgruppen verwalten	Lesen und Schreiben in Zielordner
Ausführen	-	-	-
ShowConnectionInfo	-	-	-
SwitchConnection	Laufzeitobjekte	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner Lesen in Verbindungsobjekten
TruncateLog	Laufzeitobjekte	Ausführung verwalten	Lesen und Ausführen in Ordner

pmrep-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung
UndoCheckout (für Ihren eigenen Auscheck-Vorgänge)	Designobjekte	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner
UndoCheckout (für Ihren eigenen Auscheck-Vorgänge)	Quellen und Ziele	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner
UndoCheckout (für Ihren eigenen Auscheck-Vorgänge)	Laufzeitobjekte	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner
UndoCheckout (für Auscheck-Vorgänge anderer)	Designobjekte	Versionen verwalten	Lesen und Schreiben in Ordner
UndoCheckout (für Auscheck-Vorgänge anderer)	Quellen und Ziele	Versionen verwalten	Lesen und Schreiben in Ordner
UndoCheckout (für Auscheck-Vorgänge anderer)	Laufzeitobjekte	Versionen verwalten	Lesen und Schreiben in Ordner
Unregister	Domänen-Administration	Dienste verwalten	Berechtigung für PowerCenter-Repository-Dienst
UnregisterPlugin	Domänen-Administration	Dienste verwalten	Berechtigung für PowerCenter-Repository-Dienst
UpdateConnection	-	-	Lesen und Schreiben in Verbindungsobjekten
UpdateEmailAddr	Laufzeitobjekte	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner
UpdateSeqGenVals	Designobjekte	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner
UpdateSrcPrefix	Laufzeitobjekte	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner
UpdateStatistics	Domänen-Administration	Dienste verwalten	Berechtigung für PowerCenter-Repository-Dienst
UpdateTargPrefix	Laufzeitobjekte	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner
Upgrade	Domänen-Administration	Dienste verwalten	Berechtigung für PowerCenter-Repository-Dienst
Validieren	Designobjekte	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner

pmrep-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung
Validieren	Laufzeitobjekte	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner
Version	-	-	-

Benutzerdefinierte Rollen

Dieser Anhang umfasst die folgenden Themen:

- [Benutzerdefinierte Rolle für den Analyst-Dienst, 324](#)
- [Benutzerdefinierte Rollen für den Metadata Manager-Dienst, 325](#)
- [Benutzerdefinierte Rolle für den Operator, 327](#)
- [PowerCenter-Repository-Dienst - Benutzerdefinierte Rollen, 328](#)
- [Benutzerdefinierte Rollen für den Berichterstellungsdienst, 329](#)
- [Benutzerdefinierte Rollen für den Test Data Manager-Dienst, 336](#)

Benutzerdefinierte Rolle für den Analyst-Dienst

Der Business Glossary-Verbraucher für den Analyst-Dienst ist eine benutzerdefinierte Rolle für den Analyst-Dienst.

Die folgende Tabelle listet die standardmäßige Berechtigung auf, die der benutzerdefinierten Rolle des Business Glossary-Verbrauchers für den Analyst-Dienst zugewiesen ist:

Berechtigungsgruppe	Name der Berechtigung
Zugriff auf Workspace	Glossar-Workspace

Benutzerdefinierte Rollen für den Metadata Manager-Dienst

Zu den benutzerdefinierten Rollen für den Metadata Manager-Dienst gehören die Rollen „Metadata Manager - Erweiterter Benutzer“, „Metadata Manager - Standardbenutzer“ und „Metadata Manager - Fortgeschrittener Benutzer“.

Metadata Manager – Erweiterter Benutzer

Die folgende Tabelle enthält die die Standardberechtigungen, die der benutzerdefinierten Rolle "Metadata Manager - Erweiterter Benutzer" zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Katalog	<ul style="list-style-type: none">- Verknüpfungen gemeinsam nutzen- Herkunft anzeigen- Zugehörige Kataloge anzeigen- Berichte anzeigen- Profilergebnisse anzeigen- Katalog anzeigen- Beziehungen anzeigen- Verwalten von Beziehungen- Kommentare anzeigen- Kommentare posten- Kommentare löschen- Links anzeigen- Links verwalten- Glossar anzeigen- Objekte verwalten
Laden	<ul style="list-style-type: none">- Ressource anzeigen- Ressource laden- Zeitpläne verwalten- Metadaten bereinigen- Ressource verwalten
Modell	<ul style="list-style-type: none">- Modell anzeigen- Modell verwalten- Modelle exportieren/importieren
Sicherheit	Katalogberechtigungen verwalten

Metadata Manager – Standardbenutzer

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Metadata Manager – Standardbenutzer“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Katalog	<ul style="list-style-type: none">- Herkunft anzeigen- Zugehörige Kataloge anzeigen- Katalog anzeigen- Beziehungen anzeigen- Kommentare anzeigen- Links anzeigen
Modell	Modell anzeigen

Metadata Manager – Fortgeschrittener Benutzer

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Metadata Manager – Fortgeschrittener Benutzer“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Katalog	<ul style="list-style-type: none">- Herkunft anzeigen- Zugehörige Kataloge anzeigen- Berichte anzeigen- Profilergebnisse anzeigen- Katalog anzeigen- Beziehungen anzeigen- Kommentare anzeigen- Kommentare posten- Kommentare löschen- Links anzeigen- Links verwalten- Glossar anzeigen
Laden	<ul style="list-style-type: none">- Ressource anzeigen- Ressource laden
Modell	Modell anzeigen

Benutzerdefinierte Rolle für den Operator

Die benutzerdefinierte Rolle für den Operator umfasst Berechtigungen für die Verwaltung, Planung und Überwachung von Anwendungsdiensten.

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Operator“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Anwendungsadministration	Anwendungen verwalten
Domänen-Administration	Dienstausführung verwalten
Verwaltung des Modellrepository-Diensts	Verwalten von teambasierter Entwicklung
Überwachen	<p>Die Überwachen-Berechtigungsgruppe enthält die folgenden Berechtigungen:</p> <ul style="list-style-type: none">- Ansicht: Jobs von anderen Benutzern anzeigen- Ansicht: Statistiken anzeigen- Ansicht: Berichte anzeigen- Zugriffsüberwachung: Zugriff über Analyst Tool- Zugriffsüberwachung: Zugriff über Developer Tool- Zugriffsüberwachung: Zugriff über Administrator Tool- Aktionen für Jobs durchführen <p>Hinweis: In einer Domäne, die die Kerberos-Authentifizierung verwendet, müssen Benutzer auch über die Administratorrolle für den Modellrepository-Dienst verfügen, der für die Überwachung konfiguriert wurde.</p>
Scheduler	<p>Die Scheduler-Berechtigungsgruppe enthält die folgenden Berechtigungen:</p> <ul style="list-style-type: none">- Geplante Jobs verwalten: Zeitplan erstellen- Geplante Jobs verwalten: Zeitplan löschen- Geplante Jobs verwalten: Zeitplan bearbeiten- Geplante Jobs verwalten: Zeitpläne anzeigen
Tools	Zugriff auf Informatica Administrator

PowerCenter-Repository-Dienst - Benutzerdefinierte Rollen

Die benutzerdefinierten Rollen des PowerCenter-Repository-Diensts umfassen den PowerCenter-Verbindungsadministrator, PowerCenter-Entwickler, PowerCenter-Operator und PowerCenter-Repository-Ordneradministrator.

PowerCenter – Verbindungsadministrator

Die folgende Tabelle enthält die die Standardberechtigungen, die der benutzerdefinierten Rolle "PowerCenter - Verbindungsadministrator" zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Tools	Workflow Manager öffnen
Globale Objekte	Verbindungen erstellen

PowerCenter – Entwickler

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „PowerCenter – Entwickler“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Tools	<ul style="list-style-type: none">- Designer öffnen- Workflow Manager öffnen- Workflow Monitor öffnen
Designobjekte	<ul style="list-style-type: none">- Erstellen, Bearbeiten und Löschen- Versionen verwalten
Quellen und Ziele	<ul style="list-style-type: none">- Erstellen, Bearbeiten und Löschen- Versionen verwalten
Laufzeitobjekte	<ul style="list-style-type: none">- Erstellen, Bearbeiten und Löschen- Ausführen- Versionen verwalten- Überwachen

PowerCenter – Operator

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „PowerCenter – Operator“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Tools	Workflow Monitor öffnen
Laufzeitobjekte	<ul style="list-style-type: none">- Ausführen- Ausführung verwalten- Überwachen

PowerCenter-Repository-Ordneradministrator

Die folgende Tabelle enthält die die Standardberechtigungen, die der benutzerdefinierten Rolle "PowerCenter - Repository-Ordneradministrator" zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Tools	Repository Manager öffnen
Ordner	<ul style="list-style-type: none">- Kopieren- Erstellen- Versionen verwalten
Globale Objekte	<ul style="list-style-type: none">- Bereitstellungsgruppen verwalten- Bereitstellungsgruppen werden ausgeführt- Beschriftungen erstellen- Berechtigung zum Erstellen von Anfragen

Benutzerdefinierte Rollen für den Berichterstellungsdienst

Die benutzerdefinierten Rollen des Berichterstellungsdiensts umfassen „Berichterstellungsdienst - Erweiterte Verbraucher“, „Berichterstellungsdienst - Erweiterter Provider“, „Berichterstellungsdienst - Standardverbraucher“, „Berichterstellungsdienst - Standardprovider“, „Berichterstellungsdienst -

Fortgeschrittene Verbraucher“, „Berichterstellungsdienst - Verbraucher mit Lesezugriff“ und „Berichterstellungsdienst - Schemadesigner“.

Berichterstellungsdienst – Erweiterte Verbraucher

Die folgende Tabelle enthält die die Standardberechtigungen, die der benutzerdefinierte Rolle "Berichterstellungsdienst - Erweiterte Verbraucher" zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Administration	<ul style="list-style-type: none"> - Schema pflegen - XML-Dateien exportieren/importieren - Benutzerzugriff verwalten - Zeitplan und Tasks einrichten - Systemeigenschaften verwalten - Abfragegrenzen einrichten - Echtzeit-Nachrichtenströme konfigurieren
Alarme	<ul style="list-style-type: none"> - Alarme erhalten - Echtzeitalarme erstellen - Zustelloptionen einrichten
Kommunikation	<ul style="list-style-type: none"> - Drucken - E-Mail-Objektverknüpfungen - E-Mail-Objekthinhalte - Exportieren - Export nach Excel oder CSV - Export nach Pivot-Tabellen - Diskussionen anzeigen - Diskussionen hinzufügen - Diskussionen verwalten - Feedback geben
Inhaltsverzeichnis	<ul style="list-style-type: none"> - Auf Inhaltsverzeichnis zugreifen - Erweiterte Suche öffnen - Inhaltsverzeichnis verwalten - Fortgeschrittene Suche verwalten
Dashboard	<ul style="list-style-type: none"> - Dashboards anzeigen - Persönliche Dashboards verwalten
Indikatoren	<ul style="list-style-type: none"> - Mit Indikatoren interagieren - Echtzeitindikatoren erstellen - Kontinuierliche, automatische Echtzeit-Indikatoraktualisierungen erhalten

Berechtigungsgruppe	Name der Berechtigung
Konten verwalten	Persönliche Einstellungen verwalten
Berichte	<ul style="list-style-type: none"> - Berichte anzeigen - Berichte analysieren - Mit Daten interagieren - Beliebigen Drill ausführen - Filtersätze erstellen - Benutzerdefinierte Metrik fortführen - Abfrage anzeigen - Lifecycle-Metadaten anzeigen - Berichten erstellen und löschen - Auf grundlegende Berichtserstellung zugreifen - Auf erweiterte Berichtserstellung zugreifen - Berichtskopien speichern - Berichte bearbeiten

Berichterstellungsdienst – Erweiterter Provider

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Berichterstellungsdienst – Erweiterter Provider“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Administration	Schema pflegen
Alarme	<ul style="list-style-type: none"> - Alarme erhalten - Echtzeitalarme erstellen - Zustelloptionen einrichten
Kommunikation	<ul style="list-style-type: none"> - Drucken - E-Mail-Objektverknüpfungen - E-Mail-Objektinhalte - Exportieren - Export nach Excel oder CSV - Export nach Pivot-Tabellen - Diskussionen anzeigen - Diskussionen hinzufügen - Diskussionen verwalten - Feedback geben
Inhaltsverzeichnis	<ul style="list-style-type: none"> - Auf Inhaltsverzeichnis zugreifen - Erweiterte Suche öffnen - Inhaltsverzeichnis verwalten - Fortgeschrittene Suche verwalten

Berechtigungsgruppe	Name der Berechtigung
Dashboards	<ul style="list-style-type: none"> - Dashboards anzeigen - Persönliche Dashboards verwalten - Dashboards erstellen, bearbeiten und löschen - Auf grundlegende Dashboarderstellung zugreifen - Auf erweiterte Dashboarderstellung zugreifen
Indikatoren	<ul style="list-style-type: none"> - Mit Indikatoren interagieren - Echtzeitindikatoren erstellen - Kontinuierliche, automatische Echtzeit-Indikatoraktualisierungen erhalten
Konten verwalten	Persönliche Einstellungen verwalten
Berichte	<ul style="list-style-type: none"> - Berichte anzeigen - Berichte analysieren - Mit Daten interagieren - Beliebigen Drill ausführen - Filtersätze erstellen - Benutzerdefinierte Metrik fortführen - Abfrage anzeigen - Lifecycle-Metadaten anzeigen - Berichten erstellen und löschen - Auf grundlegende Berichtserstellung zugreifen - Auf erweiterte Berichtserstellung zugreifen - Berichtskopien speichern - Berichte bearbeiten

Berichterstellungsdienst – Standardverbraucher

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Berichterstellungsdienst – Standardverbraucher“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Alarme	<ul style="list-style-type: none"> - Alarme erhalten - Zustelloptionen einrichten
Kommunikation	<ul style="list-style-type: none"> - Drucken - E-Mail-Objektverknüpfungen - Exportieren - Diskussionen anzeigen - Diskussionen hinzufügen - Feedback geben
Inhaltsverzeichnis	Auf Inhaltsverzeichnis zugreifen
Dashboards	Dashboards anzeigen

Berechtigungsgruppe	Name der Berechtigung
Konto verwalten	Persönliche Einstellungen verwalten
Berichte	<ul style="list-style-type: none"> - Berichte anzeigen - Berichte analysieren

Berichterstellungsdienst – Standardprovider

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Berichterstellungsdienst – Standardprovider“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Administration	Schema pflegen
Alarmer	<ul style="list-style-type: none"> - Alarmer erhalten - Echtzeitalarmer erstellen - Zustelloptionen einrichten
Kommunikation	<ul style="list-style-type: none"> - Drucken - E-Mail-Objektverknüpfungen - E-Mail-Objekthinhalte - Exportieren - Export nach Excel oder CSV - Export nach Pivot-Tabellen - Diskussionen anzeigen - Diskussionen hinzufügen - Diskussionen verwalten - Feedback geben
Inhaltsverzeichnis	<ul style="list-style-type: none"> - Auf Inhaltsverzeichnis zugreifen - Erweiterte Suche öffnen - Inhaltsverzeichnis verwalten - Fortgeschrittene Suche verwalten
Dashboards	<ul style="list-style-type: none"> - Dashboards anzeigen - Persönliche Dashboards verwalten - Dashboards erstellen, bearbeiten und löschen - Auf grundlegende Dashboarderstellung zugreifen
Indikatoren	<ul style="list-style-type: none"> - Mit Indikatoren interagieren - Echtzeitindikatoren erstellen - Kontinuierliche, automatische Echtzeit-Indikatoraktualisierungen erhalten

Berechtigungsgruppe	Name der Berechtigung
Konten verwalten	Persönliche Einstellungen verwalten
Berichte	<ul style="list-style-type: none"> - Berichte anzeigen - Berichte analysieren - Mit Daten interagieren - Beliebigen Drill ausführen - Filtersätze erstellen - Benutzerdefinierte Metrik fortführen - Abfrage anzeigen - Lifecycle-Metadaten anzeigen - Berichten erstellen und löschen - Auf grundlegende Berichtserstellung zugreifen - Auf erweiterte Berichtserstellung zugreifen - Berichtskopien speichern - Berichte bearbeiten

Berichterstellungsdienst – Fortgeschrittene Verbraucher

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Berichterstellungsdienst – Fortgeschrittene Verbraucher“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Alarme	<ul style="list-style-type: none"> - Alarme erhalten - Zustelloptionen einrichten
Kommunikation	<ul style="list-style-type: none"> - Drucken - E-Mail-Objektverknüpfungen - Exportieren - Export nach Excel oder CSV - Export nach Pivot-Tabellen - Diskussionen anzeigen - Diskussionen hinzufügen - Diskussionen verwalten - Feedback geben
Inhaltsverzeichnis	Auf Inhaltsverzeichnis zugreifen
Dashboards	<ul style="list-style-type: none"> - Dashboards anzeigen - Persönliche Dashboards verwalten
Indikatoren	<ul style="list-style-type: none"> - Mit Indikatoren interagieren - Kontinuierliche, automatische Echtzeit-Indikatoraktualisierungen erhalten

Berechtigungsgruppe	Name der Berechtigung
Konten verwalten	Persönliche Einstellungen verwalten
Berichte	<ul style="list-style-type: none"> - Berichte anzeigen - Berichte analysieren - Mit Daten interagieren - Lifecycle-Metadaten anzeigen - Berichtskopien speichern

Berichterstellungsdienst – Verbraucher mit Lesezugriff

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Berichterstellungsdienst – Verbraucher mit Lesezugriff“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Berichte	Berichte anzeigen

Berichterstellungsdienst – Schemadesigner

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Berichterstellungsdienst – Schemadesigner“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Administration	<ul style="list-style-type: none"> - Schema pflegen - Zeitplan und Tasks einrichten - Echtzeit-Nachrichtenströme konfigurieren
Alarmer	<ul style="list-style-type: none"> - Alarmer erhalten - Echtzeitalarmer erstellen - Zustelloptionen einrichten
Kommunikation	<ul style="list-style-type: none"> - Drucken - E-Mail-Objektverknüpfungen - E-Mail-Objekthinhalte - Exportieren - Export nach Excel oder CSV - Export nach Pivot-Tabellen - Diskussionen anzeigen - Diskussionen hinzufügen - Diskussionen verwalten - Feedback geben
Inhaltsverzeichnis	<ul style="list-style-type: none"> - Auf Inhaltsverzeichnis zugreifen - Erweiterte Suche öffnen - Inhaltsverzeichnis verwalten - Fortgeschrittene Suche verwalten

Berechtigungsgruppe	Name der Berechtigung
Dashboards	<ul style="list-style-type: none"> - Dashboards anzeigen - Persönliche Dashboards verwalten - Dashboards erstellen, bearbeiten und löschen
Indikatoren	<ul style="list-style-type: none"> - Mit Indikatoren interagieren - Echtzeitindikatoren erstellen - Kontinuierliche, automatische Echtzeit-Indikatoraktualisierungen erhalten
Konten verwalten	Persönliche Einstellungen verwalten
Berichte	<ul style="list-style-type: none"> - Berichte anzeigen - Berichte analysieren - Mit Daten interagieren - Beliebigen Drill ausführen - Filtersätze erstellen - Benutzerdefinierte Metrik fortführen - Abfrage anzeigen - Lifecycle-Metadaten anzeigen - Berichten erstellen und löschen - Auf grundlegende Berichtserstellung zugreifen - Auf erweiterte Berichtserstellung zugreifen - Berichtskopien speichern - Berichte bearbeiten

Benutzerdefinierte Rollen für den Test Data Manager-Dienst

Zu den benutzerdefinierten Rollen des Test Data Manager-Diensts gehören der Testdaten-Administrator, Testdatenentwickler, Testdaten-Projekt-DBA, Testdaten-Projektentwickler, Testdaten-Projekteigentümer, Testdaten-Risikomanager und Testdaten-Spezialist.

Testdaten-Administrator

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Testdaten-Administrator“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Projekte	Projekt prüfen
Verwaltung	<ul style="list-style-type: none"> - Verbindungen anzeigen - Verbindungen verwalten

Testdatenentwickler

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Testdaten-Entwickler“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Richtlinien	<ul style="list-style-type: none">- Richtlinien anzeigen- Richtlinien verwalten
Regeln	<ul style="list-style-type: none">- Maskierungsregeln anzeigen- Maskierungsregeln verwalten- Generierungsregeln anzeigen
Datendomänen	<ul style="list-style-type: none">- Datendomänen anzeigen- Datendomänen verwalten
Projekte	Projekt prüfen

Testdaten-Projekt-DBA

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Testdaten-Projekt-DBA“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Projekte	<ul style="list-style-type: none">- Projekt anzeigen- Projekt ausführen- Projekt überwachen- Projekt prüfen
Verwaltung	<ul style="list-style-type: none">- Verbindungen anzeigen- Verbindungen verwalten

Testdaten-Projektentwickler

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Testdaten-Projektentwickler“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Richtlinien	Richtlinien anzeigen
Regeln	<ul style="list-style-type: none">- Maskierungsregeln anzeigen- Generierungsregeln anzeigen
Datendomänen	Datendomänen anzeigen
Projekte	<ul style="list-style-type: none">- Projekt anzeigen- Projekt ermitteln- Projekt ausführen- Projekt überwachen- Projekt prüfen- Metadaten importieren

Berechtigungsgruppe	Name der Berechtigung
Datenmaskierung	<ul style="list-style-type: none"> - Datenmaskierung anzeigen - Datenmaskierung verwalten
Datenteilmenge	<ul style="list-style-type: none"> - Data Subset anzeigen - Data Subset verwalten
Datengenerierung	<ul style="list-style-type: none"> - Datengenerierung anzeigen - Datengenerierung verwalten
Verwaltung	<ul style="list-style-type: none"> - Verbindungen anzeigen - Verbindungen verwalten

Testdaten-Projekteigentümer

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Testdaten-Projekteigentümer“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Richtlinien	Richtlinien anzeigen
Regeln	<ul style="list-style-type: none"> - Maskierungsregeln anzeigen - Generierungsregeln anzeigen
Datendomänen	Datendomänen anzeigen
Projekte	<ul style="list-style-type: none"> - Projekt anzeigen - Projekt verwalten - Projekt ermitteln - Projekt ausführen - Projekt überwachen - Projekt prüfen - Metadaten importieren
Datenmaskierung	<ul style="list-style-type: none"> - Datenmaskierung anzeigen - Datenmaskierung verwalten
Datenteilmenge	<ul style="list-style-type: none"> - Data Subset anzeigen - Data Subset verwalten
Datengenerierung	<ul style="list-style-type: none"> - Datengenerierung anzeigen - Datengenerierung verwalten
Verwaltung	<ul style="list-style-type: none"> - Verbindungen anzeigen - Verbindungen verwalten

Testdaten-Risikomanager

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Testdaten-Risikomanager“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Richtlinien	Richtlinien anzeigen
Regeln	<ul style="list-style-type: none">- Maskierungsregeln anzeigen- Generierungsregeln anzeigen
Datendomänen	Datendomänen anzeigen
Projekte	Projekt prüfen

Testdaten-Spezialist

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Testdaten-Spezialist“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Richtlinien	Richtlinien anzeigen
Regeln	<ul style="list-style-type: none">- Maskierungsregeln anzeigen- Maskierungsregeln verwalten- Generierungsregeln anzeigen- Generierungsregeln verwalten
Datendomänen	<ul style="list-style-type: none">- Datendomänen anzeigen- Datendomänen verwalten
Projekte	<ul style="list-style-type: none">- Projekt verwalten- Projekt anzeigen- Projekt ermitteln- Projekt ausführen- Projekt überwachen- Projekt prüfen- Metadaten importieren
Datenmaskierung	<ul style="list-style-type: none">- Datenmaskierung anzeigen- Datenmaskierung verwalten
Datenteilmenge	<ul style="list-style-type: none">- Data Subset anzeigen- Data Subset verwalten
Datengenerierung	<ul style="list-style-type: none">- Datengenerierung anzeigen- Datengenerierung verwalten
Verwaltung	<ul style="list-style-type: none">- Verbindungen anzeigen- Verbindungen verwalten

Hinweis: Falls Sie ein Upgrade von Informatica-Dienst 9.6.1 auf Informatica-Dienst 9.6.1 HotFix 2 durchgeführt haben, kann ein Benutzer mit der Rolle „Testdaten-Spezialist“ keine Datengenerierungsregeln erstellen bzw. löschen. Die Rolle enthält nicht die Berechtigung zum Verwalten der Datengenerierung. Damit Benutzer mit dieser Rolle Datengenerierungsregeln erstellen und löschen können, müssen Sie die Rolle

manuell bearbeiten. Melden Sie sich beim Administrator-Tool an und bearbeiten Sie die benutzerdefinierte Rolle des Test Data Manager-Diensts, um die Berechtigung zum Verwalten von Generierungsregeln aus der Berechtigungsgruppe „Regeln“ einzubeziehen.

Konnektivität der Informatica-Plattform

Dieser Anhang umfasst die folgenden Themen:

- [Konnektivität der Informatica-Plattform - Übersicht, 341](#)
- [Domänen-Konnektivität, 342](#)
- [PowerCenter-Konnektivität, 344](#)
- [Native Konnektivität, 349](#)
- [ODBC-Konnektivität, 350](#)
- [JDBC-Konnektivität, 351](#)

Konnektivität der Informatica-Plattform - Übersicht

Die Informatica-Plattform verwendet die folgenden Konnektivitätstypen, um zwischen Clients, Diensten und anderen Komponenten in der Domäne zu kommunizieren:

TCP/IP-Netzwerkprotokoll

Anwendungsdienste und die Dienstmanager in einer Domäne verwenden TCP/IP-Netzwerkprotokoll zur Kommunikation mit anderen Knoten und Diensten. Auch die Clients verwenden TCP/IP, um mit Anwendungsdiensten zu kommunizieren. Wenn Sie Informatica-Dienste installieren, können Sie Hostnamen und Portnummer für die TCP/IP-Kommunikation auf einem Knoten konfigurieren. Sie können die Portnummern, die für Dienste auf einem Knoten verwendet werden, während der Installation oder im Informatica Administrator konfigurieren.

Native Treiber

Der Datenintegrationsdienst verwendet native Treiber, um mit Datenbanken zu kommunizieren. Der PowerCenter-Integrationsdienst und der PowerCenter-Repository-Dienst verwenden native Treiber, um mit Datenbanken zu kommunizieren. Native Treiber werden mit dem Datenbankserver und der Clientsoftware geliefert. Installieren und konfigurieren Sie die native Datenbank-Clientsoftware auf den Rechnern, auf denen die Dienste ausgeführt werden.

ODBC

Die ODBC-Treiber werden mit den Informatica-Diensten und Informatica-Clients installiert. Die Integrationsdienste verwenden ODBC-Treiber, um mit Datenbanken zu kommunizieren.

JDBC

Der Modellrepository-Dienst verwendet JDBC, um eine Verbindung mit der Modellrepository-Datenbank herzustellen. Der Berichterstellungsdienst verwendet JDBC, um eine Verbindung mit dem Data Analyzer-Repository und den Datenquellen herzustellen. Der Metadata Manager-Dienst verwendet JDBC, um eine Verbindung mit dem Metadata Manager-Repository und Metadaten-Quellen-Repositorys herzustellen.

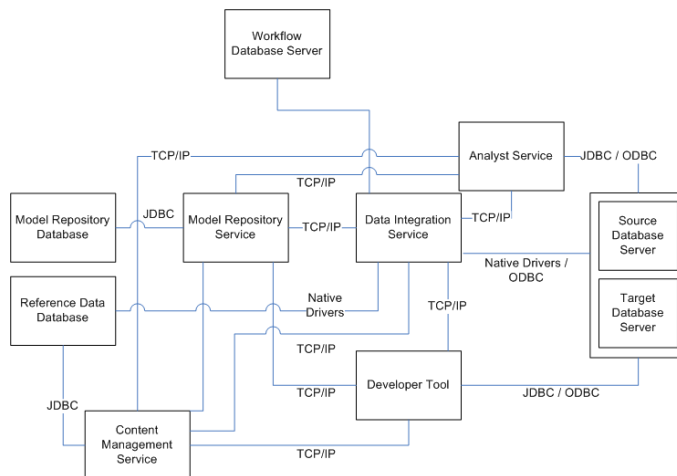
Die Gateway-Knoten in der Informatica-Domäne verwenden JDBC, um eine Verbindung mit dem Domänenkonfigurations-Repository herzustellen.

Domänen-Konnektivität

Dienste auf einem Knoten in einer Informatica-Domäne stellen mittels TCP/IP eine Verbindung zu Diensten auf anderen Knoten her. Da Dienste auf mehreren Knoten in einer Domäne ausgeführt werden können, berufen sie sich zum Weiterleiten von Anfragen auf den Dienstmanager. Der Dienstmanager auf dem Master-Gateway-Knoten wickelt Anfragen für Dienste ab und antwortet mit der Adresse des angefragten Dienstes.

Knoten kommunizieren mittels TCP/IP an dem Port, den Sie bei Installation von Informatica-Diensten für einen Knoten auswählen. Bei der Erstellung eines Knotens wählen Sie eine Portnummer für den Knoten aus. An diesem Port wartet der Dienstmanager auf eingehende TCP/IP-Verbindungen.

Die folgende Abbildung zeigt eine Übersicht der Konnektivität für Komponenten in:



Die Plattform nutzt Verbindungsobjekte, um Konnektivitätsdaten für Quell- und Zieldatenbanken zu definieren. Die Verbindungsobjekte können native oder ODBC-Konnektivität verwenden. Der Datenintegrationsdienst verwendet Verbindungsobjekte, um eine Verbindung zu Quellen und Zielen herzustellen.

Dienste und Clients stellen Verbindungen folgendermaßen her:

Modellrepository-Dienst

Der Modellrepository-Dienst verwendet JDBC zum Lesen oder Schreiben von Daten und Metadaten im Modellrepository. Er verwendet TCP/IP, um mit dem Datenintegrationsdienst und den Clients zu kommunizieren.

Datenintegrationsdienst

Der Datenintegrationsdienst verwendet ODBC oder native Treiber zum Herstellen einer Verbindung sowie zum Auslesen von Daten aus einer Quelldatenbank und Speichern der Daten in einer Zieldatenbank. Für

die Kommunikation mit dem Modellrepository-Dienst, dem Content-Managementdienst und den Client-Anwendungen wird TCP/IP genutzt.

Informatica Developer

Das Developer-Tool verwendet TCP/IP, um Datenumwandlungsanfragen an den Datenintegrationsdienst zu senden. TCP/IP wird für die Kommunikation mit dem Content-Managementdienst eingesetzt, um Referenztabelle und Dateien probabilistischer Modelle zu verwalten sowie Konfigurations- und Statusinformationen für Identitätspopulationsdateien und Dateien mit Adressvalidierungsreferenzdaten abzurufen. Wenn Sie sich eine Vorschau der Mappings oder Datenobjekte im Developer-Tool anzeigen lassen, verwendet es JDBC- oder ODBC-Treiber, um eine Verbindung zu der Quell- oder Zieldatenbank herzustellen und die für die Vorschau erforderlichen Metadaten abzurufen.

Informatica Analyst

Das Analyst-Tool verwendet TCP/IP, um Anfragen an den Datenintegrationsdienst zu senden. Es nutzt TCP/IP für die Kommunikation mit dem Content-Managementdienst zum Verwalten von Referenztabelle. Wenn Sie sich eine Vorschau der Profile oder Objekte im Analyst-Tool anzeigen lassen, verwendet es JDBC- oder ODBC-Treiber, um eine Verbindung zu der Quell- oder Zieldatenbank herzustellen und die für die Vorschau erforderlichen Metadaten abzurufen.

Wenn Sie ODBC verwenden, um eine Verbindung zu der Quell- oder Zieldatenbank herzustellen, dann installieren Sie den ODBC-Treiber auf dem Knoten, auf dem der Analyst-Dienst läuft.

Content-Managementdienst

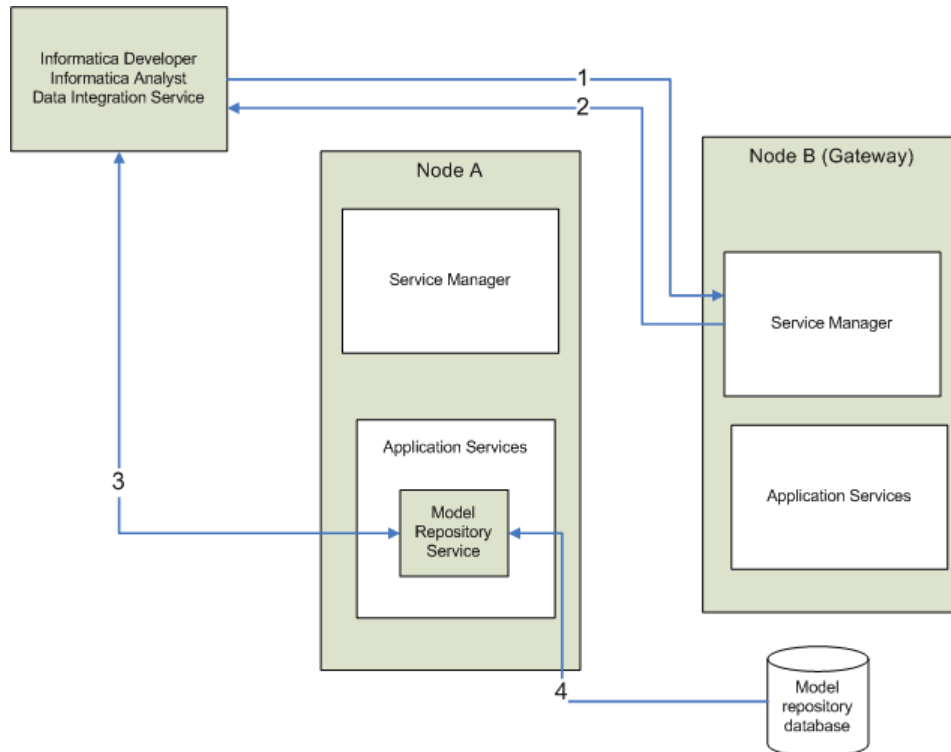
Der Content-Managementdienst verwaltet die Speicherorte und andere Eigenschaften für Referenzdaten. Der Content-Managementdienst verwendet TCP/IP zur Kommunikation mit dem Datenintegrationsdienst, um Daten in Referenztabelle zu lesen und zu schreiben. JDBC dient zur direkten Kommunikation mit dem Referenzdaten-Warehouse beim Erstellen der Referenztabelle.

Wenn mehrere Instanzen eines Content-Managementdienst in einer Informatica-Domäne existieren, aktualisiert die Masterversion des Content Managementdienstes den Datenintegrationsdienst. Die Masterversion des Content-Managementdienst verwendet TCP/IP zur Kommunikation mit dem Domänendienst, um den zu verwendenden Modellrepository-Dienst und Datenintegrationsdienst zu ermitteln.

Model Repository-Konnektivität

Der Model Repository Service stellt mithilfe von JDBC-Treibern eine Verbindung zum Model-Repository her. Informatica Developer, Informatica Analyst, Informatica Administrator und der Data Integration Service kommunizieren über TCP/IP mit dem Model Repository Service. Informatica Developer, Informatica Analyst und Data Integration Service sind Model-Repository-Clients.

In der nachstehenden Abbildung ist dargestellt, wie ein Model-Repository-Client eine Verbindung zur Model-Repository-Datenbank herstellt:



1. Ein Model-Repository-Client sendet eine Repository-Verbindungsanfrage an den Master-Gateway-Knoten; dieser stellt den Einstiegspunkt in die Domäne dar.
2. Der Service Manager sendet den Hostnamen und die Portnummer des Knotens zurück, auf dem der Model Repository Service ausgeführt wird. Im Diagramm wird der Model Repository Service auf Knoten A ausgeführt.
3. Der Repository-Client stellt eine TCP/IP-Verbindung mit dem Model Repository Service-Prozess auf Knoten A her.
4. Der Model Repository Service-Prozess kommuniziert über JDBC mit der Model-Repository-Datenbank. Basierend auf den Anfragen vom Model Repository-Client speichert der Model Repository Service-Prozess Objekte in oder ruft Objekte aus der Model-Repository-Datenbank ab.

Hinweis: Die Tabellen im Model-Repository verfügen über eine offene Architektur. Sie können die Repository-Tabellen zwar anzeigen, dürfen Sie jedoch niemals mittels anderer Dienstprogramme manuell ändern. Informatica haftet nicht für beschädigte Daten aufgrund von an den Repository-Tabellen oder den sich darin befindlichen Daten vorgenommenen Änderungen.

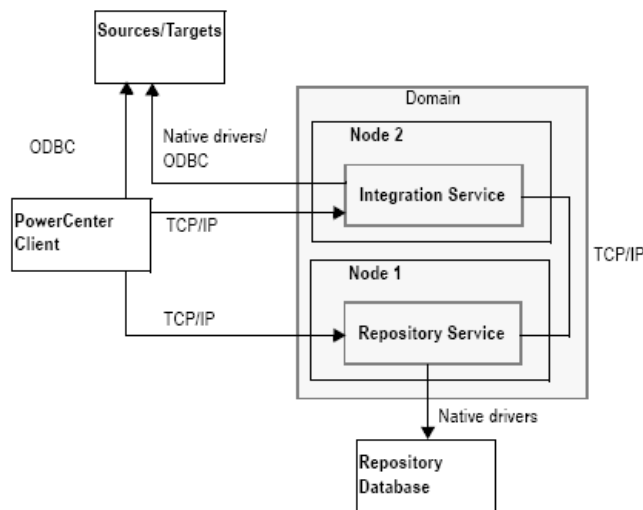
PowerCenter-Konnektivität

PowerCenter verwendet das TCP/IP-Netzwerkprotokoll, native Datenbanktreiber, ODBC und JDBC für die Kommunikation zwischen den folgenden PowerCenter-Komponenten:

- **PowerCenter Repository Service.** Der PowerCenter Repository Service verwendet native Treiber zum Kommunizieren mit dem PowerCenter-Repository. Der PowerCenter Repository Service verwendet TCP/IP zum Kommunizieren mit anderen PowerCenter-Komponenten.

- **PowerCenter Integration Service.** Der PowerCenter Integration Service verwendet die native Datenbankkonnektivität und ODBC zum Herstellen einer Verbindung zu Quell- und Zieldatenbanken. Der PowerCenter Integration Service verwendet TCP/IP zum Kommunizieren mit anderen PowerCenter-Komponenten.
- **Reporting Service und Metadata Manager Service.** Data Analyzer und Metadata Manager verwenden JDBC und ODBC für den Zugriff auf Datenquellen und Repositories.
- **PowerCenter Client.** PowerCenter Client verwendet ODBC zum Herstellen einer Verbindung zu Quell- und Zieldatenbanken. PowerCenter Client verwendet TCP/IP zur Kommunikation mit dem PowerCenter Repository Service und dem PowerCenter Integration Service.

Die nachstehende Abbildung bietet einen Überblick über die PowerCenter-Komponenten und -Konnektivität:



In der folgenden Tabelle sind die von den PowerCenter-Komponenten verwendeten Treiber aufgeführt:

Komponente	Datenbank	Treiber
PowerCenter Repository Service	PowerCenter Repository	Nativ
PowerCenter Integration Service	Quelle Target Gespeicherte Prozedur Lookup	Nativ ODBC
Reporting Service	Data Analyzer Repository	JDBC
Reporting Service	Datenquelle	JDBC ODBC mit JDBC-ODBC-Brücke
Metadata Manager Service	Metadata Manager Repository	JDBC
PowerCenter-Client	PowerCenter Repository	Nativ

Komponente	Datenbank	Treiber
PowerCenter-Client	Quelle Target Gespeicherte Prozedur Lookup	ODBC
Custom Metadata Configurator (Metadata Manager-Client)	Metadata Manager Repository	JDBC

Repository Service-Konnektivität

Der PowerCenter Repository Service verwaltet die Metadaten in der PowerCenter Repository-Datenbank. Alle Anwendungen, die eine Verbindung zum Repository herstellen, müssen dies auch zum PowerCenter Repository Service tun. Der PowerCenter Repository Service verwendet native Treiber zum Kommunizieren mit der Repository-Datenbank.

In der folgenden Tabelle ist die Konnektivität beschrieben, die für die Verbindung des Repository Service mit dem Repository sowie Quell- und Target-Datenbanken erforderlich ist.

Repository Service-Konnektivität	Anforderung für die Konnektivität
PowerCenter Client	TCP/IP
PowerCenter Integration Service	TCP/IP
PowerCenter Repository-Datenbank	Native Datenbanktreiber

Der PowerCenter Integration Service stellt eine Verbindung zum Repository Service her, um bei der Ausführung von Arbeitsabläufen Metadaten abzurufen

Verbinden über den PowerCenter Client

Um über den PowerCenter Client eine Verbindung zum PowerCenter Repository Service herzustellen, fügen Sie im PowerCenter Client-Tool eine Domäne und ein Repository hinzu. Beim Herstellen einer Verbindung über das PowerCenter Client-Tool sendet dieses eine Verbindungsanfrage an den Service Manager im Gateway-Knoten. Der Service Manager gibt den Hostnamen und die Portnummer des Knotens zurück, auf dem der PowerCenter Repository Service ausgeführt wird. Der PowerCenter Client stellt die Verbindung zum PowerCenter-Repository-Dienst über TCP/IP her.

Verbinden zu Datenbanken

Zum Einrichten einer Verbindung vom PowerCenter Repository Service zur Repository-Datenbank konfigurieren Sie die Datenbankeigenschaften in Informatica Administrator. Sie müssen die nativen Datenbanktreiber für die Repository-Datenbank auf dem Rechner installieren und konfigurieren, auf dem der PowerCenter Repository Service ausgeführt wird.

Integration Service-Konnektivität

Der PowerCenter Integration Service stellt eine Verbindung zum Repository her, um Repository-Objekte zu lesen. Der PowerCenter Integration Service stellt über den PowerCenter Repository Service eine Verbindung

zum Repository her. Verwenden Sie Informatica Administrator, um ein verbundenes Repository für den Integration Service zu konfigurieren.

In der folgenden Tabelle ist die Konnektivität beschrieben, die für die Verbindung des PowerCenter Integration Service mit den Plattformkomponenten sowie Quell- und Zieldatenbanken erforderlich ist:

PowerCenter Integration Service-Verbindung	Anforderung für die Konnektivität
PowerCenter-Client	TCP/IP
Andere PowerCenter Integration Service-Prozesse	TCP/IP
Repository Service	TCP/IP
Quell- und Zieldatenbanken	Native Datenbanktreiber oder ODBC Hinweis: Der PowerCenter Integration Service unter Windows und UNIX kann mithilfe von ODBC-Treibern eine Verbindung zu Datenbanken herstellen. Mit nativen Treibern kann die Leistung gesteigert werden.

Der PowerCenter Integration Service enthält ODBC-Bibliotheken, die zum Herstellen einer Verbindung zu anderen ODBC-Quellen verwendet werden kann. Die Informatica-Installation enthält ODBC-Treiber.

Bei Einfachdatei-, XML- oder COBOL-Quellen können Sie über Netzwerkverbindungen wie NFS auf Daten zugreifen oder Daten mittels FTP-Software auf den PowerCenter Integration Service-Knoten übertragen. Informationen zu Konnektivitätssoftware oder andere ODBC-Quellen finden Sie in der Dokumentation zu Ihrer Datenbank.

Verbinden über den PowerCenter Client

Der Workflow Manager kommuniziert über eine TCP/IP-Verbindung mit einem PowerCenter Integration Service-Vorgang. Der Workflow Manager kommuniziert jedes Mal, wenn Sie einen Arbeitsablauf starten oder Arbeitsablaufsdetails anzeigen, mit dem PowerCenter Integration Service.

Verbinden zum PowerCenter Repository Service

Bei Erstellung eines PowerCenter Integration Service legen Sie den PowerCenter Repository Service fest, der mit dem PowerCenter Integration Service verbunden werden soll. Wenn der PowerCenter Integration Service einen Arbeitsablauf ausführt, stellt es mittels TCP/IP eine Verbindung zum verbundenen PowerCenter Repository Service her und ruft Metadaten ab

Verbinden zu Datenbanken

Mithilfe des Workflow Manager können Sie Verbindungen zu Datenbanken erstellen. Sie können diese Verbindungen mit nativen Datenbanktreibern oder ODBC erstellen. Geben Sie bei Verwendung von nativen Treibern den Datenbankbenutzernamen, das Passwort und den nativen Verbindungs-String für jede Verbindung an. Der PowerCenter Integration Service verwendet diese Informationen zum Herstellen einer Verbindung zur Datenbank, wenn er die Sitzung ausführt

Hinweis: PowerCenter unterstützt ODBC-Treiber wie z. B. ISG Navigator, für die keine Benutzernamen und Passwörter erforderlich sind, um eine Verbindung herzustellen. Damit keine leeren Zeichenketten oder Nullen verwendet werden, verwenden Sie beim Konfigurieren einer Datenbankverbindung die reservierten Wörter PmNullUser für den Benutzernamen und PmNullPasswd für das Passwort. Der PowerCenter Integration Service behandelt PmNullUser und PmNullPasswd jeweils als keinen Benutzer und kein Passwort.

PowerCenter Client-Konnektivität

Der PowerCenter Client verwendet ODBC-Treiber und native Datenbank-Konnektivitätssoftware zur Kommunikation mit Datenbanken. Er kommuniziert über TCP/IP mit dem Integration Service und dem Repository.

In der folgenden Tabelle sind die Konnektivitätstypen beschrieben, die für die Verbindung des PowerCenter Client mit dem Integration Service, dem Repository sowie Quell- und Target-Datenbanken erforderlich sind.

PowerCenter Client-Konnektivität	Anforderung für die Konnektivität
Integration Service	TCP/IP
Repository Service	TCP/IP
Datenbank	ODBC-Verbindung für jede Datenbank

Verbinden zum Repository

Sie können mithilfe der PowerCenter Client-Tools eine Verbindung zum Repository herstellen. Alle PowerCenter Client-Tools verwenden TCP/IP zur Herstellung der Verbindung zum Repository über den Repository-Dienst, und dies jedes Mal, wenn Sie auf das Repository zugreifen, um Aufgaben wie das Herstellen einer Verbindung zum Repository, Erstellen von Repository-Objekten und Ausführen von Objektanfragen durchzuführen.

Verbinden zu Datenbanken

Zur Herstellung einer Verbindung zu Datenbanken über den Designer erstellen Sie mithilfe des Windows ODBC Data Source Administrator eine Datenquelle zu jeder Datenbank, auf die Sie zugreifen möchten. Wählen Sie die Namen der Datenquellen im Designer bei der Durchführung der folgenden Aufgaben:

- **Importieren einer Tabelle oder einer Definition einer gespeicherten Prozedur aus einer Datenbank**
Importieren einer Tabelle aus einer Datenbank mithilfe des Source Analyzer oder des Target Designer
Importieren einer gespeicherten Prozedur, einer Tabelle für eine Lookup-Umwandlung mithilfe des Transformation Developer, Maplet Designer oder Mapping Designer

Zum Herstellen einer Verbindung zur Datenbank müssen Sie außerdem Ihren Datenbankbenutzernamen, Ihr Passwort und den Namen des Eigentümers der Tabelle bzw. der gespeicherten Prozedur angeben.
- **Vorschau von Daten** Sie können den Namen der Datenquelle bei der Vorschau von Daten im Source Analyzer oder Target Designer auswählen. Sie müssen außerdem Ihren Datenbankbenutzernamen, Ihr Passwort und Ihren Tabelleneigentümernamen angeben.

Verbindung zum Integration Service

Workflow Manager und Workflow Monitor kommunizieren jedes Mal, wenn Sie mit Sitzungen und Arbeitsabläufen verbundene Aufgaben wie z. B. das Ausführen eines Arbeitsablaufs durchführen, über TCP/IP direkt mit dem Integration Service. Wenn Sie sich über Workflow-Manager oder Workflow-Monitor bei einem Repository anmelden, werden die Integration Services aufgelistet, die für dieses Repository in Informatica Administrator konfiguriert wurden.

Reporting Service- und Metadata Manager Service-Konnektivität

Der Reporting Service benötigt zur Herstellung einer Verbindung zu einem Data Analyzer-Repository einen Java Database Connectivity (JDBC)-Treiber. Zur Herstellung einer Verbindung zur Datenquelle kann der Reporting Service einen JDBC-Treiber oder eine JDBC-ODBC-Brücke mit einem ODBC-Treiber verwenden.

Der Metadata Manager Service benötigt zur Herstellung einer Verbindung zu einem Metadata Manager-Repository einen JDBC-Treiber. Der Custom Metadata Configurator verwendet einen JDBC-Treiber zur Herstellung einer Verbindung zum Metadata Manager-Repository.

JDBC-Treiber werden zusammen mit den Informatica-Diensten und -Clients installiert. Mithilfe des installierten JDBC-Treiber können Sie eine Verbindung zum Data Analyzer- oder Metadata Manager-Repository, der Datenquelle oder einem PowerCenter-Repository herstellen.

Die Informatica-Installationsprogramme installieren weder ODBC-Treiber noch die JDBC-ODBC-Brücke für den Reporting Service oder den Metadata Manager Service.

Native Konnektivität

Zur Herstellung einer nativen Konnektivität zwischen einem Anwendungsdienst und einer Datenbank müssen Sie die Datenbank-Client-Software auf dem Rechner installieren, auf dem der Dienst ausgeführt wird.

Der Data Integration Service verwendet native Treiber zum Kommunizieren mit Quell- und Target-Datenbanken.

PowerCenter Integration Service und PowerCenter Repository Service verwenden native Treiber zum Kommunizieren mit Quell- und Target-Datenbanken sowie Repository-Datenbanken.

In der nachstehenden Tabelle ist die Syntax für den nativen Verbindungs-String eines jeden unterstützten Datenbanksystems beschrieben:

Datenbank	Syntax der Verbindungszeichenfolge	Beispiel
IBM DB2	<i>dbname</i>	mydatabase
Microsoft SQL Server	<i>servername@dbname</i>	sqlserver@mydatabase
Oracle	<i>dbname.world</i> (identisch mit dem Eintrag TNSNAMES)	oracle.world
Sybase ASE	<i>servername@dbname</i>	sambrown@mydatabase Hinweis: Der Sybase ASE-Servername entspricht dem Namen des Adaptive Server aus der Schnittstellendatei.
Teradata	<i>ODBC_data_source_name</i> oder <i>ODBC_data_source_name@db_name</i> oder <i>ODBC_data_source_name@db_user_name</i>	TeradataODBC TeradataODBC@mydatabase TeradataODBC@sambrown Hinweis: Verwenden Sie Teradata-ODBC-Treiber zum Herstellen einer Verbindung zu Quell- und Target-Datenbanken.

ODBC-Konnektivität

Open Database Connectivity (ODBC) bietet eine gemeinsame Möglichkeit, mit unterschiedlichen Datenbanksystem zu kommunizieren.

Der Data Integration Service verwendet ODBC-Treiber, um eine Verbindung mit Datenbanken herzustellen.

PowerCenter Client verwendet ODBC-Treiber, um eine Verbindung mit Quell-, Target- und Lookup-Datenbanken herzustellen und die gespeicherten Prozeduren in Datenbanken aufzurufen. Der PowerCenter Integration Service kann ebenfalls ODBC-Treiber verwenden, um eine Verbindung mit Datenbanken herzustellen.

Um ODBC-Konnektivität zu verwenden, müssen Sie die folgenden Komponenten auf dem Computer installieren, der den Informatica-Dienst oder das Client-Tool hostet.

- **Datenbank-Clientsoftware.** Installieren Sie die Clientsoftware für das Datenbanksystem. Damit werden die Client-Bibliotheken installiert, die zur Herstellung einer Verbindung mit der Datenbank erforderlich sind.
Hinweis: Einige ODBC-Treiber enthalten Wire Protocols und benötigen keine Datenbank-Clientsoftware.
- **ODBC-Treiber.** Die geschlossenen DataDirect 32-Bit- oder 64-Bit-ODBC-Treiber werden bei der Installation der Informatica-Dienste installiert. Die geschlossenen DataDirect 32-Bit-ODBC-Treiber werden bei der Installation der Informatica-Clients installiert. Der Datenbankserver kann auch einen ODBC-Treiber enthalten.

Nach dem Installieren der erforderlichen Komponenten, müssen Sie eine ODBC-Datenquelle für jede Datenbank konfigurieren, zu der Sie eine Verbindung herstellen möchten. Eine Datenquelle enthält Informationen, die Sie benötigen, um die Datenbank zu finden und auf sie zuzugreifen, wie zum Beispiel Datenbankname, Benutzername und Datenbank-Passwort. Unter Windows verwenden Sie den ODBC-Datenquellen-Administrator, um einen Datenquellenamen zu erstellen. Unter UNIX fügen Sie Datenquelleneinträge zu der im Systemverzeichnis \$ODBCHOME gefundenen odbc.ini-Datei hinzu.

Wenn Sie eine ODBC-Datenquelle erstellen, müssen Sie auch den Treiber festlegen, dem der ODBC-Treiber-Manager Datenbankaufrufe sendet.

Die folgende Tabelle zeigt die empfohlenen ODBC-Treiber, die mit der jeweiligen Datenbank zu verwenden sind.

Datenbank	ODBC-Treiber	Benötigt Datenbank-Clientsoftware
Informix	DataDirect Informix Wire Protocol	Nein
Microsoft Access	Microsoft Access-Treiber	Nein
Microsoft Excel	Microsoft Excel-Treiber	Nein
Microsoft SQL Server	DataDirect SQL Server Wire Protocol	Nein
Netezza	Netezza SQL	Ja
Teradata	Teradata-ODBC-Treiber	Ja
SAP HANA	SAP HANA ODBC-Treiber	Ja

JDBC-Konnektivität

JDBC (Java Database Connectivity) ist eine Java-API, die für die Konnektivität von relationalen Datenbanken sorgt. Java-basierte Anwendungen können mithilfe von JDBC-Treibern eine Verbindung zu Datenbanken herstellen.

Die folgenden Dienste und Clients stellen mithilfe von JDBC eine Verbindung zu Datenbanken her:

- Datenintegrationsdienst
- Modellrepository-Dienst
- Informatica Developer
- Informatica Analyst
- Metadata Manager-Dienst
- Berichterstellungsdienst
- Custom Metadata Configurator

JDBC-Treiber werden zusammen mit den Informatica-Diensten und -Clients installiert.

Konfigurieren des Webbrowsers

- [Konfigurieren des Webbrowsers, 352](#)

Konfigurieren des Webbrowsers

Sie können das Administrator tool in den Webbrowsern Microsoft Internet Explorer oder Google Chrome ausführen.

Um das Administrator tool verwenden zu können, müssen Sie im Browser die folgenden Optionen konfigurieren:

Scripting und ActiveX

Aktivieren Sie die folgenden Steuerelemente in Microsoft Internet Explorer:

- Active Scripting
- Programmatischen Zugriff auf die Zwischenablage zulassen
- ActiveX-Steuerelemente und Plugins ausführen
- ActiveX-Steuerelemente ausführen, die für Scripting sicher sind

Um die Steuerelemente zu konfigurieren, klicken Sie auf **Extras > Internetoptionen > Sicherheit > Stufe anpassen**.

TLS 1.0

Wenn Sie HTTPS für Informatica Administrator in einer Domäne konfigurieren, die unter AIX ausgeführt wird, benötigt Internet Explorer TLS 1.0. Um TLS 1.0 zu aktivieren, klicken Sie auf **Tools > Internetoptionen > Erweitert**. Die Einstellung für TLS 1.0 befindet sich unter der Überschrift „Sicherheit“.

Vertrauenswürdige Sites

Wenn die Informatica-Domäne in einem Netzwerk mit Kerberos-Authentifizierung ausgeführt wird, müssen Sie den Browser für den Zugriff auf Informatica-Webanwendungen konfigurieren. Fügen Sie in Microsoft Internet Explorer und Google Chrome die URL der Informatica-Webanwendung zur Liste der vertrauenswürdigen Sites hinzu. Wenn Sie Chrome Version 41 oder höher verwenden, müssen Sie auch die Richtlinien `AuthServerWhitelist` und `AuthNegotiateDelegateWhitelist` festlegen.

ANHANG F

Sicherheitskonzepte

Dieser Anhang umfasst die folgenden Themen:

- [Was ist eine Gruppe?, 353](#)
- [Was ist ein Benutzer?, 353](#)
- [Was ist eine Rolle?, 354](#)
- [Was ist eine Berechtigung?, 354](#)
- [Was ist ein Betriebssystemprofil?, 354](#)

Was ist eine Gruppe?

Eine Gruppe ist eine Zusammenstellung von Benutzern und Gruppen, die dieselben Berechtigungen erhalten können. In einer Informatica-Domäne gibt es native Gruppen oder LDAP-Gruppen. Wenn Sie einer Gruppe eine Berechtigung, eine Rolle oder ein Privileg zuordnen, weisen Sie allen Benutzern und Untergruppen innerhalb dieser Gruppe dieselben Rolle, Berechtigung und dasselbe Privileg zu.

Gruppen in einer nativen Sicherheitsdomäne werden als native Gruppen bezeichnet. Sie können den Informatica Administrator zum Erstellen und Verwalten von nativen Gruppen nutzen. Eine native Gruppe kann native Benutzerkonten oder LDAP-Benutzerkonten haben.

Gruppen in einer nativen LDAP-Sicherheitsdomäne werden als LDAP-Gruppen bezeichnet. LDAP-Gruppen lassen sich im LDAP-Verzeichnisdienst erstellen und verwalten. Im Informatica Administrator können Sie jedoch keine LDAP-Gruppen oder LDAP-Gruppenzuweisungen erstellen oder löschen.

Was ist ein Benutzer?

Ein Benutzer ist eine Person, die ein Benutzerkonto in eine Informatica-Domäne besitzt. Ein Benutzer mit einem Konto in der Informatica-Domäne kann Tasks in Anwendungs-Clients ausführen.

Benutzer in einer nativen Sicherheitsdomäne werden als native Benutzer bezeichnet. Sie können den Informatica Administrator zum Erstellen und Verwalten von nativen Benutzerkonten verwenden.

Benutzer in einer nativen LDAP-Sicherheitsdomäne werden als LDAP-Benutzer bezeichnet. LDAP-Benutzerkonten lassen sich im LDAP-Verzeichnisdienst erstellen und verwalten. Im Informatica Administrator können Sie jedoch keine LDAP-Benutzer erstellen und löschen oder LDAP-Benutzerzuweisungen ändern.

Was ist eine Rolle?

Eine Rolle ist eine Zusammenstellung von Privilegien, die einem Benutzer und Gruppen zugewiesen werden können. Sie können eine vom System definierte Rolle zuweisen oder eigene Rollen für Benutzer und Gruppen zusammenstellen und diese zuweisen.

Eine systemeigene Rolle lässt sich nicht bearbeiten oder löschen. Die Rolle des Administrators ist beispielsweise eine systemeigene Rolle.

Eine benutzerdefinierte Rolle lässt sich hingegen erstellen, bearbeiten und löschen.

Was ist eine Berechtigung?

Berechtigungen legen die Aktionen fest, die ein Benutzer in den Anwendungs-Clients ausführen kann. Sie können Benutzern und Gruppen einer Domäne für jeden der nachfolgend aufgeführten Anwendungsdienste in der Domäne Berechtigungen zuweisen: Metadata Manager-Dienst, Modellrepository-Dienst, PowerCenter-Repository-Dienst und Berichterstellungsdienst.

Sie können den Benutzern und Gruppen auch Rollen zuweisen, um die Aktionen festzulegen, die diese ausführen dürfen. Eine Rolle ist eine Zusammenstellung von Berechtigungen.

Was ist ein Betriebssystemprofil?

Ein Betriebssystemprofil legt eine Sicherheitsstufe fest, die der PowerCenter-Integrationsdienst bei der Ausführung von Arbeitsabläufen berücksichtigt. Das Betriebssystemprofil enthält den Benutzernamen des Betriebssystems, die Dienstprozessvariablen und die Umgebungsvariablen. Der PowerCenter-Integrationsdienst führt die Arbeitsabläufe mit den Systemberechtigungen des Betriebssystembenutzers aus, sowie den Einstellungen, die im Betriebssystemprofil definiert sind. Wenn der PowerCenter-Integrationsdienst Betriebssystemprofile verwendet, sollten Sie die Betriebssystemprofile den Arbeitsabläufen zuweisen, wenn Sie Ordneigenschaften definieren oder wenn Sie einen Arbeitsablauf manuell starten. Um einen Arbeitsablauf zu starten, dem ein Betriebssystembenutzer zugewiesen ist, müssen Sie über Berechtigungen in dem Betriebssystemprofil verfügen, das der PowerCenter-Integrationsdienst zum Ausführen des Arbeitsablaufs verwendet.

INDEX

A

- Abhängigkeiten
 - Anwendungsdienste [79](#)
 - Dienste und Knoten anzeigen [79](#)
 - Gitter [79](#)
 - Knoten [79](#)
- Adabas-Verbindungen
 - Eigenschaften [106](#)
- Administrator Tool
 - Berichte [233](#)
 - Codepage [263](#)
 - Fehlerprotokoll, anzeigen [192](#)
 - Logs, anzeigen [187](#)
- Aktivitätsdaten
 - Web Services Report [241](#)
- Alarme
 - abonnieren [58](#)
 - anzeigen [59](#)
 - Benachrichtigungs-E-Mail [59](#)
 - Beschreibung [20](#)
 - konfigurieren [58](#)
 - nachverfolgen [59](#)
 - verwalten [57](#)
- Alarme abonnieren
 - Benutzereinstellungen [33](#)
- Allgemeine Eigenschaften
 - Informatica-Domäne [82](#)
 - Lizenz [178](#)
- Analyst Service
 - application service [39](#)
 - Log-Ereignisse [195](#)
- Analyst-Dienst
 - benutzerdefinierte Rollen [324](#)
- ändern
 - Passwort für Benutzerkonto [32](#)
- Anmeldung
 - Fehlerbehebung [31](#)
- Ansicht Dienste und Knoten.
 - Informatica Administrator [38](#)
- Anwendungen
 - überwachen [212](#)
- Anwendungsdienste
 - Abhängigkeiten [79](#)
 - aktivieren [63](#)
 - Belastbarkeit, konfigurieren [94](#)
 - deaktivieren [63](#)
 - Entfernen [64](#)
 - Lizenzen, zuweisen [175](#)
- Anwendungsdienste.
 - Lizenzen, Aufheben der Zuordnung [176](#)
- Anwendungsdienstprozess
 - aktivieren [63](#)
 - angehaltener Status [63](#)
 - deaktivieren [63](#)
 - Fehlerstatus [63](#)

- Anwendungsdienstprozess (Fortsetzung)
 - Standby-Status [63](#)
 - Status [63](#)
- Anwendungsquellen
 - Codepage [265](#)
- Anwendungstargets
 - Codepage [266](#)
- anzeigen
 - Abhängigkeiten für Dienste und Knoten [79](#)
- application service process
 - port assignment [23](#)
- application services
 - Analyst Service [39](#)
 - Content Management Service [39](#)
 - Data Integration Service [39](#)
 - description [23](#)
 - Metadata Manager Service [39](#)
 - Model Repository Service [39](#)
 - overview [39](#)
 - PowerCenter Integration Service [39](#)
 - PowerCenter Repository Service [39](#)
 - PowerExchange Listener Service [39](#)
 - PowerExchange Logger Service [39](#)
 - Reporting and Dashboards Service [39](#)
 - Reporting Service [39](#)
 - SAP BW Service [39](#)
 - Ultra Messaging Service [39](#)
 - Web Services Hub [39](#)
- Arbeitsablauf-Wiederherstellung
 - Übersicht [227](#)
 - wird ausgeführt [229](#)
- Arbeitsabläufe
 - abbrechen [227](#)
 - Protokolle [229](#)
 - Status [222](#)
 - überwachen [220](#)
 - Wiederherstellen [229](#)
- as
 - Berechtigungen per Befehl [295](#)
- ASCII-Modus
 - Übersicht [258](#)
- Aufgaben
 - Status [224](#)
- Authentifizierung
 - Protokollereignisse [194](#)
- Automatische Auswahl
 - Netzwerk, hohe Verfügbarkeit [97](#)
- Autorisierung
 - Dienstmanager [20](#)
 - Protokollereignisse [194](#)

B

- Backup-Verzeichnis
 - Knoteneigenschaft [67](#)

- bearbeiten
 - Verbindungen [102](#)
- Befehl BackupDomain
 - Beschreibung [73](#)
- Befehlszeilenprogramme
 - Belastbarkeit, konfigurieren [96](#)
 - Berechtigungen [295](#)
- Belastbarkeit
 - Anwendungsdienst [89](#)
 - Anwendungsdienstkonfiguration [94](#)
 - Befehlszeilenprogramm-Konfiguration [96](#)
 - im exklusiven Modus [96](#)
 - PowerCenter Client [88](#)
 - PowerCenter-Integrationsdienst [89](#)
 - PowerCenter-Repository-Dienst [89](#)
 - TCP KeepAlive-Timeout [97](#)
- Benutzer
 - Lizenzaktivität, überwachen [233](#)
 - Übersicht [50](#)
- Benutzeraktivität
 - Protokollierungsereignis-Kategorien [198](#)
- Benutzerdefinierte Eigenschaften
 - Domäne [86](#)
- Benutzerdefinierte Eigenschaften anzeigen (Eigenschaft)
 - Benutzereinstellungen [33](#)
- benutzerdefinierte Filter
 - Abgelaufene Zeit [232](#)
 - Datum und Uhrzeit [231](#)
 - Mehrfachauswahl [232](#)
- benutzerdefinierte Rollen
 - Analyst-Dienst [324](#)
 - Operator [327](#)
- Benutzerdefinierte Rollen
 - Berichterstellungsdienst [330](#)
 - Metadata Manager-Dienst [325](#)
 - PowerCenter-Repository-Dienst [328](#)
- Benutzerdetail
 - Lizenzverwaltungsbericht [237](#)
- Benutzereinstellungen
 - bearbeiten [32](#)
 - Beschreibung [33](#)
- Benutzerkonten
 - Ändern des Passworts [32](#)
 - verwalten [30](#)
- Benutzerschemata
 - Beschreibung [257](#)
- Benutzerverwaltung
 - Protokollereignisse [194](#)
- Benutzerzusammenfassung
 - Lizenzverwaltungsbericht [236](#)
- Berechtigungen
 - as Befehle [295](#)
 - Befehlszeilenprogramme [295](#)
 - dis-Befehle [296](#)
 - ipc Befehle [298](#)
 - isp Befehle [298](#)
 - MRS-Befehle [309](#)
 - ms Befehle [310](#)
 - oie Befehle [311](#)
 - pmcmd-Befehle [315](#)
 - pmrep-Befehle [318](#)
 - ps Befehl [311](#)
 - px - Befehle [312](#)
 - rtn Befehlsprogramme [313](#)
 - sql-Befehle [313](#)
 - wfs-Befehle [315](#)
- Bereinigen
 - Protokoll-Manager [186](#)

- Bereitgestellte Mapping-Jobs
 - Überwachen [213](#)
- Berichte
 - Administrator Tool [233](#)
 - Domäne [233](#)
 - Lizenz [233](#)
 - überwachen [205](#)
 - Web Services [233](#)
- Berichterstellungsdienst
 - Benutzerdefinierte Rollen [330](#)
- Betriebsmodus
 - Auswirkungen auf die Belastbarkeit [96](#)

C

- catalina.out
 - Fehlersuche [185](#)
- COBOL
 - Konnektivität [346](#)
- Codepage Relaxation
 - Konfigurieren des Integration Service [271](#)
- Codepage-Entspannung
 - Dateninkonsistenzen [270](#)
 - Fehlersuche [271](#)
 - Übersicht [270](#)
- Codepage-Lockerung
 - kompatible Codepages, auswählen [271](#)
- Codepage-Validierung
 - Entspannte Validierung [270](#)
 - Übersicht [269](#)
- Codepages
 - Administrator Tool [263](#)
 - Anwendungsquellen [265](#)
 - Anwendungstargets [266](#)
 - auswählen [261](#)
 - Benutzerdefinierte Umwandlung [267](#)
 - Beschreibungen [284](#)
 - Beziehungen [269](#)
 - Datenbank für gespeicherte Prozeduren [267](#)
 - Datenintegrationsdienst-Prozess [282](#)
 - Domänenkonfigurationsdatenbank [263](#)
 - Einfachdatei-Targets [266](#)
 - Entspannte Validierung für Quellen und Targets [270](#)
 - Flatfile-Quellen [265](#)
 - ID [284](#)
 - Kompatibilität - Übersicht [261](#)
 - Kompatibilitätsdiagramm [267](#)
 - Lookup-Datenbank [267](#)
 - Metadata Manager Service [265](#)
 - Namen [284](#)
 - pmcmd [264](#)
 - PowerCenter Integration Service-Prozess [264](#)
 - PowerCenter-Client [264](#)
 - PowerCenter-Integrationsdienst-Prozess [282](#)
 - Quellen [265](#), [284](#)
 - Relationale Quellen [265](#)
 - Relationale Targets [266](#)
 - Sortierreihenfolge - Übersicht [264](#)
 - Speicher [264](#), [282](#)
 - Targets [266](#)
 - Übersicht [259](#)
 - Umwandlung [272](#)
 - Umwandlung externer Verfahren [267](#)
 - UNIX [260](#)
 - Unterstützte Codepages [282](#), [284](#)
 - Validierung [269](#)
 - Windows [261](#)

- Codepages (*Fortsetzung*)
 - Ziele [284](#)
- Conexões JDBC
 - propriedades [135](#)
- Configuration Support Manager
 - zur Analyse der Knotendiagnostik verwenden [252](#)
 - zur Knotendiagnose [248](#)
- Content Management Service
 - application service [39](#)
- Content-Managementdienst
 - Konnektivität [342](#)
- CPU-Detail
 - Lizenzverwaltungsbericht [235](#)
- CPU-Profil
 - Knoteneigenschaft [67](#)
- CPU-Zusammenfassung
 - Lizenzverwaltungsbericht [235](#)
- CPUs
 - Überschreiten des Grenzwerts [235](#)

D

- Data Analyzer
 - JDBC-ODBC-Brücke [349](#)
 - Konnektivität [349](#)
 - ODBC (Open Database Connectivity) [341](#)
- Data Integration Service
 - application service [39](#)
 - Protokollereignisse [195](#)
- Data Integration Services
 - Überwachung [210](#)
- DataDirect ODBC-Treiber
 - plattformspezifische Treiber erforderlich [350](#)
- DataSift-Verbindungen
 - Eigenschaften [109](#)
- Dateien für die garantierte Meldungsauslieferung
 - Protokoll-Manager [183](#)
- Datenbank
 - Domänenkonfiguration [72](#)
- Datenbankeigenschaften
 - Informatica-Domäne [83](#)
- Datenbanktreiber
 - Integrationsdienst [341](#)
 - Repository-Dienst [341](#)
- Datenbankverbindungen
 - Aktualisierung für Domänenkonfiguration [76](#)
- Datenintegrationsdienst
 - Konnektivität [342](#)
 - Wiederherstellung [92](#)
- Datenintegrationsdienst-Prozess
 - Unterstützte Codepages [282](#)
- Datenobjekt-Zwischenspeicherung
 - mit Pass-Through-Sicherheit [104](#)
- Datenverschiebungsmodus
 - ändern [258](#)
 - ASCII [258](#)
 - Auswirkungen auf Sitzungsdateien und Cache-Speicher [258](#)
 - Beschreibung [257](#)
 - Übersicht [257](#)
 - Unicode [258](#)
- Deaktivierungsmodus
 - PowerCenter Integration Services und Dienstprozesse [63](#)
- Dienste und Knoten
 - Abhängigkeiten anzeigen [79](#)
- Dienstmanager
 - Autorisierung [20](#)
 - Beschreibung [20](#)

- Dienstname
 - Protokollereignisse [193](#)
- dis
 - Berechtigungen per Befehl [296](#)
- Domäne
 - Benutzeraktivität, überwachen [233](#)
 - Benutzersicherheit [62](#)
 - Berichte [233](#)
 - Protokollereigniskategorien [194](#)
- Domänen
 - mehrere [56](#)
- Domänen-Bericht
 - Web Services-Bericht [240](#)
- Domänen-Konfigurationsdatenbank
 - Aktualisieren [76](#)
 - Migrieren [74](#)
 - Sichere Datenbank [84](#)
 - Verbindung für Gateway-Knoten [76](#)
 - Wiederherstellen [73](#)
- Domänenberichte
 - ausführen [233](#)
 - Lizenzverwaltungsbericht [233](#)
- Domäneneigenschaften
 - Informatica-Domäne [81](#)
- Domänenkonfiguration
 - Beschreibung [72](#)
 - Migrieren [74](#)
 - Protokollereignisse [194](#)
- Domänenkonfigurationsdatenbank
 - Beschreibung [72](#)
 - Codepage [263](#)
 - sichern [73](#)
- Durchschn. Anz. der Ausführungsinstanzen (Eigenschaft)
 - Web Services Report [241](#)
- Durchschn. Anz. der Dienstpartitionen (Eigenschaft)
 - Web Services Report [241](#)
- Durchschn. DTM-Zeit (Eigenschaft)
 - Web Services Report [241](#)
- Durchschnittliche Dienstzeit (Eigenschaft)
 - Web Services Report [241](#)

E

- Einfachdateien
 - Konnektivität [346](#)
 - Logs exportieren [192](#)
 - Quell-Codepage [265](#)
 - Target-Codepage [266](#)
- Eingabe-Gebietsschemata
 - IME (Windows Input Method Editor) [257](#)
 - konfigurieren [257](#)
- Einstellungen
 - überwachen [209](#)

F

- Facebook-Verbindungen
 - Eigenschaften [110](#)
- Failover
 - Anwendungsdienst [92](#)
 - Domäne [91](#)
- Fallstudie
 - ISO 8859-1 Datenverarbeitung [273](#)
 - Verarbeiten von Unicode UTF-16LE Daten [276](#)
- Fehler protokollieren
 - Administrator Tool [192](#)

Fehlerbehebung
 anmelden [31](#)
 Kerberos-Authentifizierung [31](#)
Fehlersuche
 catalina.out [185](#)
 Codepage-Entspannung [271](#)
 localhost_.txt [185](#)
 node.log [185](#)
 Umgebungsvariablen [65](#)
FTP
 Erreichen hoher Verfügbarkeit [97](#)

G

Gateway
 verwalten [72](#)
Gateway-Knoten
 Beschreibung [20](#)
 konfigurieren [72](#)
 Log-Verzeichnis [72](#)
 Protokollieren [184](#)
gateways
 Status [224](#)
GB18030
 Beschreibung [255](#)
Gebietsschemata
 Übersicht [256](#)
gespeicherte Prozeduren
 Codepages [267](#)
Gitter
 Abhängigkeiten [79](#)
 Registerkarten des Informatica Administrators [45](#)
Globale Einstellungen
 konfigurieren [208](#)
Globalisierung
 Übersicht [254](#)
Grafikanzeige-Server
 Anforderung [233](#)
Greenplum-Verbindungen
 Eigenschaften [111](#)
Gruppen
 Übersicht [49](#)

H

Hardwarekonfiguration
 Lizenzverwaltungsbericht [237](#)
HBase connections
 properties [112](#)
HDFS connections
 properties [113](#)
Herunterfahren
 Informatica-Domäne [81](#)
Hive-Verbindungen
 Eigenschaften [114](#)
Hohe Verfügbarkeit
 Beschreibung [28, 87](#)
 Failover [91](#)
 Neustart [91](#)
 TCP KeepAlive-Timeout [97](#)
 Wiederherstellung [92](#)
HTTP-Verbindungen
 Eigenschaften [121](#)

IBM DB2
 Verbindungszeichenfolge, Syntax [349](#)
IBM DB2 für i5/OS-Verbindungen
 Eigenschaften [125](#)
IBM DB2 für z/OS-Verbindungen
 Eigenschaften [129](#)
IBM DB2-Verbindungen
 Eigenschaften [123](#)
IME (Windows Input Method Editor)
 Eingabe-Gebietsschemata [257](#)
IMS-Verbindungen
 Eigenschaften [132](#)
Informatica Administrator
 anmelden [30](#)
 Ansicht Dienste und Knoten. [38](#)
 Dienste, Aktivieren und Deaktivieren [63](#)
 Dienstprozess, Aktivieren und Deaktivieren [63](#)
 Navigator [48](#)
 Registerkarte "Protokolle" [46](#)
 Registerkarte "Überwachen" [47](#)
 Registerkarte Berichte [47](#)
 Registerkarte Domäne [36](#)
 Registerkarten, anzeigen [34](#)
 Sicherheitsseite [48](#)
 Suche wird ausgeführt [48](#)
 Übersicht [34, 56](#)
Informatica Analyst
 Konnektivität [342](#)
Informatica Cloud
 Cloud-Organisationen [279, 281](#)
 Cloud-Verbindungen [281](#)
 Eigenschaften von Cloud-Organisationen [280](#)
 Übersicht [279](#)
Informatica Data Explorer
 Konnektivität [342](#)
Informatica Data Quality
 Konnektivität [342](#)
Informatica Data Services
 Konnektivität [342](#)
Informatica Developer
 Konnektivität [342](#)
Informatica MySupport-Portal
 anmelden [249](#)
Informatica-Domäne
 Alarme [58](#)
 Allgemeine Eigenschaften [82](#)
 Benutzersicherheit [62](#)
 Berechtigungen [62](#)
 Beschreibung [18](#)
 Datenbankeigenschaften [83](#)
 Domänen-Konfigurationsdatenbank [84](#)
 Domäneneigenschaften [81](#)
 Herunterfahren [81](#)
 mehrere Domänen [56](#)
 Neu starten [81](#)
 Protokoll- und Gateway-Konfiguration [84](#)
 Status der Operationen [92](#)
Information and Content Exchange (ICE)
 Protokolldateien [192](#)
Inkrementelle Schlüssel
 Lizenzen [173](#)
Innerhalb des Neustartzeitraums (Eigenschaft)
 Informatica-Domäne [64](#)
Integration Service
 Konnektivität [346](#)

Integrationsdienst
 ODBC (Open Database Connectivity) [341](#)
ipc
 Berechtigungen per Befehl [298](#)
isp
 Berechtigungen per Befehl [298](#)

J

JDBC (Java Database Connectivity)
 Übersicht [351](#)
JDBC-ODBC-Brücke
 Data Analyzer [349](#)
JDBC-Treiber
 Data Analyzer [341](#)
 Data Analyzer-Verbindung zum Repository [349](#)
 installierte Treiber [349](#)
 Metadata Manager [341](#)
 Metadata Manager-Verbindung zu Datenbanken [349](#)
 PowerCenter-Domäne [341](#)
 Referenztabellen-Manager [341](#)
Jobs
 überwachen [211](#)

K

Kategorie
 Domänenprotokollereignisse [194](#)
Kerberos-Authentifizierung
 Fehlerbehebung [31](#)
Knoten
 Abhängigkeiten [79](#)
 Beschreibung [18](#), [20](#)
 Eigenschaften [65](#)
 Entfernen [71](#)
 Gateway [20](#), [72](#)
 Herunterfahren [70](#)
 Host-Namen und Portnummer, Entfernen [67](#)
 konfigurieren [67](#)
 Log Manager [193](#)
 Neu starten [70](#)
 Portnummer [67](#)
 Register im Informatica Administrator [44](#)
 Starten [70](#)
 TCP/IP-Netzwerkprotokoll [341](#)
 verwalten [65](#)
 Worker [20](#)
Knotendiagnostik
 analysieren [252](#)
 herunterladen [251](#)
Knotendiagnostiken [248](#)
Knoteneigenschaften
 Backup-Verzeichnis [67](#)
 CPU-Profil [67](#)
 konfigurieren [65](#), [67](#)
 Maximale Anzahl der Prozesse [67](#)
 Maximale Länge der CPU-Ausführungswarteschlange [67](#)
 Maximale Speichergröße in Prozent [67](#)
Knotenkonfiguration
 Lizenzverwaltungsbericht [238](#)
 Protokollereignisse [194](#)
kompatibel
 definiert für die Codepage-Kompatibilität [261](#)
Kompatibilität
 zwischen Codepages [261](#)
 zwischen Quell- und Target-Codepages [271](#)

Konnektivität
 COBOL [346](#)
 Content-Managementdienst [342](#)
 Data Analyzer [349](#)
 Datenintegrationsdienst [342](#)
 Diagramm des [341](#)
 Informatica Analyst [342](#)
 Informatica Developer [342](#)
 Integration Service [346](#)
 Metadata Manager [349](#)
 Modellrepository-Dienst [342](#)
 PowerCenter Client [348](#)
 PowerCenter Repository Service [346](#)
 Übersicht [341](#)
 Verbindungszeichenfolge, Beispiele [349](#)

Konten
 Ändern des Passworts [32](#)
 verwalten [30](#)

L

LANG_C Umgebungsvariable
 Gebietsschema unter UNIX einrichten [260](#)
Laufzeitstatistiken
 Web Services-Bericht [243](#)
LC_ALL Umgebungsvariable
 Gebietsschema unter UNIX einrichten [260](#)
LinkedIn-Verbindungen
 Eigenschaften [138](#)
Listener Service Logs
 Log-Ereignisse [195](#)
Lizenz
 Aktualisieren [176](#)
 Allgemeine Eigenschaften [178](#)
 Aufheben der Zuordnung von einem Dienst [176](#)
 Details, anzeigen [178](#)
 einem Dienst zuweisen [175](#)
 Entfernen [177](#)
 erstellen [174](#)
 Lizenzdatei [174](#)
 Log-Ereignisse [197](#)
 Protokollereignisse [194](#)
 Register im Informatica Administrator [45](#)
 Schlüssel [173](#)
 Validierung [172](#)
 verwalten [173](#)
Lizenzierte Optionen
 Lizenzverwaltungsbericht [238](#)
Lizenzierung
 Lizenzverwaltungsbericht [234](#)
 Log-Ereignisse [196](#)
 verwalten [173](#)
Lizenzierungsprotokolle
 Protokollereignisse [172](#)
Lizenznutzung
 Protokollereignisse [194](#)
Lizenzschlüssel
 Inkrementell [173](#), [176](#)
 Ursprünglich [173](#)
Lizenzverwaltungsbericht
 ausführen [233](#)
 Benutzerdetail [237](#)
 Benutzerzusammenfassung [236](#)
 CPU-Detail [235](#)
 CPU-Zusammenfassung [235](#)
 Hardwarekonfiguration [237](#)
 Knotenkonfiguration [238](#)

Lizenzverwaltungsbericht (Fortsetzung)

- Lizenzierte Optionen [238](#)
- Lizenzierung [234](#)
- Multibyte-Zeichen [239](#)
- Per E-Mail [240](#)
- Repository-Zusammenfassung [236](#)
- Unicode-Schriftart [239](#)
- wird ausgeführt [239](#)
- localhost_.txt
 - Fehlersuche [185](#)
- Log Agent
 - Beschreibung [182](#)
 - Protokollereignisse [194](#)
- Log Manager
 - catalina.out [185](#)
 - Dienstname [193](#)
 - Fehlersuche [185](#)
 - Knoten [193](#)
 - konfigurieren [187](#)
 - Log-Ereignisse des PowerCenter Integration Service [196](#)
 - Log-Ereignisse des PowerCenter Repository Service [197](#)
 - Log-Ereignisse des SAP NetWeaver BI [198](#)
 - Log-Ereignisse, bereinigen [186](#)
 - Log-Ereignisse, speichern [190](#)
 - Logs, anzeigen [187](#)
 - Meldungscode [193](#)
 - message [193](#)
 - node.log [185](#)
 - ProcessID [193](#)
 - Protokollereignisse - Komponenten [193](#)
 - Schweregradstufen [193](#)
 - Sicherheits-Audit-Trail [197](#)
 - Thread [193](#)
 - Zeitstempel [193](#)
 - Zeitzone [186](#)
- Log-Ereignisdateien
 - Bereinigen [186](#)
- Log-Ereignisse
 - anzeigen [187](#)
 - Exportieren mit Mozilla Firefox [190](#)
 - Lizenzierung [196](#), [197](#)
 - PowerCenter Repository Service [197](#)
 - Sicherheits-Audit-Trail [197](#)
 - speichern [190](#)
 - Speichern [190](#)
 - Web Services Hub [198](#)
 - Zeitzone [186](#)
- Log-Verzeichnis
 - für Gateway-Knoten [72](#)
- Logger Service Logs
 - Log-Ereignisse [196](#)
- Logische CPUs
 - Berechnung [235](#)
- Logische Datenobjekte
 - Überwachung [215](#)
- Logs
 - anzeigen [187](#)
 - Speichern [190](#)
- Lookup-Datenbanken
 - Codepages [267](#)
- löschen
 - Verbindungen [102](#)

M

- Master-Gateway-Knoten
 - Beschreibung [20](#)

- Maximale Anzahl der Prozesse
 - Knoteneigenschaft [67](#)
- Maximale Anzahl Neustartversuche (Eigenschaft)
 - Informatica-Domäne [64](#)
- Maximale Länge der CPU-Ausführungswarteschlange
 - Knoteneigenschaft [67](#)
- Maximale Speichergröße in Prozent
 - Knoteneigenschaft [67](#)
- Meldungscode
 - Log Manager [193](#)
- Metadata Manager
 - Konnektivität [349](#)
 - ODBC (Open Database Connectivity) [341](#)
- Metadata Manager Service
 - application service [39](#)
 - Codepage [265](#)
 - Log-Ereignisse [196](#)
- Metadata Manager-Dienst
 - Benutzerdefinierte Rollen [325](#)
- Metadaten
 - Auswählen von Zeichen [272](#)
 - Zum Repository hinzufügen [272](#)
- Microsoft SQL Server
 - Verbindungszeichenfolge, Syntax [349](#)
- migrieren
 - Domänenkonfiguration [74](#)
- Model Repository Service
 - application service [39](#)
- Modellrepository-Dienst
 - Konnektivität [342](#)
 - Protokollereignisse [196](#)
- MRS
 - Berechtigungen nach Befehl [309](#)
 - Berechtigungen per Befehl [309](#)
- ms
 - Berechtigungen per Befehl [310](#)
- MS SQL Server-Verbindungen
 - Eigenschaften [139](#)
- Multibyte-Daten
 - Eingeben in den PowerCenter Client [257](#)

N

- Navigator
 - Registerkarte Domäne [36](#)
 - Sicherheitsseite [48](#)
- Netzwerk
 - Hohe Verfügbarkeit [97](#)
- Neustart
 - Anwendungsdienst [92](#)
- Neustarten
 - Konfigurieren für PowerCenter Integration Service-Prozesse [64](#)
- NLS_LANG
 - Einstellung Gebietsschema [274](#), [277](#)
- node.log
 - Fehlersuche [185](#)
- nodemeta.xml
 - für Gateway-Knoten [72](#)

O

- ODBC (Open Database Connectivity)
 - Anforderung für PowerCenter Client [348](#)
 - DataDirect-Treiberprobleme [350](#)
 - Integrationsdienst [341](#)
 - Konnektivität herstellen [350](#)

ODBC (Open Database Connectivity) (Fortsetzung)

Metadata Manager [341](#)

PowerCenter Client [341](#)

ODBC-Verbindungen

Eigenschaften [142](#)

oie

Berechtigungen per Befehl [311](#)

Operator}

benutzerdefinierte Rollen [327](#)

Oracle

Einstellung Gebietsschema mit NLS_LANG [274](#), [277](#)

Verbindungszeichenfolge, Syntax [349](#)

Oracle-Verbindungen

Eigenschaften [143](#)

Ordner

Administrator Tool [59](#)

Entfernen [61](#)

erstellen [59](#), [60](#)

Objekte, verschieben [60](#)

Übersicht [39](#)

verwalten [59](#)

Originalschlüssel

Lizenzen [173](#)

P

Pass-Through-Sicherheit

Cache aktivieren [104](#)

Operations-Mappings bei Web-Diensten [103](#)

Verbindung mit einem SQL-Datendienst [103](#)

Verbindungen hinzufügen [104](#)

Passwort

Ändern für ein Benutzerkonto [32](#)

pmcmd

Berechtigungen nach Befehl [315](#)

Berechtigungen per Befehl [315](#)

Codepage-Probleme [264](#)

Kommunizieren mit dem PowerCenter Integration Service [264](#)

PmNullPasswd

reserviertes Wort [347](#)

PmNullUser

reserviertes Wort [347](#)

pmrep

Berechtigungen nach Befehl [318](#)

Berechtigungen per Befehl [318](#)

port

application service [23](#)

Port

Bereich für Dienstprozesse [67](#)

Knoten [67](#)

Knoten-Maximalwert [67](#)

Knoten-Minimalwert [67](#)

PowerCenter

Konnektivität [341](#)

PowerCenter Client

Belastbarkeit [88](#)

Konnektivität [348](#)

Multibyte-Zeichen, eingeben [257](#)

ODBC (Open Database Connectivity) [341](#)

TCP/IP-Netzwerkprotokoll [341](#)

PowerCenter Integration Service

Aktivieren und Deaktivieren [63](#)

application service [39](#)

Log-Ereignisse [196](#)

PowerCenter Integration Service-Prozess

Aktivieren und Deaktivieren [63](#)

Codepage [264](#)

PowerCenter Integration Service-Prozess (Fortsetzung)

Neustart, konfigurieren [64](#)

Status anzeigen [70](#)

PowerCenter Repository Service

Anforderungen für die Konnektivität [346](#)

application service [39](#)

Log-Ereignisse [197](#)

PowerCenter Sicherheit

verwalten [48](#)

PowerCenter-Client

Codepage [264](#)

PowerCenter-Domänen

Konnektivität [344](#)

TCP/IP-Netzwerkprotokoll [341](#)

PowerCenter-Integrationsdienst

Belastbarkeit [89](#)

Failover-Konfiguration [95](#)

Status der Operationen [92](#)

Tabellen zur Hochverfügbarkeits-Persistenz [95](#)

Wiederherstellung [92](#)

Wiederherstellungskonfiguration [95](#)

PowerCenter-Integrationsdienst-Prozess

Unterstützte Codepages [282](#)

PowerCenter-Repository-Dienst

Belastbarkeit [89](#)

Benutzerdefinierte Rollen [328](#)

Status der Operationen [92](#)

Wiederherstellung [92](#)

PowerExchange Listener Service

application service [39](#)

PowerExchange Logger Service

application service [39](#)

ProcessID

Log Manager [193](#)

Meldungscode [193](#)

Protokoll- und Gateway-Konfiguration

Informatica-Domäne [84](#)

Protokoll-Manager

Architektur [183](#)

Bereinigen [186](#)

Domänenprotokollereignisse [194](#)

Protokollereignisse [194](#)

Protokollereignisse der Benutzeraktivität [198](#)

verwenden [182](#)

Verzeichnis-Speicherort, Konfigurieren [185](#)

Protokolle

Arbeitsablauf [229](#)

Benutzeraktivität [198](#)

Bereinigen [186](#)

Domäne [194](#)

Komponenten [193](#)

konfigurieren [185](#)

PowerCenter Integration Service [196](#)

PowerCenter Repository Service [197](#)

SAP BW Service [198](#)

Speicherort [185](#)

Protokollereignisdateien

Beschreibung [183](#)

Protokollereignisse

Arbeitsablauf [229](#)

Authentifizierung [194](#)

Autorisierung [194](#)

Benutzeraktivität [198](#)

Benutzerverwaltung [194](#)

Beschreibung [183](#)

Code [193](#)

Details, anzeigen [187](#)

Dienstname [193](#)

Protokollereignisse (Fortsetzung)

- Domäne [194](#)
- Domänenfunktionskategorien [193](#)
- Domänenkonfiguration [194](#)
- Knoten [193](#)
- Knotenkonfiguration [194](#)
- Komponenten [193](#)
- Lizenzierung [194](#)
- Lizenzierungsnutzung [194](#)
- Lizenzierungsprotokolle [172](#)
- Log Agent [194](#)
- Meldungscode [193](#)
- message [193](#)
- Protokoll-Manager [194](#)
- Schweregradstufen [193](#)
- Service Manager [194](#)
- Thread [193](#)
- Zeitstempel [193](#)
- Protokollmanager
 - Wiederherstellung [184](#)
- Protokollverzeichnis
 - Speicherort, Konfigurieren [185](#)
- Proz. Anteil verwendeter Partitionen (Eigenschaft)
 - Web Services Report [241](#)
- Prozessidentifikationsnummer
 - Log Manager [193](#)
- ps
 - Berechtigungen per Befehl [311](#)
- pwX
 - Berechtigungen nach Befehl [312](#)
 - Berechtigungen per Befehl [312](#)

Q

- Quelldatenbanken
 - Codepage [265](#)
- Quellen
 - Codepages [265](#), [284](#)

R

- Registerkarte "Protokolle"
 - Informatica Administrator [46](#)
- Registerkarte "Überwachen"
 - Informatica Administrator [47](#)
- Registerkarte „Verwalten“
 - Ansicht Verbindungen [46](#)
- Registerkarte Berichte
 - Informatica Administrator [47](#)
- Registerkarte Domäne
 - Ansicht Dienste und Knoten. [36](#)
 - Informatica Administrator [36](#)
 - Navigator [36](#)
- Reporting and Dashboards Service
 - application service [39](#)
- Reporting Service
 - application service [39](#)
- Repository-Metadaten
 - Auswählen von Zeichen [272](#)
- Repository-Zusammenfassung
 - Lizenzverwaltungsbericht [236](#)
- Repositories
 - Backup-Verzeichnis [67](#)
 - Codepages [264](#)
 - Unicode [255](#)
 - Unterstützte Codepages [282](#)

Repositorys (Fortsetzung)

- UTF-16LE [255](#)
- Rollen
 - Übersicht [50](#)
- rtm
 - Berechtigungen per Befehl [313](#)

S

- SAP BW Service
 - application service [39](#)
 - Log-Ereignisse [198](#)
- SAP-Verbindungen
 - Eigenschaften [146](#)
- Schwellenwert für die Ressourcenbereitstellung
 - Einstellung für Knoten [67](#)
- Sequenzielle Verbindungen
 - Eigenschaften [148](#)
- Service Manager
 - Protokollereignisse [194](#)
- Severity levels
 - Protokollereignisse [193](#)
- Sicherheit
 - Audit Trail [197](#)
 - Berechtigungen [62](#)
- Sicherheitsseite
 - Informatica Administrator [48](#)
 - Navigator [48](#)
- sichern
 - Domänenkonfigurationsdatenbank [73](#)
- Sitzungen
 - Sortierreihenfolge [264](#)
- SMTP-Konfiguration
 - Alarmer [58](#)
- Sortierreihenfolge
 - Codepage [264](#)
- sql
 - Berechtigungen nach Befehl [313](#)
 - Berechtigungen per Befehl [313](#)
- SQL-Datendienste
 - Überwachung [216](#)
- Stacktraces
 - anzeigen [187](#)
- Statistik
 - zum Überwachen [204](#)
- Statistiken
 - Web Services Hub [240](#)
- Status der Operationen
 - Domäne [92](#)
 - PowerCenter-Integrationsdienst [92](#)
 - PowerCenter-Repository-Dienst [92](#)
- Stoppen
 - Informatica-Domäne [81](#)
- Suchbereich
 - Informatica Administrator [48](#)
- Sybase ASE
 - Verbindungszeichenfolge, Syntax [349](#)
- Systemgebietsschemata
 - Beschreibung [257](#)

T

- Tabellen zur Hochverfügbarkeits-Persistenz
 - PowerCenter-Integrationsdienst [95](#)
- Target-Datenbanken
 - Codepage [266](#)

- Targets
 - Codepages [266](#)
- TCP KeepAlive-Timeout
 - Hohe Verfügbarkeit [97](#)
- TCP/IP-Netzwerkprotokoll
 - Anforderung für Integration Service [348](#)
 - Knoten [341](#)
 - PowerCenter Client [341](#)
 - PowerCenter-Domänen [341](#)
- Teilmenge
 - definiert für die Codepage-Kompatibilität [261](#)
- Teradata
 - Verbindungszeichenfolge, Syntax [349](#)
- testen
 - Datenbankverbindungen [102](#)
- Thread-Identifizierung
 - Registerkarte "Protokolle" [193](#)
- Threads
 - Log Manager [193](#)
- Twitter-Streaming-Verbindungen
 - Eigenschaften [153](#)
- Twitter-Verbindungen
 - Eigenschaften [152](#)

U

- Übergeordnete Menge
 - definiert für die Codepage-Kompatibilität [261](#)
- Übersicht
 - Verbindungen [99](#)
- überwachen
 - Anwendungen [212](#)
 - Arbeitsabläufe [220](#)
 - Berichte [205](#)
 - Beschreibung [201](#)
 - Einstellungen, konfigurieren [209](#)
 - Jobs [211](#)
 - Statistik [204](#)
- Überwachen
 - Bereitgestellte Mapping-Jobs [213](#)
- überwachung
 - Globale Einstellungen, Konfigurieren [208](#)
- Überwachung
 - Data Integration Services [210](#)
 - Logische Datenobjekte [215](#)
 - Setup [208](#)
 - SQL-Datendienste [216](#)
 - Web-Dienste [219](#)
- UCS-2
 - Beschreibung [255](#)
- Ultra Messaging Service
 - application service [39](#)
- Umgebungsvariablen
 - Fehlersuche [65](#)
 - LANG_C [260](#)
 - LC_ALL [260](#)
 - LC_CTYPE [260](#)
 - NLS_LANG [274](#), [277](#)
- Unicode
 - GB18030 [255](#)
 - Repositorys [255](#)
 - UCS-2 [255](#)
 - UTF-16 [255](#)
 - UTF-16LE [255](#)
 - UTF-32 [255](#)
- Unicode-Modus
 - Übersicht [258](#)

- UNIX
 - Codepages [260](#)
- UNIX-Umgebungsvariablen
 - LANG_C [260](#)
 - LC_ALL [260](#)
 - LC_CTYPE [260](#)
- UTF-16
 - Beschreibung [255](#)
- UTF-16LE
 - Beschreibung [255](#)
 - Speicher [264](#)
- UTF-32
 - Beschreibung [255](#)

V

- validieren
 - Codepages [269](#)
 - Lizenzen [172](#)
- Verbinden von
 - SQL-Datendienst [103](#)
- Verbindungen
 - aktualisieren [101](#)
 - bearbeiten [102](#)
 - Erstellen von Datenbankverbindungen [100](#)
 - löschen [102](#)
 - Pass-Through-Sicherheit [103](#)
 - Pass-Through-Sicherheit hinzufügen [104](#)
 - testen [102](#)
 - Übersicht [99](#)
 - Web Services-Eigenschaften [158](#)
- Verbindungs-Strings
 - native Konnektivität [349](#)
- Verbindungspooling
 - Eigenschaften [105](#)
- Verbindungszeichenfolge
 - Beispiele [349](#)
 - Syntax [349](#)
- verknüpfte Domäne
 - mehrere Domänen [56](#)
- verwalten
 - Benutzerkonten [30](#)
 - Konten [30](#)
- Vollständige Historienstatistik
 - Web Services-Bericht [245](#)
- VSAM-Verbindungen
 - Eigenschaften [154](#)

W

- Web Content-Kapow Katalyst-Verbindungen
 - Eigenschaften [157](#)
- Web Services Hub
 - Anwendungsdienst [28](#)
 - application service [39](#)
 - Log-Ereignisse [198](#)
 - Statistiken [240](#)
- Web Services Report
 - Aktivitätsdaten [241](#)
 - Durchschn. Anz. der Ausführungsinstanzen (Eigenschaft) [241](#)
 - Durchschn. Anz. der Dienstpartitionen (Eigenschaft) [241](#)
 - Durchschn. DTM-Zeit (Eigenschaft) [241](#)
 - Durchschnittliche Dienstzeit (Eigenschaft) [241](#)
 - Inhalt [241](#)
 - Proz. Anteil verwendeter Partitionen (Eigenschaft) [241](#)

- Web Services-Bericht
 - Laufzeitstatistiken [243](#)
 - Vollständige Historienstatistik [245](#)
- Web-Dienste
 - Überwachung [219](#)
- Web-Verbindungen
 - Eigenschaften [121](#)
- wfs
 - Berechtigungen per Befehl [315](#)
- Wiederherstellen
 - Domänen-Konfigurationsdatenbank [73](#)
- Wiederherstellung
 - Datenintegrationsdienst [92](#)
 - Hohe Verfügbarkeit [92](#)
 - Integration Service [92](#)
 - PowerCenter-Repository-Dienst [92](#)
- Worker-Knoten
 - Beschreibung [20](#)
 - Konfigurieren als Gateway [72](#)

X

- X Virtual Frame Buffer
 - für Lizenzbericht [233](#)

- X Virtual Frame Buffer (*Fortsetzung*)
 - für Web-Dienste-Bericht [233](#)
- XML
 - Logs exportieren in [191](#)

Z

- Zeichengrößen
 - Doppeltes Byte [261](#)
 - Einfaches Byte [261](#)
 - Multibyte [261](#)
- Zeitstempel
 - Log Manager [193](#)
- Zeitzone
 - Log Manager [186](#)
- Ziele
 - Codepages [284](#)
- zu Datenbanken verbinden
 - JDBC [349](#)