Informatica

Informatica®
10.1.1 HotFix 1

Installations- und Konfigurationshandbuch

Informatica Installations- und Konfigurationshandbuch
10.1.1 HotFix 1

© Copyright Informatica LLC 1998, 2018

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

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

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

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

Teile dieser Software und/oder 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 GARANTIEN ODER KONDITIONEN IRGENDEINER ART, weder ausdrücklich noch impliziert. Berechtigungen und Einschränkungen für bestimmte Sprachen finden Sie in der Lizenz.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

HINWEISE

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

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

Die in dieser Dokumentation enthaltenen Informationen können jederzeit ohne vorherige Ankündigung geändert werden. Wenn Sie Probleme in dieser Dokumentation finden, zeigen Sie uns diese bitte schriftlich an: Informatica LLC 2100 Seaport Blvd. Redwood City, CA 94063, USA.

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

Publikationsdatum: 2018-07-02

Inhalt

Einleitung 13

Informatica-Ressourcen. 13

Informatica-Netzwerk. 13

Informatica-Wissensdatenbank. 13

Informatica-Dokumentation. 14

Informatica-Produktverfügbarkeitsmatrizen. 14

Informatica Velocity. 14

Informatica Marketplace. 14

Globaler Kundensupport von Informatica. 14

Teil I: Installation - Übersicht. 15

Kapitel 1: Installation - Übersicht. 16

Installation von Informatica. 16

Installationsvorgang. 17

Teil II: Vor dem Installieren der Dienste. 18

Kapitel 2: Planen der Domäne. 19

Einführung in die Informatica-Domäne. 19

Domäne mit einem oder mehreren Knoten. 19

Knoten. 20

Dienstmanager. 21

Anwendungsdienste. 21

Lizenzschlüssel. 22

Benutzerauthentifizierung. 22

Verschlüsselungsschlüssel für sicheren Datenspeicher. 22

Domänensicherheit. 23

Informatica-Clients. 23

Informatica Administrator 24

Planungsprozess für die Domäne. 25

Geteilte Domäne für Metadata Manager. 25

Überlegungen zu geteilten Domänen. 26

Planen der Anwendungsdienste. 27

Anwendungsdienste nach Produkt. 27

Analyst-Dienst. 28

Content-Managementdienst. 29

Datenintegrationsdienst. 30

Metadata Manager-Dienst. 31

Modellrepository-Dienst. 32

PowerCenter-Integrationsdienst. . . . 32
PowerCenter-Repository-Dienst. . . . 33
Suchdienst. . . . 33
Webdienst-Hub. . . . 34
Überprüfen der Systemvoraussetzungen. . . . 35
Überprüfen der Installationsanforderungen für Dienste. . . . 35
Überprüfen der Anforderungen an temporären Festplattenspeicher. . . . 35
Überprüfen der Portanforderungen. . . . 35
Überprüfen der Datenbankanforderungen. . . . 37
Überprüfen der Hardwarevoraussetzungen für Anwendungsdienste. . . . 38
Aufzeichnen der Informatica-Domänen- und -Knoteninformationen. . . . 39
Benennungskonventionen für Datenobjekte. . . . 40
Domäne. . . . 41
Knoten. . . . 42
Anwendungsdienste. . . . 42
Datenbanken. . . . 43
Sicherer Datenspeicher. . . . 46
Domänensicherheit. . . . 46
Kerberos-Authentifizierung. . . . 48

Kapitel 3: Vorbereiten von Datenbanken für die Informatica-Domäne 49

Vorbereiten von Datenbanken für die Informatica-Domäne - Übersicht. . . . 49
Einrichten von Datenbankbenutzerkonten. . . . 50
Datenbankanforderungen des Domänen-Konfigurations-Repositorys. . . . 50
IBM DB2-Datenbankanforderungen. . . . 51
Microsoft SQL Server-Datenbankanforderungen. . . . 52
Oracle-Datenbankanforderungen. . . . 52
Sybase ASE-Datenbankanforderungen. . . . 53
Anforderungen für Datenobjekt-Cache-Datenbank. . . . 54
IBM DB2-Datenbankanforderungen. . . . 54
Microsoft SQL Server-Datenbankanforderungen. . . . 54
Oracle-Datenbankanforderungen. . . . 55
Anforderungen an die Audit-Datenbank der Ausnahmeverwaltung. . . . 55
IBM DB2-Datenbankanforderungen. . . . 55
Microsoft SQL Server-Datenbankanforderungen. . . . 56
Oracle-Datenbankanforderungen. . . . 56
Metadata Manager Repository-Datenbankanforderungen. . . . 56
IBM DB2-Datenbankanforderungen. . . . 57
Microsoft SQL Server-Datenbankanforderungen. . . . 58
Oracle-Datenbankanforderungen. . . . 59
Modellrepository-Datenbankanforderungen. . . . 60
IBM DB2-Datenbankanforderungen. . . . 60
Microsoft SQL Server-Datenbankanforderungen. . . . 61

Oracle-Datenbankanforderungen. 61
PowerCenter-Repository-Datenbankanforderungen. 62
IBM DB2-Datenbankanforderungen. 62
Microsoft SQL Server-Datenbankanforderungen. 62
Oracle-Datenbankanforderungen. 62
Sybase ASE-Datenbankanforderungen. 63
Anforderungen an das Profiling-Warehouse. 64
IBM DB2-Datenbankanforderungen. 64
Microsoft SQL Server-Datenbankanforderungen. 64
Oracle-Datenbankanforderungen. 65
Anforderungen des Referenzdaten-Warehouse. 65
IBM DB2-Datenbankanforderungen. 66
Microsoft SQL Server-Datenbankanforderungen. 66
Oracle-Datenbankanforderungen. 66
Anforderungen an Arbeitsablauf-Datenbanken. 67
IBM DB2-Datenbankanforderungen 67
Microsoft SQL Server-Datenbankanforderungen. 67
Oracle-Datenbankanforderungen. 68
Konfigurieren der nativen Konnektivität auf dem Dienst-Computer. 68
Installieren der Datenbank-Client-Software. 70
Konfigurieren von Datenbank-Client-Umgebungsvariablen auf UNIX. 70
Verbindungszeichenfolge für eine sichere Datenbank. 71

Kapitel 4: Vorbereiten der Einrichtung der Kerberos-Authentifizierung. 73

Vorbereiten der Einrichtung der Kerberos-Authentifizierung - Übersicht. 73
Einrichten der Kerberos-Konfigurationsdatei. 74
Generieren des Namensformats für Dienstprinzipale und Keytab-Dateien. 75
Dienstprinzipalanforderungen auf der Knotenebene. 76
Dienstprinzipalanforderungen auf Prozessebene. 76
Ausführen des Kerberos SPN-Formatgenerators von Informatica unter Windows. 77
Ausführen des Kerberos SPN-Formatgenerators von Informatica unter UNIX. 79
Überprüfen der SPN- und Keytab-Format-Textdatei. 80
Erstellen der Dienstprinzipalnamen und Keytab-Dateien. 82
Fehlerbehebung bei den Dienstprinzipalnamen und Keytab-Dateien. 83

Kapitel 5: Vor der Installation der Dienste unter Windows. 86

Vor der Installation der Dienste unter Windows - Übersicht. 86
Lesen der Versionshinweise. 86
Überprüfen Sie die Patch Anforderungen. 87
Data Transformation-Dateien sichern. 87
Überprüfen der Umgebungsvariablen. 87
Erstellen eines Systembenutzerkontos. 88
Einrichten von Schlüsselspeicher- und Truststore-Dateien. 88

Extrahieren der Dateien des Installationsprogramms. 90
Überprüfen Sie den Lizenzschlüssel. 91
Ausführen des Vorinstallations-Systemprüfungstools (i10Pi). 91

Kapitel 6: Vor der Installation von Diensten unter UNIX. 94

Vor der Installation von Diensten unter UNIX - Übersicht. 94
Lesen der Versionshinweise. 95
Überprüfen Sie die Patch Anforderungen. 95
Installieren der Java-Laufzeitumgebung. 95
Data Transformation-Dateien sichern. 96
Überprüfen der Umgebungsvariablen. 97
Erstellen eines Systembenutzerkontos. 97
Einrichten von Schlüsselspeicher- und Truststore-Dateien. 98
Festlegen des Grenzwerts für den Dateideskriptor. 99
Konfigurieren von POSIX Asynchronous I/O. 100
Extrahieren der Dateien des Installationsprogramms. 100
Überprüfen Sie den Lizenzschlüssel. 101
Ausführen des Vorinstallations-Systemprüfungstools (i10Pi). 101

Teil III: Installation von Diensten. 105

Kapitel 7: Installation von Informatica-Diensten. 106

Installation von Informatica-Diensten - Übersicht. 106
- Erstellen oder Anfügen einer Domäne. 106
- Systemprüfungstool (i10Pi) und SPN-Formatgenerator. 107
- Sichere Dateien und Verzeichnisse. 107

Installieren der Informatica-Dienste im Grafikmodus. 108
- Erstellen einer Domäne. 108
- Beitreten zu einer Domäne. 123

Installieren der Informatica-Dienste im Konsolenmodus. 131
- Erstellen einer Domäne. 131
- Beitreten zu einer Domäne. 146

Automatisches Installieren der Informatica-Dienst. 154
- Konfigurieren der Eigenschaftendatei. 155
- Ausführen des automatischen Installationsprogramms. 167
- Sichern der Passwörter in der Eigenschaftendatei. 168

Kapitel 8: Fehlerbehebung 169

Behebung von Problemen bei der Installation - Übersicht. 169
Fehlerbehebung bei Installationsprotokolldateien. 169
- Debug-Protokolldateien. 169
- Dateiinstallations-Protokolldatei. 170
- Service Manager-Protokolldateien. 170

Fehlerbehebung von Domänen und Knoten. 171
Erstellen des Domänen-Konfigurations-Repository. 171
Erstellen oder Anfügen einer Domäne. 172
Starten von Informatica. 172
Pingen der Domäne. 173
Hinzufügen einer Lizenz. 173

Teil IV: Nach dem Installieren der Dienste. 174

Kapitel 9: Durchführen der Domänenkonfiguration. 175
Durchführen der Domänenkonfiguration - Übersicht. 175
Überprüfen der Gebietsschemaeinstellungen und der Codepage-Kompatibilität. 175
Konfigurieren der lokalen Umgebungsvariablen unter UNIX. 176
Konfigurieren der Umgebungsvariablen. 177
Konfigurieren der Informatica-Umgebungsvariablen. 177
Konfigurieren der Bibliothekspfad-Umgebungsvariablen unter UNIX. 178
Konfigurieren der Kerberos-Umgebungsvariablen. 180
Konfigurieren der Windows-Firewall. 180

Kapitel 10: Vorbereiten zum Erstellen der Anwendungsdienste. 182
Vorbereitung zum Erstellen der Anwendungsdienste - Übersicht. 182
Überprüfen des Setups für 64-Bit-Windows. 182
Erstellen von Verzeichnissen für den Analyst-Dienst. 183
Erstellen der Dienstprinzipalnamen und Keytab-Dateien für Anwendungsdienste. 184
Erstellen eines Schlüsselspeichers für eine sichere Verbindung zu einem Web-Anwendungsdienst 184
Anmelden beim Informatica Administrator. 185
Fehlerbehebung bei der Anmeldung bei Informatica Administrator. 186
Erstellen von Verbindungen. 186
Eigenschaften von IBM DB2-Verbindungen. 187
Eigenschaften von Microsoft SQL Server-Verbindungen. 188
Eigenschaften für Oracle-Verbindungen. 189
Erstellen einer Verbindung. 190

Kapitel 11: Erstellen der Anwendungsdienste. 191
Erstellen der Anwendungsdienste – Übersicht. 191
Überprüfen der Voraussetzungen für Anwendungsdienste. 192
Anwendungsdienst-Abhängigkeiten. 194
Erstellen und Konfigurieren des Modellrepository-Dienstes. 195
Erstellen des Modellrepository-Dienstes. 195
Nach dem Erstellen des Modellrepository-Dienstes. 198
Erstellen und Konfigurieren des Datenintegrationsdienstes. 200
Erstellen des Datenintegrationsdienstes. 200
Nach dem Erstellen des Datenintegrationsdienstes. 203

Erstellen und Konfigurieren des Analyst-Dienstes. 204
Erstellen des Analyst-Dienstes. 204
Nach dem Erstellen des Analyst-Dienstes. 206
Erstellen und Konfigurieren des Content-Management-Dienstes. 206
Erstellen des Content-Management-Dienstes. 207
Erstellen und Konfigurieren des Suchdienstes. 208
Erstellen des Suchdienstes. 209
Erstellen und Konfigurieren des PowerCenter-Repository-Dienstes. 210
Erstellen des PowerCenter-Repository-Dienstes 210
Nach dem Erstellen des PowerCenter-Repository-Dienstes. 212
Erstellen und Konfigurieren des PowerCenter-Integrationsdienstes. 214
Erstellen des PowerCenter-Integrationsdienstes. 214
Nach dem Erstellen des PowerCenter-Integrationsdienstes. 216
Erstellen und Konfigurieren des Metadata Manager-Dienstes. 216
Erstellen des Metadata Manager-Dienstes. 217
Nach dem Erstellen des Metadata Manager-Dienstes. 222
Erstellen und Konfigurieren des Webdienst-Hub-Dienstes. 222
Erstellen des Webdienst-Hub-Dienstes. 222

Teil V: Client-Installation. 225

Kapitel 12: Vor dem Installieren der Clients. 226

Vor dem Installieren der Clients - Übersicht. 226
Überprüfen der Installationsanforderungen. 226
Überprüfen des Bedarfs an Software von Drittanbietern. 227
PowerCenter Client-Anforderungen. 227
Anforderungen für Data Transformation. 227

Kapitel 13: Installieren der Clients. 228

Installieren der Clients - Übersicht. 228
Installation im Grafikmodus. 229
Automatische Installation. 230
Konfigurieren der Eigenschaftendatei. 230
Ausführen des Installationsprogramms. 231

Kapitel 14: Nach dem Installieren der Informatica-Clients. 232

Installieren von Sprachen. 232
Konfigurieren des Client für eine sichere Domäne. 232
Konfigurieren des Workspace-Verzeichnisses für das Developer-Tool. 233

Kapitel 15: Starten der Informatica-Clients. 235

Starten des Developer Tools. 235
Starten von PowerCenter Client. 236

Fehlerbehebung bei der Client-Installation. 236

Teil VI: Deinstallation. 237

Kapitel 16: Deinstallation. 238

Deinstallation - Übersicht. 238
Regeln und Richtlinien für die Deinstallation. 239
Deinstallation von Informatica Server. 239
Deinstallation unter Windows. 240
Deinstallieren des Informatica-Servers im Grafikmodus. 240
Deinstallieren des Informatica-Servers im Konsolenmodus. 240
Deinstallieren des Informatica-Servers im automatischen Modus. 241
Deinstallation der Informatica-Clients. 242
Deinstallation unter Windows. 242
Deinstallieren von Informatica-Clients im Grafikmodus. 242
Deinstallieren von Informatica-Clients im automatischen Modus. 243

Anhang A: Starten und Anhalten der Informatica-Dienste. 245

Starten und Anhalten der Informatica-Dienste - Übersicht. 245
Starten und Anhalten von Informatica unter UNIX. 246
Starten und Anhalten von Informatica unter Windows. 246
Starten oder Anhalten von Informatica über das Startmenü. 246
Starten oder Beenden von Informatica über die Systemsteuerung. 246
Starten bzw. Anhalten von Informatica über eine Eingabeaufforderung. 247
Konfigurieren des Informatica-Windows-Diensts. 247
Regeln und Richtlinien für das Benutzerkonto. 247
Konfigurieren des Informatica-Windows-Diensts. 247
Beenden von Informatica in Informatica Administrator. 248
Regeln und Richtlinien zum Starten oder Beenden von Informatica. 248

Anhang B: Verbinden zu Datenbanken unter Windows. 250

Verbinden zu Datenbanken unter Windows - Übersicht. 250
Verbinden zu einer IBM DB2 Universal-Datenbank unter Windows. 251
Konfigurieren der nativen Konnektivität. 251
Herstellen einer Verbindung zu einer Informix-Datenbank unter Windows. 252
Konfigurieren der ODBC-Konnektivität. 252
Verbinden mit Microsoft Access und Microsoft Excel unter Windows. 252
Konfigurieren der ODBC-Konnektivität. 252
Verbinden mit einer Microsoft SQL Server-Datenbank von Windows aus. 253
Konfigurieren der nativen Konnektivität. 253
Konfigurieren von benutzerdefinierten Eigenschaften für Microsoft SQL Server. 254
Verbinden zu einer Netezza-Datenbank unter Windows. 254
Konfigurieren der ODBC-Konnektivität. 255

Herstellen einer Verbindung zu einer Oracle-Datenbank unter Windows. 255
Konfigurieren der nativen Konnektivität. 255
Verbinden zu einer Sybase ASE-Datenbank unter Windows. 257
Konfigurieren der nativen Konnektivität. 257
Herstellen einer Verbindung zu einer Teradata-Datenbank über Windows. 258
Konfigurieren der ODBC-Konnektivität. 258

Anhang C: Verbinden zu Datenbanken unter UNIX. 260

Verbinden zu Datenbanken unter UNIX - Übersicht. 260
Verbinden zu einer IBM DB2 Universal-Datenbank unter UNIX. 261
Konfigurieren von nativer Konnektivität. 261
Verbinden zu einer Informix-Datenbank unter UNIX. 263
Konfigurieren der ODBC-Konnektivität. 263
Herstellen einer Verbindung zu Microsoft SQL Server unter UNIX. 264
Konfigurieren der nativen Konnektivität. 264
Konfigurieren der SSL-Authentifizierung über ODBC. 265
Konfigurieren von benutzerdefinierten Eigenschaften für Microsoft SQL Server. 266
Verbinden zu einer Netezza-Datenbank unter UNIX. 266
Konfigurieren der ODBC-Konnektivität. 267
Herstellen einer Verbindung zu einer Oracle-Datenbank unter UNIX. 269
Konfigurieren der nativen Konnektivität. 269
Herstellen einer Verbindung zu einer Sybase ASE-Datenbank unter UNIX. 271
Konfigurieren von nativer Konnektivität. 271
Herstellen einer Verbindung zu einer Teradata-Datenbank über UNIX. 273
Konfigurieren der ODBC-Konnektivität. 273
Herstellen einer Verbindung zu einer ODBC-Datenquelle. 276
odbc.ini-Beispieldatei. 278

Anhang D: Aktualisieren des DynamicSections-Parameters einer DB2-Datenbank. 285

DynamicSections-Parameter - Übersicht. 285
Aktualisieren des DynamicSections-Parameters. 285
Herunterladen und Installieren des Dienstprogramms DataDirect Connect für JDBC. 286
Ausführen des Test für JDBC-Tools. 286

Anhang E: Konfiguration einer geteilten Domäne für Metadata Manager. . . . 287

Konfiguration einer geteilten Domäne für Metadata Manager - Übersicht. 287
Geteilte Domäne - Beispiel. 288
Konfiguration der Anwendungsdienste. 289
Produktinstallation für eine geteilte Domäne. 289
Vor der Installation einer geteilten Domäne durchzuführende Aufgaben. 290
Regeln und Richtlinien für Einzelcomputer. 290

Anhang F: Installations- und Konfigurations- Checkliste. 291

Checkliste für die Installation - Übersicht. 291

Planen der Domäne. 292

Vorbereiten von Datenbanken für die Informatica-Domäne. 293

Single Sign-On für Informatica-Webanwendungen. 294

Vorbereiten der Kerberos-Authentifizierung. 294

Vor der Installation der Dienste unter Windows. 294

Vor der Installation von Diensten unter UNIX. 295

Installation von Informatica-Diensten. 296

Durchführen der Domänenkonfiguration. 296

Vorbereiten zum Erstellen der Anwendungsdienste. 297

Erstellen der Anwendungsdienste. 297

Vor dem Installieren der Clients. 298

Installieren der Clients. 298

Nach dem Installieren der Informatica-Clients. 299

Index. 300

Einleitung

Das *Informatica --Installations- und Konfigurationshandbuch* wurde für Systemadministratoren geschrieben, die für das Installieren des Informatica-Produkts zuständig sind. Bei diesem Handbuch wird davon ausgegangen, dass Sie über Kenntnisse über Betriebssysteme, relationale Datenbankkonzepte sowie die Datenbank-Engines, Einfachdateien oder Mainframe-Systeme in Ihrer Umgebung verfügen. Des Weiteren wird vorausgesetzt, dass Sie mit den Schnittstellenanforderungen für die unterstützenden Anwendungen vertraut sind.

Informatica-Ressourcen

Informatica-Netzwerk

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

Als Mitglied können Sie:

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

Informatica-Wissensdatenbank

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

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

Informatica-Dokumentation

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

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

Informatica-Produktverfügbarkeitsmatrizen

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

Informatica Velocity

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

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

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

Informatica Marketplace

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

Globaler Kundensupport von Informatica

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

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

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

Teil I: Installation - Übersicht

- Installation - Übersicht, 16

KAPITEL 1

Installation - Übersicht

Dieses Kapitel umfasst die folgenden Themen:

- Installation von Informatica, 16
- Installationsvorgang, 17

Installation von Informatica

Informatica stellt separate Installationsprogramme für die Installation der Informatica-Dienste und Informatica-Clients bereit. Laden Sie die Dateien des Informatica-Installationsprogramms zum Installieren der Informatica-Dienste und -Clients für die Informatica-Domäne herunter.

Die Informatica-Dienste bestehen aus Diensten zur Unterstützung der Domäne und Anwendungsdienste, um Aufgaben auszuführen und Datenbanken zu verwalten. Die Informatica-Domäne ist die administrative Einheit für die Informatica-Umgebung. Die Domäne ist eine Sammlung von Knoten, die die Computer darstellen, auf denen die Anwendungsdienste ausgeführt werden. Wenn Sie die Informatica-Dienste auf einem Computer installieren, installieren Sie alle Dateien für alle Dienste. Nach Abschluss der Installation können Sie basierend auf den Produkten und Funktionen, die Ihr Unternehmen erworben hat, Anwendungsdienste erstellen.

Unter Windows können Sie das Installationsprogramm der Informatica-Dienste verwenden, um die Informatica-Dienste oder die Data Transformation-Engine zu installieren. Unter Unix können Sie das Installationsprogramm der Informatica-Dienste verwenden, um die Informatica-Dienste, Live Data Map oder die Data Transformation-Engine zu installieren.

Bei der Installation der Informatica-Dienste werden Sie aufgefordert, eine Domäne zu erstellen oder einer Domäne beizutreten. Bei erstmaliger Ausführung des Installationsprogramms müssen Sie die Domäne erstellen. Bei Installation auf einem einzelnen Computer erstellen Sie die Informatica-Domäne und einen Gateway-Knoten auf diesem Computer. Bei Installation auf mehreren Computern erstellen Sie eine Informatica-Domäne und einen Gateway-Knoten während der ersten Installation. Während der Installation auf den zusätzlichen Computern erstellen Sie Gateway- oder Worker-Knoten, die Sie mit der Domäne verknüpfen.

Die Informatica-Clients bestehen aus Thick-Client- und Webclient-Anwendungen. Sie verwenden die Clients für den Zugriff auf die Dienste in der Domäne. Beim Ausführen des Clientinstallationsprogramms können Sie die Thick-Client-Anwendungen installieren.

Installationsvorgang

Die Installation der Informatica-Dienste und -Clients besteht aus mehreren Phasen.

Der Installationsprozess besteht aus den folgenden Phasen:

1. Führen Sie vor der Installation der Informatica-Dienste die folgenden Aufgaben zum Planen und Vorbereiten der Installation aus:
   a. Planen Sie die Informatica-Domäne. Berücksichtigen Sie die Anzahl der Knoten in der Domäne, die Anwendungsdienste, die auf jedem Knoten ausgeführt werden, die Systemanforderungen und den Typ der Benutzerauthentifizierung, die die Domäne verwenden wird.
   b. Bereiten Sie die Datenbanken für die Domäne vor. Überprüfen Sie die Datenbankanforderungen und richten Sie die Datenbanken ein.
   c. Führen Sie die Einrichtung der Computer zur Erfüllung der Anforderungen von Windows oder UNIX durch, sodass die Informatica-Dienste erfolgreich installiert und ausgeführt werden können.
2. Installieren der Informatica-Dienste

   Installieren Sie die Informatica-Dienste mithilfe des Server-Installationsprogramms auf einem oder mehreren Windows- oder UNIX-Computern. Bei erstmaliger Ausführung des Installationsprogramms müssen Sie die Domäne erstellen. Während der Installation auf zusätzlichen Computern erstellen Sie Worker-Knoten, die Sie mit der Domäne verknüpfen.
3. Führen Sie nach der Installation der Informatica-Dienste die folgenden Aufgaben durch, um die Installation der Dienste abzuschließen:
   a. Führen Sie die Domänenkonfiguration durch. Überprüfen Sie die Codepage-Kompatibilität, führen Sie die Aufgaben durch, die für den in der Domäne verwendeten Typ der Benutzerauthentifizierung erforderlich sind, und konfigurieren Sie die Umgebungsvariablen. Optional können Sie die sichere Kommunikation für die Domäne konfigurieren.
   b. Bereiten Sie das Erstellen der Anwendungsdienste vor. Überprüfen Sie Betriebssystemanforderungen für Anwendungsdienste und erstellen Sie die Benutzer und Verbindungen, die für die Anwendungsdienste erforderlich sind.
   c. Erstellen Sie die Anwendungsdienste in der erforderlichen Reihenfolge.
4. Installieren der Informatica-Clients

   Führen Sie zum Installieren der Clients die folgenden Aufgaben durch:
   a. Überprüfen Sie vor dem Installieren der Clients die Installations- und Drittanbietersoftware-Anforderungen für die Clients.
   b. Verwenden Sie das Client-Installationsprogramm zum Installieren der Clients auf Windows-Computern.
   c. Nach dem Installieren der Clients können Sie optional weitere Sprachen installieren und die erforderlichen Umgebungsvariablen für die Clients konfigurieren.

Teil II: Vor dem Installieren der Dienste

Dieser Teil enthält die folgenden Kapitel:

- Planen der Domäne, 19
- Vorbereiten von Datenbanken für die Informatica-Domäne , 49
- Vorbereiten der Einrichtung der Kerberos-Authentifizierung, 73
- Vor der Installation der Dienste unter Windows, 86
- Vor der Installation von Diensten unter UNIX, 94

KAPITEL 2

Planen der Domäne

Dieses Kapitel umfasst die folgenden Themen:

- Einführung in die Informatica-Domäne, 19
- Planungsprozess für die Domäne, 25
- Geteilte Domäne für Metadata Manager, 25
- Planen der Anwendungsdienste, 27
- Überprüfen der Systemvoraussetzungen, 35
- Aufzeichnen der Informatica-Domänen- und -Knoteninformationen, 39

Einführung in die Informatica-Domäne

Eine Informatica-Domäne ist eine Sammlung von Knoten und Diensten. Ein Knoten entspricht der logischen Darstellung eines einzelnen Computers in einer Domäne. Zu den Diensten für die Domäne gehören der Dienstmanager, der alle Domänenvorgänge verwaltet, und eine Reihe von Anwendungsdiensten, bei denen es sich um serverbasierte Funktionen handelt.

Die Domäne erfordert eine relationale Datenbank zur Speicherung der Konfigurationsinformationen und Benutzerkontorechte und -berechtigungen. Bei der ersten Installation der Informatica-Dienste muss das Domänenkonfigurations-Repository in einer relationalen Datenbank erstellt werden.

Verwenden Sie Informatica-Clients für den Zugriff auf die zu Grunde liegende Informatica-Funktionalität in der Domäne. Die Clients stellen Anfragen an den Dienstmanager oder an Anwendungsdienste.

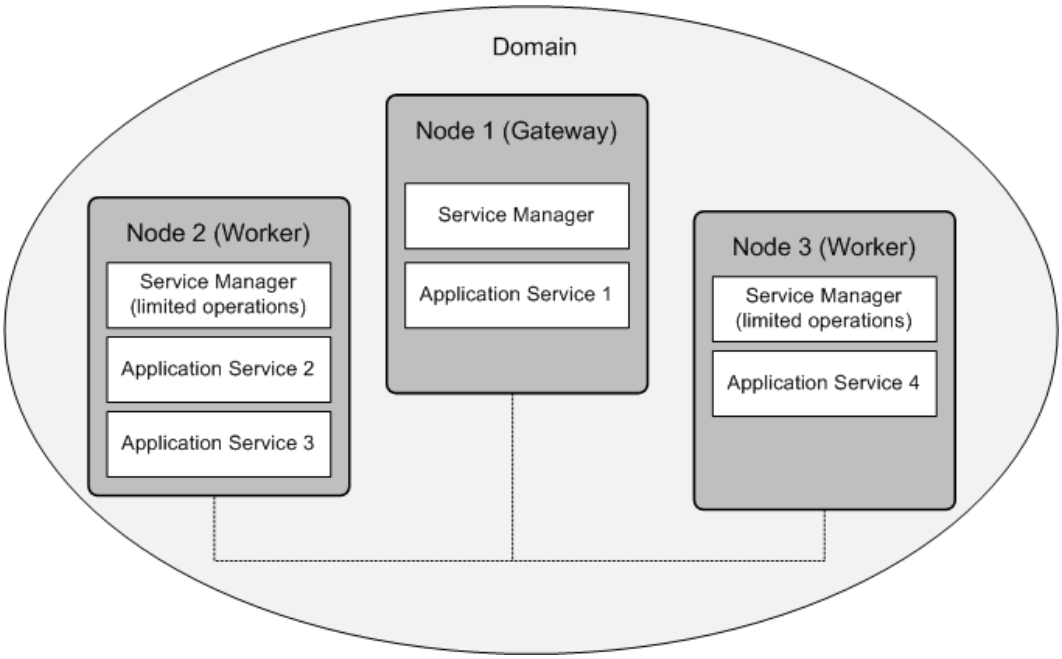
Domäne mit einem oder mehreren Knoten

Wenn Sie die Informatica-Dienste auf einem Computer installieren, erstellen Sie einen Knoten und eine Domäne. Sie können die Informatica-Dienste auf mehreren Computern installieren, um zusätzliche Knoten zu erstellen, die Sie mit der Domäne verknüpfen.

Die Installation auf einem Einzelknoten besteht aus einer Domäne mit einem Knoten. Der Knoten hostet die Domäne. Der Dienstmanager und alle Informatica-Anwendungsdienste werden auf dem Knoten ausgeführt.

Eine Installation auf mehreren Knoten besteht aus einem Gateway-Knoten, auf dem sich die Domäne und zusätzliche Knoten befinden, auf denen Informatica-Anwendungsdienste ausgeführt werden. Der Dienstmanager wird auf allen Knoten in der Domäne ausgeführt.

Die folgende Abbildung zeigt eine Installation auf mehreren Knoten:



Knoten

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. 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.

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

Ein Worker-Knoten ist ein Knoten, der nicht als Gateway konfiguriert ist. Ein Worker-Knoten kann zwar Anwendungsdienste ausführen, aber nicht als Gateway dienen. Der Dienstmanager führt auf einem Worker-Knoten nur bestimmte Domänenoperationen aus.

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.

Weitere Informationen finden Sie im *Infomatica Administrator-Handbuch*.

Weitere Informationen über Datenintegrationsdienst-Gitter finden Sie im *Handbuch für Informatica-Anwendungsdienste*.

Dienstmanager

Der Dienstmanager in der Informatica-Domäne unterstützt die Domäne und die Anwendungsdienste. Der Dienstmanager wird auf jedem Knoten in der Domäne ausgeführt.

Der Dienstmanager wird auf allen Knoten in der Domäne ausgeführt, um folgende Bereiche zu unterstützen:

Domäne

Der Dienstmanager führt auf jedem Knoten Funktionen aus, um die Domäne zu unterstützen. Die Domänenfunktionen beinhalten Authentifizierung, Autorisierung und Protokollierung. Die Domänenfunktionen, die der Dienstmanager auf einem Knoten ausführt, variieren je nach Typ und Rolle des Knotens. Zum Beispiel führt der Dienstmanager, der auf dem Master-Gateway-Knoten läuft, alle Domänenfunktionen auf diesem Knoten aus. Der Dienstmanager, der auf einem anderen Knotentyp läuft, führt auf diesem Knoten eingeschränkte Domänenfunktionen aus.

Anwendungsdienste

Wenn ein Knoten über die Dienstrolle verfügt, startet der Dienstmanager die zur Ausführung auf diesem Knoten konfigurierten Anwendungsdienste. Er startet und stoppt Dienste und Dienstprozesse entsprechend den Anfragen von Informatica-Clients.

Weitere Informationen über den Dienstmanager finden Sie im *Handbuch für Informatica Administrator*.

Anwendungsdienste

Bei Anwendungsdiensten handelt es sich um serverbasierte Funktionen. Anwendungsdienste umfassen Dienste, die mehrere Instanzen in der Domäne haben können, und Systemdienste, die eine einzige Instanz in der Domäne haben. Systemdienste werden erstellt, wenn Sie die Domäne erstellen. Nachdem Sie die Installation abgeschlossen haben, erstellen Sie andere Anwendungsdienste basierend auf dem Lizenzschlüssel, der für Ihr Unternehmen generiert wurde.

Beim Erstellen eines Anwendungsdiensts benennen Sie einen Knoten mit der Dienstrolle, auf dem der Dienstprozess ausgeführt werden soll. Der Dienstprozess ist die Laufzeitdarstellung eines auf einem Knoten ausgeführten Diensts. Wie viele Prozesse gleichzeitig ausgeführt werden können, richtet sich nach dem Diensttyp.

Haben Sie die Hochverfügbarkeitsoption, können Sie einen Anwendungsdienst auf mehreren Knoten ausführen. Falls Sie nicht über die Hochverfügbarkeitsoption verfügen sollten, konfigurieren Sie die einzelnen Anwendungsdienste für die Ausführung auf jeweils einem Knoten.

Einige Anwendungsdienste erfordern Datenbanken, um Informationen zu speichern, die vom Anwendungsdienst verarbeitet wurden. Wenn Sie die Informatica-Domäne planen, müssen Sie auch die Datenbanken planen, die für jeden Anwendungsdienst erforderlich sind.

Weitere Informationen zu den Anwendungsdiensten Sie im *Handbuch für Informatica-Anwendungsdienste*.

Lizenzschlüssel

Informatica generiert einen Lizenzschlüssel basierend auf dem Produkt und den Produktoptionen, die Ihr Unternehmen erworben hat. Der Lizenzschlüssel steuert die Anwendungsdienste und die Funktionen, die Sie verwenden können.

Wenn Sie die Informatica-Dienste installieren, müssen Sie den Pfad und Dateinamen des Informatica-Lizenzschlüssels eingeben. Das Installationsprogramm erstellt ein Lizenzobjekt in der Domäne basierend auf dem Lizenzschlüssel, den Sie eingeben. Wenn Sie Anwendungsdienste erstellen, müssen Sie das Lizenzobjekt für jeden Anwendungsdienst zuweisen, bevor Sie den Dienst ausführen können.

Benutzerauthentifizierung

Während der Installation können Sie die Authentifizierung auswählen, die für die Informatica-Domäne verwendet werden soll.

Die Informatica-Domäne kann die folgenden Authentifizierungstypen verwenden, um Benutzer in der Informatica-Domäne zu authentifizieren:

- Native Benutzerauthentifizierung
- LDAP-Benutzerauthentifizierung
- Kerberos-Netzwerk-Authentifizierung

Native Benutzerkonten werden in der Informatica-Domäne gespeichert und können nur innerhalb der Informatica-Domäne verwendet werden. Kerberos- und LDAP-Benutzerkonten werden in einem LDAP-Verzeichnisdienst gespeichert und von Anwendungen innerhalb des Unternehmens gemeinsam verwendet.

Wenn Sie die Kerberos-Authentifizierung während der Installation aktivieren, müssen Sie die Informatica-Domäne für die Arbeit mit dem Kerberos-Schlüsselverteilungscenter (KDC) konfigurieren. Sie müssen die Dienstprinzipalnamen (SPN) erstellen, die von der Informatica-Domäne in der Kerberos-Prinzipaldatenbank benötigt werden. Bei der Kerberos-Prinzipaldatenbank kann es sich um ein LDAP-Verzeichnisdienst handeln. Sie müssen auch die Schlüsseltabellen-Dateien für die SPNs erstellen und sie, wie von der Informatica-Domäne benötigt, im Informatica-Verzeichnis speichern.

Wenn Sie die Kerberos-Authentifizierung nicht während der Installation aktivieren, konfiguriert das Installationsprogramm die Informatica-Domäne für die Verwendung der nativen Authentifizierung. Nach der Installation können Sie eine Verbindung zu einem LDAP-Server einrichten und die Informatica-Domäne für die Verwendung der LDAP-Authentifizierung zusätzlich zur nativen Authentifizierung konfigurieren.

Weitere Informationen über die Benutzerauthentifizierung finden Sie im *Sicherheitshandbuch für Informatica*.

Verschlüsselungsschlüssel für sicheren Datenspeicher

Informatica verschlüsselt vertrauliche Daten wie Passwörter und sichere Verbindungsparameter, bevor die Daten in den Informatica-Repositorys gespeichert werden. Informatica verwendet ein Schlüsselwort zum Erstellen eines Verschlüsselungsschlüssels, mit dem vertrauliche Daten verschlüsselt werden.

Wenn Sie die Informatica-Dienste installieren und eine Domäne erstellen, müssen Sie ein Schlüsselwort für das Installationsprogramm angeben, um den Verschlüsselungsschlüssel für die Domäne zu erstellen. Basierend auf dem Schlüsselwort generiert das Installationsprogramm eine Verschlüsselungsschlüsseldatei namens *siteKey* und speichert sie in einem von Ihnen angegebenen Verzeichnis. Wenn Sie kein Verzeichnis angeben, speichert das Installationsprogramm die Datei *siteKey* im Standardverzeichnis: `<Informatica-Installationsverzeichnis>/isp/config/keys`

Alle Knoten in einer Domäne müssen denselben Verschlüsselungsschlüssel verwenden. Bei einer Installation auf mehreren Knoten verwendet das Installationsprogramm denselben Verschlüsselungsschlüssel für alle Knoten in der Domäne. Wenn Sie das Installationsprogramm nach dem Erstellen der Domäne ausführen,

müssen Sie denselben Verschlüsselungsschlüssel für alle Knoten festlegen, die Sie mit der Domäne verknüpfen.

Sie müssen einen Schlüsselbegriff angeben, auch wenn Sie keine sichere Kommunikation für die Domäne aktivieren oder die Kerberos-Authentifizierung verwenden.

Wichtig: Sie müssen den Namen der Domäne, das Schlüsselwort für den Verschlüsselungsschlüssel und die Verschlüsselungsschlüsseldatei an einem sicheren Speicherort aufbewahren. Der Verschlüsselungsschlüssel wird benötigt, wenn Sie den Verschlüsselungsschlüssel der Domäne ändern oder ein Repository in eine andere Domäne verschieben. Wenn Sie nicht über den Verschlüsselungsschlüssel verfügen, benötigen Sie den Domänennamen und das Schlüsselwort, das Sie zum Generieren des Verschlüsselungsschlüssels verwendet haben.

Domänensicherheit

Wenn Sie die Informatica-Dienste installieren und eine Domäne erstellen, können Sie Optionen zum Konfigurieren der Sicherheit in der Domäne aktivieren.

Sie können Sie die folgenden Sicherheitsoptionen für die Domäne konfigurieren:

Sichere Kommunikation für Dienste und den Dienstmanager

Wenn Sie die sichere Kommunikation für die Domäne konfigurieren, sichern Sie die Verbindungen zwischen dem Dienstmanager und den Diensten in der Domäne. Informatica stellt ein SSL-Zertifikat zur Verfügung, das Sie zum Sichern der Domäne verwenden können. Für eine bessere Sicherheit in der Domäne können Sie das SSL-Zertifikat jedoch während der Installation bereitstellen. Stellen Sie die Schlüsselspeicher- und Truststore-Dateien bereit, die die zu verwendenden SSL-Zertifikate enthalten.

Sichere Domänen-Konfigurations-Repository-Datenbank

Wenn Sie die Informatica-Dienste installieren und eine Domäne erstellen, können Sie das Domänen-Konfigurations-Repository in einer mit dem SSL-Protokoll gesicherten Datenbank erstellen. Der Zugriff auf die sichere Datenbank erfordert einen Truststore, der die SSL-Zertifikate für die Datenbank enthält. Während der Installation stellen Sie die Truststore-Datei bereit, die das SSL-Zertifikat enthält, das Sie verwenden möchten.

Sichere Verbindung für das Administrator-Tool

Informatica Administrator (das Administrator-Tool) ist das Tool zum Verwalten der Informatica-Domäne. Während der Installation können Sie eine sichere HTTPS-Verbindung für das Administrator-Tool konfigurieren. Sie können die Schlüsselspeicherdatei für die HTTPS-Verbindung bereitstellen.

Weitere Informationen über Domänensicherheit finden Sie im *Sicherheitshandbuch für Informatica*.

Informatica-Clients

Die Informatica-Clients sind eine Gruppe von Clients, die Sie verwenden, um auf die zugrunde liegenden Informatica-Funktionen zuzugreifen. Die Clients stellen Anfragen an den Dienstmanager oder an Anwendungsdienste.

Die Informatica-Clients bestehen aus Thick-Client-Anwendungen und Thin- oder Web-Client-Anwendungen. Sie verwenden die Clients für den Zugriff auf die Dienste in der Domäne. Beim Ausführen der Informatica-Client-Installation können Sie die Thick-Client-Anwendungen installieren.

Welche Clients Sie verwenden, hängt vom Lizenzschlüssel ab, der für Ihr Unternehmen generiert wurde.

Sie können die folgenden Thick-Client-Anwendungen installieren:

Informatica Developer

Das Developer Tool ist eine Client-Anwendung, mit der Datenobjekte, Mappings, Profile, Arbeitsabläufe und virtuelle Datenbanken erstellt und ausgeführt werden. Im Developer Tool erstellte Objekte werden in einem Modellrepository gespeichert und von einem Datenintegrationsdienst ausgeführt.

PowerCenter®Client

Der PowerCenter Client ist eine Client-Anwendung zum Definieren von Quellen und Zielen, Erstellen von Umwandlungen und Mappings sowie Arbeitsabläufen zum Ausführen von Mappings. Im PowerCenter Client erstellte Objekte werden in einem PowerCenter-Repository gespeichert und von einem PowerCenter-Integrationsdienst ausgeführt.

Sie können Anwendungsdienste zum Ausführen der folgenden Thin- oder Web-Client-Anwendungen erstellen:

Analyst Tool

Das Analyst Tool ist eine Webanwendung zum Analysieren, Bereinigen, Integrieren und Standardisieren von Daten in einem Unternehmen. Der Analyst-Dienst führt das Analyst Tool aus. Im Analyst Tool erstellte Objekte werden in einem Modellrepository gespeichert und von einem Datenintegrationsdienst ausgeführt.

Metadata Manager

Metadata Manager ist eine Webanwendung zum Durchsuchen und Analysieren von Metadaten aus unterschiedlichen Metadaten-Repositorys. Der Metadata Manager-Dienst führt die Metadata Manager-Anwendung aus. In Metadata Manager erstellte Objekte werden in einem Metadata Manager-Repository gespeichert.

Webdienst-Hub-Konsole

Die Webdienst-Hub-Konsole ist eine Webanwendung zum Verwalten der Webdienste, die Sie in PowerCenter erstellen. Der Webdienst-Hub-Dienst führt die Webdienst-Hub-Konsole aus.

Informatica Administrator

Informatica Administrator (das Administrator-Tool) ist das Verwaltungstool zum Verwalten der Informatica-Domäne und Informatica-Sicherheit. Das Administrator-Tool ist eine Thin- oder Web-Client-Anwendung.

Sie können das Administrator-Tool zur Durchführung folgender Aufgaben verwenden:

Administrative Domänenaufgaben

Verwalten von Protokollen, Domänenobjekten und Domänenberichten. Anwendungsdienste, Knoten, Gitter, Ordner, Datenbankverbindungen, Anwendungen und Lizenzen gehören zu den Domänenobjekten.

Administrative Sicherheitsaufgaben

Verwalten von Benutzern, Gruppen, Rollen, Rechten und Berechtigungen.

Auf jedem Knoten, auf dem Informatica-Dienste installiert sind, wird ein Windows-Dienst oder ein UNIX-Dämon für das Ausführen von Informatica erstellt. Wenn der Installationsvorgang erfolgreich abgeschlossen wurde, wird der Informatica-Dienst unter Windows bzw. der Informatica-Dämon unter UNIX gestartet.

Der Informatica-Dienst führt auch das Administrator-Tool aus. Melden Sie sich beim Administrator-Tool an, um die Benutzerkonten für Informatica-Benutzer zu erstellen und die Anwendungsdienste in der Domäne zu erstellen und zu konfigurieren.

Planungsprozess für die Domäne

Bevor Sie die Informatica-Dienste installieren, müssen Sie alle Komponenten in der Informatica-Domäne planen.

Beim Planen der Domäne müssen Sie die Anzahl der in der Domäne erforderlichen Knoten, die von der Domäne benötigten Anwendungsdiensttypen sowie die Anzahl der Anwendungsdienste berücksichtigen, die auf den einzelnen Knoten ausgeführt werden. Sie müssen den Datenbanktyp und den Hostnamen für das Domänenkonfigurations-Repository und die Datenbanken festlegen, die von den einzelnen Anwendungsdiensten benötigt werden. Bei Verwendung von Metadata Manager müssen Sie darüber hinaus angeben, ob eine Domäne oder eine geteilte Domäne erstellt werden soll.

Sie müssen ein Schlüsselwort für das Installationsprogramm bereitstellen, um den Verschlüsselungsschlüssel für die Domäne zu generieren. Informatica verwendet den Verschlüsselungsschlüssel zum Verschlüsseln von vertraulichen Daten.

Wenn Sie sich dafür entscheiden, SAML-basiertes Single Sign-On (SSO) für die Domäne zu konfigurieren, können Sie für die Informatica-Domäne keine Kerberos-Authentifizierung konfigurieren.

Wenn Sie die Sicherheit für die Domäne konfigurieren, müssen Sie den Speicherort und das Passwort für die Schlüsselspeicher- und Truststore-Dateien kennen. Wenn Sie die Kerberos-Authentifizierung für die Informatica-Domäne verwenden, müssen Sie mit dem Kerberos-Administrator die Benutzer- und Dienstprinzipale einrichten, die für die Domäne erforderlich sind.

Im Rahmen der Planung müssen Sie außerdem überprüfen, ob jeder Computer und jeder Datenbankserver in der Domäne die Mindestsystemanforderungen erfüllt.

Geteilte Domäne für Metadata Manager

Befindet sich Metadata Manager im Lieferumfang Ihres Produktpakets, müssen Sie angeben, ob eine Domäne oder eine geteilte Domäne erstellt werden soll. In einer geteilten Domäne werden die mit den Hauptkomponenten Ihres Produktpakets verknüpften Anwendungsdienste in einer Domäne und die mit Metadata Manager verknüpften Anwendungsdienste in einer anderen Domäne ausgeführt.

Beim Konfigurieren einer geteilten Domäne können Sie Metadata Manager aktualisieren, ohne dass die Hauptkomponenten des Produktpakets aktualisiert werden müssen. Metadata Manager kann mit einer neueren Produktversion als die anderen Komponenten ausgeführt werden.

Ihr Produktpaket umfasst beispielsweise PowerCenter und Metadata Manager. In einer geteilten Domäne werden die mit PowerCenter verknüpften Anwendungsdienste in der Hauptdomäne ausgeführt, während die mit Metadata Manager verknüpften Anwendungsdienste in der sekundären Domäne ausgeführt werden. Zum Aktualisieren von Metadata Manager aktualisieren Sie die Produktkomponenten in der sekundären Domäne. Sie können Metadata Manager aktualisieren, ohne gleichzeitig PowerCenter aktualisieren zu müssen.

Zum Erstellen der beiden Domänen führen Sie jeweils das Installationsprogramm der Informatica-Dienste aus. Sie können jede Domäne auf einem separaten Computer oder beide Domänen auf demselben Computer erstellen.

Verwandte Themen:

- "Konfiguration einer geteilten Domäne für Metadata Manager" auf Seite 287

Überlegungen zu geteilten Domänen

Beachten Sie die Vorteile und möglichen Probleme bei der Erstellung einer geteilten Domäne.

Der größte Vorteil einer geteilten Domäne besteht darin, dass häufige Aktualisierungen für Metadata Manager unterstützt werden. Sie können Metadata Manager aktualisieren, ohne dass andere Komponenten des Produktpakets gleichzeitig aktualisiert werden müssen. Somit können Sie die Vorteile neuer Funktionen und Bugfixes von Metadata Manager nutzen, ohne dass Aktivitäten (wie z. B. Datenintegrationsvorgänge) in den Hauptdomäne davon beeinflusst werden. Die Hauptdomäne bleibt während der Aktualisierung von Metadata Manager voll funktionsfähig.

Sie sollten jedoch folgende Aspekte beachten:

Die Konfiguration einer geteilten Domäne ist weitaus komplexer als die einer einzelnen Domäne.

In einer geteilten Domäne müssen Sie doppelte Dienste, Repositorys und Benutzer erstellen. Wenn Sie beide Domänen auf demselben Computer installieren, müssen Sie sicherstellen, dass zwischen den Komponenten der beiden Domänen keine Portkonflikte bestehen. Wenn Sie verschiedene Informatica-Versionen in den Domänen ausführen, müssen Sie auf mögliche Versionskonflikte bei den Datenbanken achten. Sie erstellen beispielsweise PowerCenter-Repositorys für verschiedene Informatica-Produktversionen in derselben Oracle-Datenbank. Sie müssen sicherstellen, dass beide Informatica-Produktversionen die Oracle-Datenbankversion unterstützen.

Unter Umständen treten Lizenzprobleme auf.

Wenn Sie Informatica-Produkte für die Datenintegration verwenden, sind gemäß Lizenzvereinbarung Datenintegrationsaktivitäten in der Regel auf eine Domäne beschränkt. Es ist möglich, dass in der Lizenzvereinbarung die Anzahl der Computer, auf denen Anwendungsdienste erstellt werden können, oder die zu duplizierenden Diensttypen beschränkt sind. Darüber hinaus benötigen Sie gegebenenfalls eine separate Lizenzdatei für jede Domäne.

Bei Fragen zur Lizenzierung wenden Sie sich an einen Vertreter für Informatica-Produkte.

Sie benötigen zusätzliche Datenbankschemas und Benutzerkonten.

In einer geteilten Domäne müssen Sie doppelte Repositorys erstellen. Sie erstellen beispielsweise ein Domänenkonfigurations-Repository in jeder Domäne. Wenn Sie PowerCenter und Metadata Manager in verschiedenen Domänen ausführen, erstellen Sie außerdem ein PowerCenter-Repository in jeder Domäne.

Jedes Repository muss sich in einem separaten Schema befinden. Sie benötigen weiterhin ein separates Datenbankbenutzerkonto für jedes Domänenkonfigurations-Repository.

Sie benötigen zusätzlichen Arbeits- und Festplattenspeicher.

Wenn Sie Informatica-Dienste installieren, beläuft sich der benötigte Arbeits- und Festplattenspeicher für beide Domänen auf das Doppelte des für eine Domäne benötigten Arbeits- und Festplattenspeichers.

Es gibt Beschränkungen bei der Produktversion.

In einer geteilten Domäne können die Komponenten in der sekundären Domäne dieselbe oder eine höhere Version der Informatica-Produkte im Vergleich zu den Komponenten in der Hauptdomäne aufweisen. Daher können Sie Metadata Manager in einer höheren Version als PowerCenter ausführen. Die PowerCenter-Version darf jedoch nicht höher als die Metadata Manager-Version sein.

Sie müssen unter Umständen verschiedene PowerCenter Client-Versionen in den Domänen ausführen.

Sie führen den PowerCenter Client beispielsweise in der Hauptdomäne aus, um Datenintegrationsvorgänge durchzuführen. In der sekundären Domäne führen Sie eine neuere Version des Metadata Manager aus. Zum Anzeigen von Sitzungsprotokollen aus Metadata Manager-Ressourcenladevorgängen müssen Sie eine höhere Version des PowerCenter Client in der sekundären Domäne ausführen.

Über PowerCenter Designer kann nicht auf die Metadata Manager-Datenverlaufskontrolle zugegriffen werden.

In einer geteilten Domäne kommunizieren die PowerCenter-Dienste in der Hauptdomäne nicht mit dem Metadata Manager-Dienst in der sekundären Domäne. Über PowerCenter Designer kann daher nicht auf die Metadata Manager-Datenverlaufskontrolle zugegriffen werden.

Planen der Anwendungsdienste

Wenn Sie die Informatica-Domäne planen, müssen Sie auch die Anwendungsdienste planen, die in der Domäne ausgeführt werden. Sie erstellen die Anwendungsdienste basierend auf dem Lizenzschlüssel, der für Ihr Unternehmen generiert wurde.

Wenn Sie die Anwendungsdienste planen, müssen Sie die zugeordneten Dienste berücksichtigen, die eine Verbindung zum Anwendungsdienst herstellen. Sie müssen außerdem die relationalen Datenbanken planen, die erforderlich sind, um den Anwendungsdienst zu erstellen.

Sie erstellen die Anwendungsdienste nach Abschluss der Installation.

Weitere Informationen zu den Anwendungsdiensten Sie im *Handbuch für Informatica-Anwendungsdienste*.

Anwendungsdienste nach Produkt

Jeder Anwendungsdienst bietet verschiedene Funktionen innerhalb der Informatica-Domäne. Sie erstellen die Anwendungsdienste basierend auf dem Lizenzschlüssel, der für Ihr Unternehmen generiert wurde.

Die folgende Tabelle führt die Anwendungsdienste auf, die Sie für jedes Produkt erstellen können:

Produkt	Anwendungsdienste
Big Data-Management	- Analyst-Dienst - Datenintegrationsdienst - Modellrepository-Dienst - Suchdienst
Data Quality Standard Edition oder Data Quality Advanced Edition	- Analyst-Dienst - Content-Managementdienst - Datenintegrationsdienst - Modellrepository-Dienst - Suchdienst

Produkt	Anwendungsdienste
Data Quality Governance Edition	- Analyst-Dienst - Content-Managementdienst - Datenintegrationsdienst - Metadata Manager-Dienst - Modellrepository-Dienst - PowerCenter-Integrationsdienst - PowerCenter-Repository-Dienst - Suchdienst
Data Services	- Analyst-Dienst - Content-Managementdienst - Datenintegrationsdienst - Modellrepository-Dienst - PowerCenter-Integrationsdienst - PowerCenter-Repository-Dienst - Suchdienst
Data Transformation	- Datenintegrationsdienst - Modellrepository-Dienst
PowerCenter Standard Edition	- Analyst-Dienst - Content-Managementdienst - Datenintegrationsdienst - Modellrepository-Dienst - PowerCenter-Integrationsdienst - PowerCenter-Repository-Dienst - Suchdienst - Webdienst-Hub (mit der Echtzeitoption verfügbar)
PowerCenter Advanced Edition oder PowerCenter Premium Edition	- Analyst-Dienst - Content-Managementdienst - Datenintegrationsdienst - Metadata Manager-Dienst - Modellrepository-Dienst - PowerCenter-Integrationsdienst - PowerCenter-Repository-Dienst - Suchdienst - Webdienst-Hub (mit der Echtzeitoption verfügbar)

Analyst-Dienst

Der Analyst-Dienst ist ein Anwendungsdienst, der das Analyst-Tool in der Informatica-Domäne ausführt. Der Analyst-Dienst verwaltet die Verbindungen zwischen Dienstkomponenten und den Benutzern, die Zugriff auf das Analyst-Tool haben.

Beim Ausführen der Profile, Scorecards oder Mapping-Spezifikationen im Analyst-Tool stellt der Analyst-Dienst eine Verbindung zum Datenintegrationsdienst zur Durchführung der Datenintegrationsaufgaben her. Wenn Sie Human-Tasks im Analyst Tool durchführen, stellt der Analyst-Dienst eine Verbindung zum Datenintegrationsdienst her, um die Metadaten der Aufgabe aus der Arbeitsablauf-Datenbank abzurufen.

Wenn Sie ein Modellrepository-Objekt im Analyst-Tool anzeigen, erstellen oder löschen, stellt der Analyst-Dienst eine Verbindung zum Modellrepository-Dienst für den Zugriff auf die Metadaten her. Wenn Sie Datenherkunftsanalysen für Scorecards im Analyst-Tool anzeigen, sendet der Analyst-Dienst die Anfrage an den Metadata Manager-Dienst zum Ausführen der Datenherkunft.

Hinweis: Wenn Sie den Analyst-Dienst erstellen, verbinden Sie ihn nicht mit einer relationalen Datenbank.

Assoziierte Dienste

Der Analyst-Dienst stellt eine Verbindung zu anderen Anwendungsdiensten innerhalb der Domäne her.

Wenn Sie den Analyst-Dienst erstellen, können Sie ihn mit den folgenden Anwendungsdiensten verbinden:

Datenintegrationsdienste

Sie können bis zu zwei Datenintegrationsdienste mit dem Analyst-Dienst verbinden. Der Analyst-Dienst verwaltet die Verbindung zu einem Datenintegrationsdienst, mit dem Benutzer Datenvorschau-, Mappingspezifikations-, Scorecard- und Profil-Jobs im Analyst-Tool durchführen können. Der Analyst-Dienst verwaltet außerdem die Verbindung zum Datenintegrationsdienst, den Sie zum Ausführen von Arbeitsabläufen konfigurieren. Wenn Sie den Analyst-Dienst erstellen, geben Sie den Namen des Datenintegrationsdiensts an. Sie können den Analyst-Dienst mit demselben Datenintegrationsdienst für alle Vorgänge verbinden.

Metadata Manager-Dienst

Der Analyst-Dienst verwaltet die Verbindung zu einem Metadata Manager-Dienst, der Datenherkunft für Scorecards im Analyst-Tool ausführt. Wenn Sie den Analyst-Dienst erstellen, können Sie den Namen des Metadata Manager-Diensts angeben.

Modellrepository-Dienst

Der Analyst-Dienst verwaltet die Verbindungen zum Modellrepository-Dienst für das Analyst-Tool. Das Analyst-Tool stellt die Verbindung zum Modellrepository-Dienst her, um Modellrepository-Objekte im Analyst-Tool zu erstellen, zu aktualisieren und zu löschen. Wenn Sie den Analyst-Dienst erstellen, geben Sie den Namen des Modellrepository-Diensts an.

Content-Managementdienst

Der Content-Managementdienst ist ein Anwendungsdienst zum Verwalten der Referenzdaten. Ein Referenzdatenobjekt enthält einen Satz von Datenwerten, die Sie bei der Ausführung von Vorgängen zur Datenqualität für Quelldaten suchen können. Der Content-Managementdienst kompiliert außerdem Regelspezifikationen in Mapplets. Ein Regelspezifikationsobjekt beschreibt die Datenanforderungen an eine Geschäftsregel in logischen Bedingungen.

Der Content-Managementdienst verwendet den Datenintegrationsdienst zum Ausführen von Mappings, die Daten zwischen Referenztabellen und externen Datenquellen übertragen. Der Content-Managementdienst enthält auch Umwandlungen, Mapping-Spezifikationen und Regelspezifikationen mit den folgenden Typen von Referenzdaten:

- Adressreferenzdaten
- Identitätspopulationen
- Probabilistische Modelle und Klassifizierungsmodelle
- Referenztabellen

Assoziierte Dienste

Der Content-Management-Dienst stellt eine Verbindung zu anderen Anwendungsdiensten innerhalb der Domäne her.

Wenn Sie den Content-Management-Dienst erstellen, können Sie ihn mit den folgenden Anwendungsdiensten verbinden:

Datenintegrationsdienst

Der Content-Management-Dienst verwendet den Datenintegrationsdienst zum Ausführen von Mappings, die Daten zwischen Referenztabellen und externen Datenquellen übertragen. Wenn Sie den Content-

Management-Dienst erstellen, geben Sie den Namen des Datenintegrationsdiensts an. Sie müssen den Datenintegrationsdienst und Content-Management-Dienst auf demselben Knoten erstellen.

Modellrepository-Dienst

Der Content-Management-Dienst stellt eine Verbindung zum Modellrepository-Dienst her, um Metadaten für Referenzdatenobjekte im Modellrepository zu speichern. Wenn Sie den Content-Management-Dienst erstellen, geben Sie den Namen des Modellrepository-Diensts an.

Sie können mehrere Content-Management-Dienste mit einem Modellrepository-Dienst verbinden. Der Modellrepository-Dienst identifiziert den ersten Content-Management-Dienst, den Sie zuordnen, als Master-Content-Management-Dienst. Der Master-Content-Management-Dienst verwaltet die Daten für die probabilistischen Modelle und Klassifizierungsmodelle im Modellrepository.

Erforderlich, Datenbanken

Der Content-Management-Dienst erfordert ein Referenzdaten-Warehouse in einer relationalen Datenbank. Wenn Sie den Content-Management-Dienst erstellen, müssen Sie die Verbindungsinformationen für das Referenzdaten-Warehouse angeben.

Erstellen Sie die folgende Datenbank, bevor Sie den Content-Management-Dienst erstellen:

Referenzdaten-Warehouse

Speichert die Datenwerte für die Referenztabellenobjekte, die Sie im Modellrepository definieren. Beim Hinzufügen von Daten zu einer Referenztabelle schreibt der Content-Management-Dienst die Datenwerte in eine Tabelle im Referenzdaten-Warehouse. Sie benötigen ein Referenzdaten-Warehouse zum Verwalten von Referenztabellendaten im Analyst-Tool und Developer-Tool.

Datenintegrationsdienst

Der Datenintegrationsdienst ist ein Anwendungsdienst, der Datenintegrationsaufgaben für das Analyst-Tool, das Developer-Tool und externe Clients übernimmt.

Bei der Vorschau oder Ausführung von Datenprofilen, SQL-Datendiensten und Mappings im Analyst-Tool oder Developer-Tool sendet der Client Anfragen zur Ausführung der Datenintegrationsaufgaben an den Datenintegrationsdienst. Wenn Sie SQL-Datendienste, Mappings und Arbeitsabläufe über das Befehlszeilenprogramm oder einen externen Client ausführen, sendet der Befehl die Anfrage an den Datenintegrationsdienst.

Assoziierte Dienste

Der Datenintegrationsdienst stellt eine Verbindung zu anderen Anwendungsdiensten innerhalb der Domäne her.

Wenn Sie den Datenintegrationsdienst erstellen, können Sie ihn mit den folgenden Anwendungsdiensten verbinden:

Modellrepository-Dienst

Der Datenintegrationsdienst stellt eine Verbindung zum Modellrepository-Dienst zur Durchführung von Jobs wie dem Ausführen von Mappings, Arbeitsabläufen und Profilen her. Wenn Sie den Datenintegrationsdienst erstellen, geben Sie den Namen des Modellrepository-Diensts an.

Erforderlich, Datenbanken

Der Datenintegrationsdienst kann eine Verbindung zu mehreren relationalen Datenbanken herstellen. Zu welchen Datenbanken der Dienst eine Verbindung herstellen kann, hängt von dem Lizenzschlüssel ab, der für

Ihr Unternehmen generiert wurde. Wenn Sie den Datenintegrationsdienst erstellen, geben Sie Verbindungsinformationen für die Datenbanken an.

Erstellen Sie die folgenden Datenbanken, bevor Sie den Datenintegrationsdienst erstellen:

Datenobjekt-Cache-Datenbank

Speichert zwischengespeicherte logische Datenobjekte und virtuelle Tabellen. Die Datenobjekt-Zwischenspeicherung aktiviert den Datenintegrationsdienst für den Zugriff auf vorgefertigte logische Datenobjekte und virtuelle Tabellen. Sie benötigen eine Datenobjekt-Cache-Datenbank, um die Leistung für Mappings, SQL-Datendienstabfragen und Webdienst-Anfragen zu erhöhen.

Profiling-Warehouse

Speichert Profiling-Informationen wie Profilergebnisse und Scorecard-Ergebnisse. Sie benötigen ein Profiling-Warehouse, um Profilerstellung und Datenerkennung durchzuführen.

Arbeitsablauf-Datenbank

Speichert alle Laufzeitmetadaten für Arbeitsabläufe, einschließlich Human-Task-Metadaten.

Metadata Manager-Dienst

Der Metadata Manager-Dienst ist ein Anwendungsdienst, der den Metadata Manager-Web-Client in der Informatica-Domäne ausführt. Der Metadata Manager-Dienst verwaltet die Verbindungen zwischen Dienstkomponenten und den Benutzern, die Zugriff auf Metadata Manager haben.

Beim Laden von Metadaten in das Metadata Manager-Warehouse stellt der Metadata Manager-Dienst eine Verbindung zum PowerCenter-Integrationsdienst her. Der PowerCenter-Integrationsdienst führt die Arbeitsabläufe im PowerCenter-Repository aus, um aus Metadatenquellen zu lesen und Metadaten in das Metadata Manager-Warehouse zu laden. Wenn Sie Metadata Manager verwenden, um Metadaten zu durchsuchen und zu analysieren, greift der Metadata Manager-Dienst auf die Metadaten aus dem Metadata Manager-Repository zu.

Assoziierte Dienste

Der Metadata Manager-Dienst stellt eine Verbindung zu anderen Anwendungsdiensten innerhalb der Domäne her.

Wenn Sie den Metadata Manager-Dienst erstellen, können Sie ihn mit den folgenden Anwendungsdiensten verbinden:

PowerCenter-Integrationsdienst

Beim Laden von Metadaten in das Metadata Manager-Warehouse stellt der Metadata Manager-Dienst eine Verbindung zum PowerCenter-Integrationsdienst her. Der PowerCenter-Integrationsdienst führt die Arbeitsabläufe im PowerCenter-Repository aus, um aus Metadatenquellen zu lesen und Metadaten in das Metadata Manager-Warehouse zu laden. Wenn Sie den Metadata Manager-Dienst erstellen, geben Sie den Namen des PowerCenter-Integrationsdiensts an.

PowerCenter-Repository-Dienst

Der Metadata Manager-Dienst stellt eine Verbindung zum PowerCenter-Repository-Dienst für den Zugriff auf Metadatenobjekte im PowerCenter-Repository her. Der PowerCenter-Integrationsdienst verwendet die Metadatenobjekte zum Laden von Metadaten in das Metadata Manager-Warehouse. Zu den Metadatenobjekten zählen Quellen, Ziele, Sitzungen und Arbeitsabläufe. Der Metadata Manager-Dienst bestimmt den zugehörigen PowerCenter-Repository-Dienst basierend auf dem PowerCenter-Integrationsdienst, der mit dem Metadata Manager-Dienst verbunden ist.

Erforderlich, Datenbanken

Der Metadata Manager-Dienst erfordert ein Metadata Manager-Repository in einer relationalen Datenbank. Wenn Sie den Metadata Manager-Dienst erstellen, müssen Sie die Verbindungsinformationen für die Datenbank angeben.

Erstellen Sie die folgende Datenbank, bevor Sie den Metadata Manager-Dienst erstellen:

Metadata Manager-Repository

Speichert das Metadata Manager-Warehouse und Modelle. Das Metadata Manager-Warehouse ist ein zentralisiertes Metadaten-Warehouse, in dem die Metadaten aus Metadatenquellen gespeichert werden. Modelle definieren die Metadaten, die Metadata Manager aus den Metadatenquellen extrahiert. Sie benötigen ein Metadata Manager-Repository zum Durchsuchen und Analysieren von Metadaten in Metadata Manager.

Modellrepository-Dienst

Der Modellrepository-Dienst ist ein Anwendungsdienst, der das Modellrepository verwaltet. Im Modellrepository werden die von Informatica-Clients und -Anwendungsdiensten erstellten Metadaten in einer relationalen Datenbank gespeichert, um die Zusammenarbeit zwischen den Clients und Diensten zu ermöglichen.

Wenn Sie auf ein Modellrepository-Objekt im Developer-Tool, Analyst-Tool, Administrator-Tool oder im Datenintegrationsdienst zugreifen, sendet der Client oder Dienst eine Anfrage an den Modellrepository-Dienst. Der Modellrepository-Dienst-Prozess ruft Metadaten aus den Modellrepository-Datenbanktabellen ab, fügt sie dort ein und aktualisiert sie.

Sie können einen Modellrepository-Dienst so konfigurieren, dass er Statistiken über Objekte speichert, die in der Domäne ausgeführt werden. Wenn ein Datenintegrationsdienst Objekte ausführt, speichert er die Laufzeitstatistiken über die Objekte im Modellrepository, das Sie für die Überwachung konfiguriert haben. Um die Überwachungsleistung zu verbessern, erstellen Sie einen Modellrepository-Dienst, der speziell für das Speichern der Überwachungsdaten eingerichtet ist.

Hinweis: Wenn Sie den Modellrepository-Dienst erstellen, verbinden Sie ihn nicht mit anderen Anwendungsdiensten.

Erforderlich, Datenbanken

Der Modellrepository-Dienst erfordert ein Modellrepository in einer relationalen Datenbank. Wenn Sie den Modellrepository-Dienst erstellen, müssen Sie die Verbindungsinformationen für die Datenbank angeben.

Erstellen Sie die folgende Datenbank, bevor Sie den Modellrepository-Dienst erstellen:

Modellrepository

Speichert von Informatica-Clients und -Anwendungsdiensten erstellte Metadaten in einer relationalen Datenbank, um die Zusammenarbeit zwischen den Clients und Diensten zu ermöglichen. Sie benötigen ein Modellrepository zum Speichern der Entwurfszeit- und Laufzeitobjekte, die von Informatica-Clients und -Anwendungsdiensten erstellt wurden.

PowerCenter-Integrationsdienst

Der PowerCenter-Integrationsdienst ist ein Anwendungsdienst, der Arbeitsabläufe und Sitzungen für den PowerCenter Client ausführt.

Wenn Sie einen Arbeitsablauf im PowerCenter Client ausführen, sendet der Client die Anfragen an den PowerCenter-Integrationsdienst. Der PowerCenter-Integrationsdienst stellt eine Verbindung zum

PowerCenter-Repository-Dienst zum Abrufen von Metadaten aus dem PowerCenter-Repository her und führt anschließend die Sitzungen und Arbeitsabläufe aus und überwacht sie.

Hinweis: Wenn Sie den PowerCenter-Integrationsdienst erstellen, verbinden Sie ihn nicht mit einer relationalen Datenbank.

Assoziierte Dienste

Der PowerCenter-Integrationsdienst stellt eine Verbindung zu anderen Anwendungsdiensten innerhalb der Domäne her.

Wenn Sie den PowerCenter-Integrationsdienst erstellen, können Sie ihn mit den folgenden Anwendungsdiensten verbinden:

PowerCenter-Repository-Dienst

Der PowerCenter-Integrationsdienst erfordert den PowerCenter-Repository-Dienst. Der PowerCenter-Integrationsdienst stellt eine Verbindung zum PowerCenter-Repository-Dienst her, um Arbeitsabläufe und Sitzungen auszuführen. Wenn Sie den PowerCenter-Integrationsdienst erstellen, geben Sie den Namen des PowerCenter-Repository-Diensts an.

PowerCenter-Repository-Dienst

Der PowerCenter-Repository-Dienst ist ein Anwendungsdienst, der das PowerCenter-Repository verwaltet. Das PowerCenter-Repository speichert vom PowerCenter Client und Anwendungsdiensten erstellte Metadaten in einer relationalen Datenbank.

Wenn Sie auf ein PowerCenter-Repository-Objekt im PowerCenter Client oder PowerCenter-Integrationsdienst zugreifen, sendet der Client oder Dienst eine Anfrage an den PowerCenter-Repository-Dienst. Der PowerCenter-Repository-Dienst-Prozess ruft Metadaten aus den PowerCenter-Repository-Datenbanktabellen ab, fügt sie dort ein und aktualisiert sie.

Hinweis: Wenn Sie den PowerCenter-Repository-Dienst erstellen, verbinden Sie ihn nicht mit anderen Anwendungsdiensten.

Erforderlich, Datenbanken

Der PowerCenter-Repository-Dienst erfordert ein PowerCenter-Repository in einer relationalen Datenbank. Wenn Sie den PowerCenter-Repository-Dienst erstellen, müssen Sie die Verbindungsinformationen für die Datenbank angeben.

Erstellen Sie die folgende Datenbank, bevor Sie den PowerCenter-Repository-Dienst erstellen:

PowerCenter-Repository

Speichert vom PowerCenter Client erstellte Metadaten in einer relationalen Datenbank. Sie benötigen ein PowerCenter-Repository zum Speichern von Objekten, die vom PowerCenter Client erstellt wurden, und zum Speichern von Objekten, die vom PowerCenter-Integrationsdienst ausgeführt werden.

Suchdienst

Der Suchdienst ist ein Anwendungsdienst, der Suchvorgänge im Analyst-Tool und in Business Glossary Desktop verwaltet.

Der Suchdienst gibt standardgemäß Suchergebnisse aus einem Modellrepository zurück, z. B. Datenobjekte, Mapping-Spezifikationen, Profile, Referenztabellen, Regeln, Scorecards und Unternehmensglossarbegriffe. Die Suchergebnisse können auch Ergebnisse für Spaltenprofile und Ergebnisse der Domänenerkennung aus einem Profiling Warehouse beinhalten.

Hinweis: Wenn Sie den Suchdienst erstellen, verbinden Sie ihn nicht mit einer relationalen Datenbank.

Assoziierte Dienste

Der Suchdienst stellt eine Verbindung zu anderen Anwendungsdiensten innerhalb der Domäne her.

Wenn Sie den Suchdienst erstellen, können Sie ihn mit den folgenden Anwendungsdiensten verbinden:

Analyst-Dienst

Der Analyst-Dienst verwaltet die Verbindung zum Suchdienst, der Suchvorgänge im Analyst-Tool aktiviert und verwaltet. Der Analyst-Dienst bestimmt den verbundenen Suchdienst basierend auf dem mit dem Analyst-Dienst verbundenen Modellrepository-Dienst.

Datenintegrationsdienst

Der Suchdienst stellt eine Verbindung zum Datenintegrationsdienst her, um Spaltenprofil- und Domänenerkennungs-Suchergebnisse aus dem mit dem Datenintegrationsdienst verbundenen Profiling-Warehouse zurückzugeben. Der Suchdienst bestimmt den verbundenen Datenintegrationsdienst basierend auf dem Modellrepository-Dienst.

Modellrepository-Dienst

Der Suchdienst stellt eine Verbindung zum Modellrepository-Dienst her, um die Suchergebnisse aus einem Modellrepository zurückzugeben. Die Suchergebnisse können Datenobjekte, Mapping-Spezifikationen, Profile, Referenztabellen, Regeln und Scorecards umfassen. Wenn Sie den Suchdienst erstellen, geben Sie den Namen des Modellrepository-Diensts an.

Webdienst-Hub

Der Webdienst-Hub-Dienst ist ein Anwendungsdienst in der Informatica-Domäne, der die PowerCenter-Funktionalität über die Webdienste an externe Clients freigibt.

Der Webdienst-Hub-Dienst erhält Anfragen von Web-Dienst-Clients und übergibt diese an den PowerCenter-Repository-Dienst. Der PowerCenter-Repository-Dienst verarbeitet die Anfragen und sendet eine Antwort an den Webdienst-Hub. Der Webdienst-Hub sendet eine Antwort zurück an den Webdienst-Client.

Hinweis: Wenn Sie den Webdienst-Hub-Dienst erstellen, verbinden Sie ihn nicht mit einer relationalen Datenbank.

Assoziierte Dienste

Der Webdienst-Hub-Dienst stellt eine Verbindung zu anderen Anwendungsdiensten innerhalb der Domäne her.

Wenn Sie den Webdienst-Hub-Dienst erstellen, können Sie ihn mit dem folgenden Anwendungsdienst verbinden:

PowerCenter-Repository-Dienst

Der Webdienst-Hub-Dienst stellt eine Verbindung zum PowerCenter-Repository-Dienst her, um Anfragen von Webdienst-Clients zum PowerCenter-Integrationsdienst zu senden. Wenn Sie den Webdienst-Hub-Dienst erstellen, geben Sie den Namen des PowerCenter-Repository-Diensts an.

Überprüfen der Systemvoraussetzungen

Stellen Sie sicher, dass die geplante Domäne die Mindestsystemanforderungen für die Installation, den temporären Festplattenspeicher, die Portverfügbarkeit, Datenbanken und Anwendungsdienst-Hardware erfüllt.

Weitere Informationen zu Produktanforderungen und unterstützten Plattformen finden Sie in der Produktverfügbarkeitsmatrix auf Informatica Network: https://network.informatica.com/community/informatica-network/product-availability-matrices/overview

Überprüfen der Installationsanforderungen für Dienste

Überprüfen Sie, ob Ihr System die Mindestsystemanforderungen für die Installation der Informatica-Dienste erfüllt.

In der folgenden Tabelle wird der minimale Festplatten- und Arbeitsspeicher für die Installation der Informatica-Dienste aufgelistet:

Betriebssystem	RAM	Festplattenspeicher
Windows	6 GB	10 GB
AIX	6 GB	13 GB
Linux	6 GB	13 GB
Solaris	6 GB	13 GB

Überprüfen der Anforderungen an temporären Festplattenspeicher

Das Installationsprogramm schreibt temporäre Dateien auf die Festplatte. Stellen Sie sicher, dass für die Installation genügend Speicherplatz auf dem Computer vorhanden ist. Nach Abschluss der Installation werden die temporären Dateien gelöscht und der Speicherplatz wird freigegeben.

Das Installationsprogramm benötigt 1 GB temporären Festplattenspeicher.

Überprüfen der Portanforderungen

Das Installationsprogramm richtet die Ports für Komponenten in der Informatica-Domäne ein und legt einen Bereich von dynamischen Ports für einige Anwendungsdienste fest.

Sie können die für die Komponenten zu verwendenden Portnummern und einen Bereich von dynamischen Portnummern festlegen, der für die Anwendungsdienste verwendet werden soll. Alternativ können Sie die Standardportnummern verwenden, die vom Installationsprogramm bereitgestellt werden. Vergewissern Sie sich, dass die Portnummern auf den Computern verfügbar sind, auf denen Sie die Informatica-Dienste installieren.

In der folgenden Tabelle werden die Ports beschrieben, die von Ihnen festgelegt werden können:

Port	Beschreibung
Dienstmanager-Port	Portnummer, die vom Dienstmanager auf dem Knoten verwendet wird. Der Dienstmanager überwacht eingehende Verbindungsanfragen auf diesem Port. Clientanwendungen verwenden diesen Port zur Kommunikation mit den Diensten in dieser Domäne. Die Informatica-Befehlszeilenprogramme verwenden diesen Port für die Kommunikation mit der Domäne. Dies ist auch der Port für den JDBC-/ODBC-Treiber des SQL-Datendiensts. Standardwert ist 6006.
Schließungsport des Dienstmanagers	Portnummer, die das Herunterfahren des Servers für den Dienstmanager der Domäne steuert. An diesem Port wartet der Dienstmanager auf Ausschaltbefehle. Standardwert ist 6007.
Informatica Administrator-Port	Portnummer von Informatica Administrator. Standardwert ist 6008.
Informatica Administrator-Schließungsport	Portnummer, die das Herunterfahren des Servers für Informatica Administrator steuert. Informatica Administrator überwacht Befehle zum Herunterfahren auf diesem Port. Standardwert ist 6009.
Niedrigste Portnummer	Niedrigste Portnummer des dynamischen Portnummernbereichs, die den Anwendungsdienstprozessen, die auf diesem Knoten laufen, zugewiesen werden kann. Standardwert ist 6014.
Höchste Portnummer	Höchste Portnummer des dynamischen Portnummernbereichs, die den Anwendungsdienstprozessen, die auf diesem Knoten laufen, zugewiesen werden kann. Standardwert ist 6114.

Richtlinien für die Portkonfiguration

Das Installationsprogramm validiert die von Ihnen angegebenen Portnummern, um sicherzustellen, dass es in der Domäne zu keinen Portkonflikten kommt.

Beachten Sie beim Festlegen der Portnummern die folgenden Richtlinien:

- Sie müssen für jede Domäne und jede Komponente in der Domäne eine einmalige Portnummer angeben.
- Die Portnummer für die Domäne und die Domänenkomponenten darf sich nicht im Bereich der Portnummern befinden, die Sie für die Anwendungsdienstprozesse festlegen.
- Die höchste Nummer im Bereich der Portnummern, die für die Anwendungsdienstprozesse festgelegt wurde, muss mindestens drei größer als die niedrigste Portnummer sein. Beispiel: Wenn die niedrigste Portnummer im Bereich 6400 lautet, muss die höchste Portnummer mindestens 6403 lauten.
- Die angegebenen Portnummern dürfen nicht niedriger als 1025 oder höher als 65535 sein.

Überprüfen der Datenbankanforderungen

Stellen Sie sicher, dass der Datenbankserver über ausreichend Speicherplatz für das Domänen-Konfigurations-Repository und für die anderen für die Anwendungsdienste erforderlichen Datenbanken verfügt.

Die folgende Tabelle beschreibt die Datenbankanforderungen für das Domänenkonfigurations-Repository und für die anderen Datenbanken, die für die Anwendungsdienste erforderlich sind:

Datenbank	Anforderungen
Domänenkonfigurations-Repository von Informatica	Das Domänenkonfigurations-Repository unterstützt die folgenden Datenbanktypen: - IBM DB2 UDB - Microsoft SQL Server - Oracle - Sybase ASE Zulassen von 200 MB Speicherplatz für die Datenbank.
Datenobjekt-Cache-Datenbank	Die Datenobjekt-Cache-Datenbank unterstützt die folgenden Datenbanktypen: - IBM DB2 UDB - Microsoft SQL Server - Oracle Zulassen von 200 MB Speicherplatz für die Datenbank. Weisen Sie basierend auf der Menge der Daten, die Sie zwischenspeichern möchten, mehr Speicherplatz zu.
Metadata Manager-Repository	Das Metadata Manager-Repository unterstützt die folgenden Datenbanktypen: - IBM DB2 UDB - Microsoft SQL Server - Oracle Zulassen von 1 GB Speicherplatz für die Datenbank.
Modellrepository	Das Modellrepository unterstützt die folgenden Datenbanktypen: - IBM DB2 UDB - Microsoft SQL Server - Oracle Zulassen von 3 GB Speicherplatz für DB2. Lassen Sie 200 MB Festplattenspeicher für alle anderen Datenbanktypen zu. Weisen Sie basierend auf der Menge der Metadaten, die Sie speichern möchten, mehr Speicherplatz zu.
PowerCenter-Repository	Das PowerCenter-Repository unterstützt die folgenden Datenbanktypen: - IBM DB2 UDB - Microsoft SQL Server - Oracle - Sybase ASE Zulassen von 35 MB Speicherplatz für die Datenbank. Weisen Sie basierend auf der Menge der Metadaten, die Sie speichern möchten, mehr Speicherplatz zu.
Profiling-Warehouse	Das Profiling-Warehouse unterstützt die folgenden Datenbanktypen: - IBM DB2 UDB - Microsoft SQL Server - Oracle Zulassen von 10 GB Speicherplatz für die Datenbank.

Datenbank	Anforderungen
Referenzdaten-Warehouse	Das Referenzdaten-Warehouse unterstützt die folgenden Datenbanktypen: - IBM DB2 UDB - Microsoft SQL Server - Oracle Zulassen von 200 MB Speicherplatz für die Datenbank.
Arbeitsablauf-Datenbank	Die Arbeitsablauf-Datenbank unterstützt die folgenden Datenbanktypen: - IBM DB2 UDB - Microsoft SQL Server - Oracle Zulassen von 200 MB Speicherplatz für die Datenbank. Weisen Sie basierend auf der Menge der Metadaten, die Sie speichern möchten, Speicherplatz zu.

Überprüfen der Hardwarevoraussetzungen für Anwendungsdienste

Stellen Sie sicher, dass die Knoten in der Domäne über ausreichend Hardware für den Dienstmanager und die Anwendungsdienste verfügen, die auf dem Knoten ausgeführt werden.

Sie können eine Informatica-Domäne mit einem Knoten erstellen und alle Anwendungsdienste auf ein und demselben Knoten ausführen. Bei Erstellung eienr Informatica-Domäne mit mehreren Konten können die Anwendungsdienste auf separaten Knoten ausgeführt werden. Wenn Sie die Anwendungsdienste für die Domäne planen, berücksichtigen Sie die Systemanforderungen basierend auf den Diensten, die auf einem Knoten laufen.

Hinweis: Basierend auf der Arbeitsauslastung und den Parallelverarbeitungsanforderungen müssen Sie möglicherweise die Leistung optimieren, indem Sie Cores und Speicherplatz auf einem Knoten hinzufügen.

Die folgende Tabelle listet die Mindestsystemanforderungen für einen Knoten basierend auf einigen allgemeinen Konfigurationsszenarien auf. Diese Informationen dienen als Richtlinie für andere Konfigurationen in der Domäne.

Dienste	Prozessor	Speicherkapazität	Festplattenspeicher
Ein Knoten führt die folgenden Dienste aus: - Analyst-Dienst - Content-Managementdienst - Datenintegrationsdienst - Metadata Manager-Dienst - Modellrepository-Dienst - PowerCenter-Integrationsdienst - PowerCenter-Repository-Dienst - Suchdienst - Webdienst-Hub	2 CPUs mit mehreren Cores	12 GB	20 GB
Ein Knoten führt die folgenden Dienste aus: - Analyst-Dienst - Content-Managementdienst - Datenintegrationsdienst - Modellrepository-Dienst - Suchdienst	2 CPUs mit mehreren Cores	12 GB	20 GB

Dienste	Prozessor	Speicherkapazität	Festplattenspeicher
Ein Knoten führt den folgenden Dienst aus: - Analyst-Dienst	1 CPU mit mehreren Cores	4 GB	n/v
Ein Knoten führt den folgenden Dienst aus: - Suchdienst	1 CPU mit mehreren Cores	4 GB	10 GB
Ein Knoten führt die folgenden Dienste aus: - Analyst-Dienst - Suchdienst	1 CPU mit mehreren Cores	4 GB	10 GB
Ein Knoten führt die folgenden Dienste aus: - Metadata Manager-Dienst - PowerCenter-Integrationsdienst - PowerCenter-Repository-Dienst	2 CPUs mit mehreren Cores	8 GB	10 GB
Ein Knoten führt die folgenden Dienste aus: - Metadata Manager-Dienst - PowerCenter-Integrationsdienst - PowerCenter-Repository-Dienst	2 CPUs mit mehreren Cores	8 GB	10 GB
Ein Knoten führt die folgenden Dienste aus: - PowerCenter-Integrationsdienst - PowerCenter-Repository-Dienst	1 CPU mit mehreren Cores	4 GB	10 GB
Ein Knoten führt die folgenden Dienste aus: - Datenintegrationsdienst - Modellrepository-Dienst	1 CPU mit mehreren Cores	4 GB	10 GB
Ein Knoten führt die folgenden Dienste aus: - Datenintegrationsdienst - Content-Managementdienst	1 CPU mit mehreren Cores	4 GB	10 GB
Ein Knoten führt den folgenden Dienst aus: - Metadata Manager-Dienst	1 CPU mit mehreren Cores	4 GB	10 GB
Ein Knoten führt die folgende Dienstkomponente aus: - Metadata Manager-Agent	1 CPU mit mehreren Cores	4 GB	400 MB
Ein Knoten führt den folgenden Dienst aus: - Webdienst-Hub	1 CPU mit mehreren Cores	4 GB	5 GB

Aufzeichnen der Informatica-Domänen- und -Knoteninformationen

Wenn Sie die Informatica-Dienste installieren, benötigen Sie Informationen über die Domäne, Knoten, Anwendungsdienste und Datenbanken, die Sie erstellen möchten. Wenn Sie die Informatica-Dienste auf

einem Netzwerk installieren möchten, das die Kerberos-Authentifizierung verwendet, benötigen Sie außerdem Informationen über den Server der Kerberos-Authentifizierung.

Verwenden Sie die Tabellen in diesem Abschnitt zum Erfassen der benötigten Informationen.

Benennungskonventionen für Datenobjekte

Wählen Sie eine Benennungskonvention zur Verwendung für die Domäne, die Knoten und die Anwendungsdienste aus, wenn Sie die Domäne planen.

Sie können die Namen von Domänen, Knoten und Anwendungsdiensten nicht ändern. Verwenden Sie Namen, die auch dann gültig sind, wenn Sie einen Knoten auf einen anderen Computer migrieren oder wenn Sie der Domäne weitere Knoten und Dienste hinzufügen. Verwenden Sie zudem Namen, aus denen hervorgeht, wie das Domänenobjekt verwendet wird.

Weitere Informationen zu Benennungskonventionen für Domänenobjekte finden Sie in folgendem Artikel über die schnelle Anwendung von optimalen Vorgehensweisen in Informatica auf Informatica Network: http://velocity.informatica.com/index.php/best-practices-all/139-configuration-management-and-security/708-infa-nam-conv

In der folgenden Tabelle werden empfohlene Benennungskonventionen für Domänenobjekte aufgelistet:

Objekt	Namenskonvention	Beispiele
Domäne	DMN, DOM, DOMAIN, _<ORG>_<ENV>	DOM_FIN_DEV (Finanzentwicklung) DOMAIN_ICC_PD (Integrationskompetenzcenter - Produktion)
Knoten	Node<node##>_<ORG>_<optional distinguisher>_<ENV>	Node01_ICC_DEV Node07_FIN_REVENUE_DV
Analyst-Dienst	AS_<ORG>_<ENV>	AS_FIN_DEV
Content-Managementdienst	CMS_<ORG>_<ENV>	CMS_FIN_DEV
Datenintegrationsdienst	DIS_<ORG>_<ENV>	DIS_ICC_DEV
Metadata Manager-Dienst	MM, MMS _<ORG>_<ENV>	MM_ICC_DEV
Modellrepository-Dienst	MRS_<ORG>_<ENV>	MRS_FIN_DEV
PowerCenter-Integrationsdienst	PCIS, IS _<ORG>_<ENV>	PCIS_FIN_DEV
PowerCenter-Repository-Dienst	PCRS, RS _<ORG>_<ENV>	PCRS_FIN_QA
Suchdienst	SCH_<ORG>_<ENV>	SCH_ORG_PROD
Webdienst-Hub	WS, WSH, WSHUB_<ORG>_<ENV>	WSH_ICC_PROD

Domäne

Bei der ersten Installation der Informatica-Dienste erstellen Sie den Master-Gateway-Knoten und die Informatica-Domäne.

Verwenden Sie die folgende Tabelle zum Erfassen der benötigten Domäneninformationen:

Domäneninformationen	Beschreibung	Wert
Domänenname	Der Name der Domäne, die Sie erstellen möchten. Der Name darf nicht länger als 128 Zeichen und muss im 7-Bit-ASCII-Format sein. Er darf weder Leerzeichen noch die folgenden Zeichen enthalten: ` % * + ; " ? , < > \ /	
Hostname des Master-Gateway-Knotens	Vollständig qualifizierter Hostnamen des Computers, auf dem der Master-Gateway-Knoten erstellt wird. Wenn der Rechner einen einzigen Netzwerknamen aufweist, verwenden Sie den Standard-Hostnamen. Der Knoten-Hostname darf keine Unterstriche (_) enthalten. Wenn der Rechner mehrere Netzwerknamen aufweist, können Sie den Standard-Hostnamen ändern und einen alternativen Netzwerknamen verwenden. Wenn der Rechner einen einzigen Netzwerknamen aufweist, verwenden Sie den Standard-Hostnamen. **Hinweis:** Verwenden Sie nicht localhost. Der Hostname muss den Computer eindeutig kennzeichnen.	
Name des Master-Gateway-Knotens	Der Name des Master-Gateway-Knotens, der auf dem Computer erstellt werden soll. Der Knotenname ist nicht der Hostname des Computers.	

Knoten

Wenn Sie die Informatica-Dienste installieren, fügen Sie die Installationsmaschine der Domäne als Knoten hinzu. Sie können einer Domäne mehrere Knoten hinzufügen.

Verwenden Sie die folgende Tabelle zum Erfassen der Knoteninformationen, die Sie benötigen:

Knoteninformationen	Beschreibung	Wert für Knoten1	Wert für Knoten2	Wert für Knoten3
Knoten-Hostname	Vollständig qualifizierter Hostname des Computers, auf dem der Knoten erstellt wird. Wenn der Computer einen einzigen Netzwerknamen aufweist, verwenden Sie den Standard-Hostnamen. Der Knoten-Hostname darf keine Unterstriche (_) enthalten. Wenn der Computer mehrere Netzwerknamen aufweist, können Sie den Standard-Hostnamen ändern und einen alternativen Netzwerknamen verwenden. Wenn der Computer einen einzigen Netzwerknamen aufweist, verwenden Sie den Standard-Hostnamen. **Hinweis:** Verwenden Sie nicht localhost. Der Hostname muss den Computer eindeutig kennzeichnen.			
Knotenname	Name des Knotens, den Sie auf diesem Computer erstellen möchten. Der Knotenname ist nicht der Hostname des Computers.			

Anwendungsdienste

Welche Anwendungsdienste Sie erstellen, hängt vom Lizenzschlüssel ab, der für Ihr Unternehmen generiert wurde.

Wichtig: Wenn Sie die Kerberos-Authentifizierung verwenden möchten, müssen Sie den Anwendungsdienst und Knotennemen kennen, bevor Sie die Keytab-Dateien erstellen.

Verwenden Sie die folgende Tabelle zum Erfassen der Anwendungsdienste, die Sie in der Domäne und zum Erfassen der Knoten benötigen, auf denen Anwendungsdienste ausgeführt werden:

Anwendungsdienst	Dienstname	Knotenname
Analyst-Dienst		
Content-Management		
Datenintegrationsdienst		
Metadata Manager-Dienst		
Modellrepository-Dienst		
PowerCenter-Integrationsdienst		
PowerCenter-Repository-Dienst		

Anwendungsdienst	Dienstname	Knotenname
Suchdienst		
Webdienst-Hub		

Datenbanken

Wenn Sie die Informatica-Domäne planen, müssen Sie auch die erforderlichen relationalen Datenbanken planen. Die Domäne erfordert eine Datenbank zur Speicherung der Konfigurationsinformationen und Benutzerkontorechte und -berechtigungen. Einige Anwendungsdienste benötigen Datenbanken, um Informationen zu speichern, die vom Anwendungsdienst verarbeitet wurden.

Domäne

Verwenden Sie die folgende Tabelle, um die für die Domäne benötigten Datenbankinformationen zu erfassen:

Datenbankinformationen	Beschreibung	Wert
Typ der Domänenkonfigurationsdatenbank	Der Datenbanktyp für das Domänen-Konfigurations-Repository. Das Domänenkonfigurations-Repository unterstützt IBM DB2 UDB, Microsoft SQL Server, Oracle oder Sybase ASE.	
Hostname der Domänen-Konfigurationsdatenbank	Der Name des Computers, der die Datenbank hostet.	

Content-Managementdienst

Verwenden Sie die folgende Tabelle, um die für den Content-Managementdienst benötigten Datenbankinformationen zu erfassen:

Datenbankinformationen	Beschreibung	Wert
Datenbanktyp des Referenzdaten-Warehouse	Der Datenbanktyp für das Referenzdaten-Warehouse. Das Referenzdaten-Warehouse unterstützt IBM DB2 UDB, Microsoft SQL Server oder Oracle.	
Datenbank-Hostname des Referenzdaten-Warehouse	Der Name des Computers, der die Datenbank hostet.	

Datenintegrationsdienst

Verwenden Sie die folgende Tabelle, um die für den Datenintegrationsdienst benötigten Datenbankinformationen zu erfassen:

Datenbankinformationen	Beschreibung	Wert
Typ der Datenobjekt-Cache-Datenbank	Der Datenbanktyp für die Datenobjekt-Cache-Datenbank.Die Datenobjekt-Cache-Datenbank unterstützt IBM DB2 UDB, Microsoft SQL Server oder Oracle.	
Hostname der Datenobjekt-Cache-Datenbank	Der Name des Computers, der die Datenbank hostet.	
Typ der Profiling-Warehouse-Datenbank	Der Datenbanktyp für das Profiling Warehouse. Das Profiling-Warehouse unterstützt IBM DB2 UDB, Microsoft SQL Server oder Oracle.	
Hostname der Profiling-Warehouse-Datenbank	Der Name des Computers, der die Datenbank hostet.	
Arbeitsablauf-Datenbanktyp	Datenbanktyp für die Arbeitsablauf-Datenbank. Die Arbeitsablauf-Datenbank unterstützt IBM DB2 UDB, Microsoft SQL Server oder Oracle.	
Hostname der Arbeitsablauf-Datenbank	Der Name des Computers, der die Datenbank hostet.	

Metadata Manager-Dienst

Verwenden Sie die folgende Tabelle, um die für den Metadata Manager-Dienst benötigten Datenbankinformationen zu erfassen:

Datenbankinformationen	Beschreibung	Wert
Typ der Metadata Manager-Repository-Datenbanktyp	Der Datenbanktyp für das Metadata Manager-Repository. Das Metadata Manager-Repository unterstützt IBM DB2 UDB, Microsoft SQL Server oder Oracle.	
Hostname der Metadata Manager-Repository-Datenbank	Der Name des Computers, der die Datenbank hostet.	

Modellrepository-Dienst

Verwenden Sie die folgende Tabelle, um die für den Modellrepository-Dienst benötigten Datenbankinformationen zu erfassen:

Datenbankinformationen	Beschreibung	Wert
Typ der Modellrepository-Datenbank	Der Datenbanktyp für das Modellrepository. Das Modellrepository unterstützt IBM DB2 UDB, Microsoft SQL Server oder Oracle.	
Hostname der Modellrepository-Datenbank	Der Name des Computers, der die Datenbank hostet.	

PowerCenter-Repository-Dienst

Verwenden Sie die folgende Tabelle, um die für den PowerCenter-Repository-Dienst benötigten Datenbankinformationen zu erfassen:

Datenbankinformationen	Beschreibung	Wert
Typ der PowerCenter-Repository-Datenbank	Der Datenbanktyp für das PowerCenter-Repository. Das PowerCenter-Repository unterstützt IBM DB2 UDB, Microsoft SQL Server, Oracle oder Sybase ASE.	
Hostname der PowerCenter-Repository-Datenbank	Der Name des Computers, der die Datenbank hostet.	

Sicherer Datenspeicher

Bei der Installation der Informatica-Dienste müssen Sie ein Schlüsselwort angeben, das das Installationsprogramm zum Generieren der Verschlüsselungsschlüssel für die Domäne verwendet.

Verwenden Sie die folgende Tabelle zum Erfassen von Informationen, die Sie benötigen, um sichere Datenspeicher zu konfigurieren:

Informationen zum Verschlüsselungsschlüssel	Beschreibung	Wert
Schlüsselwort	Schlüsselwort zum Erstellen eines benutzerdefinierten Verschlüsselungsschlüssels für die Sicherung vertraulicher Daten in der Domäne. Das Schlüsselwort muss die folgenden Kriterien erfüllen: - Hat eine Länge von 8 bis 20 Zeichen - Enthält mindestens einen Großbuchstaben - Enthält mindestens einen Kleinbuchstaben - Enthält mindestens eine Zahl - Enthält keine Leerzeichen Der Verschlüsselungsschlüssel wird basierend auf dem Schlüsselwort erstellt, das Sie beim Erstellen der Informatica-Domäne angeben.	
Verzeichnis des Verschlüsselungsschlüssels	Verzeichnis, in dem der Verschlüsselungsschlüssel für die Domäne gespeichert werden soll. Der Standardspeicherort befindet sich in folgendem Verzeichnis: `<Informatica-Installationsverzeichnis>/isp/config/keys`.	

Domänensicherheit

Wenn Sie die Informatica-Dienste installieren, können Sie Optionen in der Informatica-Domäne zum Konfigurieren der Sicherheit für die Domäne aktivieren.

Sichere Kommunikation für Dienste und den Dienstmanager

Optional können Sie die sichere Kommunikation zwischen Diensten und dem Dienstmanager konfigurieren.

Wichtig: Wenn Sie Ihre SSL-Zertifikate anstelle der Standardzertifikate verwenden, müssen Sie während der Installation Informationen über die SSL-Zertifikate angeben. Sie können ein selbstsigniertes Zertifikat oder ein von einer Zertifizierungsstelle ausgegebenes Zertifikat verwenden. Sie müssen SSL-Zertifikate im PEM-Format und in Java-Schlüsselspeicherdateien (JKS) bereitstellen. Informatica benötigt bestimmte Namen für die SSL-Zertifikatsdateien in der Informatica-Domäne.

Verwenden Sie die folgende Tabelle zum Erfassen von Informationen über die Schlüsselspeicher- und Truststore-Dateien, die SSL-Zertifikate enthalten, die Sie verwenden möchten:

Sicherheitsinformationen	Beschreibung	Wert
Schlüsselspeicherdatei-Verzeichnis	Das Verzeichnis, das die Schlüsselspeicherdateien enthält. Das Verzeichnis muss Dateien mit der Bezeichnung „infa_keystore.jks“ und „infa_keystore.pem“ enthalten.	
Schlüsselspeicher-Passwort	Das Passwort für den Schlüsselspeicher „infa_keystore.jks“.	

Sicherheitsinformationen	Beschreibung	Wert
Verzeichnis der Truststore-Datei	Das Verzeichnis, das die Truststore-Dateien enthält. Das Verzeichnis muss Dateien mit der Bezeichnung „infa_truststore.jks“ und „infa_truststore.pem“ enthalten.	
Truststore-Passwort	Das Passwort für die Datei „infa_truststore.jks“.	

Sichere Domänen-Konfigurations-Repository-Datenbank

Sie können optional das Domänen-Konfigurations-Repository in einer Datenbank erstellen, die durch das SSL-Protokoll gesichert ist.

Wichtig: Der Zugriff auf die sichere Datenbank erfordert ein Truststore, der die Zertifikate für die Datenbank enthält.

Verwenden Sie die folgende Tabelle zum Erfassen der Informationen über die Truststore-Datei für die sichere Datenbank:

Sicherheitsinformationen	Beschreibung	Wert
Datenbank-Truststore-Datei	Der Pfad und der Dateiname der Truststore-Datei für die sichere Datenbank.	
Datenbank-Truststore-Passwort	Das Passwort für die TrustStore-Datei.	

Sichere Verbindung für das Administrator-Tool

Optional können Sie eine sichere HTTPS-Verbindung für das Administrator-Tool konfigurieren.

Wichtig: Wenn Sie eine von Ihnen erstellte Schlüsselspeicherdatei anstelle der Standarddatei verwenden möchten, müssen Sie während der Installation Informationen über die Datei angeben.

Verwenden Sie die folgende Tabelle zum Erfassen von Informationen über die Schlüsselspeicherdatei, die Sie verwenden möchten:

Sicherheitsinformationen	Beschreibung	Wert
Schlüsselspeicher-Passwort	Ein Volltext-Passwort für die Schlüsselspeicherdatei.	
Schlüsselspeicherdatei-Verzeichnis	Der Speicherort der Schlüsselspeicherdatei.	

Kerberos-Authentifizierung

Um die Informatica-Domäne zur Ausführung in einem Netzwerk mit Kerberos-Authentifizierung zu konfigurieren, benötigen Sie Informationen über den Kerberos-Authentifizierungsserver.

Verwenden Sie die folgende Tabelle, um Informationen über den Kerberos-Authentifizierungsserver zu überprüfen und aufzuzeichnen:

Domäneninformationen	Beschreibung	Wert
Dienstbereichsname	Name des Kerberos-Bereichs, zu dem die Informatica-Domänendienste gehören. Der Bereichsname muss in Großbuchstaben geschrieben sein. Der Dienstbereichsname und der Benutzerbereichsname müssen identisch sein.	
Benutzerbereichsname	Name des Kerberos-Bereichs, zu dem die Informatica-Domänenbenutzer gehören. Der Bereichsname muss in Großbuchstaben geschrieben sein. Der Dienstbereichsname und der Benutzerbereichsname müssen identisch sein.	
Speicherort der Kerberos-Konfigurationsdatei	Verzeichnis, in dem die Kerberos-Konfigurationsdatei mit der Bezeichnung *krb5.conf* gespeichert ist. Für Informatica müssen in der Konfigurationsdatei bestimmte Eigenschaften eingerichtet werden. Wenn Sie nicht über die Berechtigung zum Kopieren oder Aktualisieren der Kerberos-Konfigurationsdatei verfügen, müssen Sie unter Umständen den Kerberos-Administrator bitten, die Datei zu aktualisieren.	

KAPITEL 3

Vorbereiten von Datenbanken für die Informatica-Domäne

Dieses Kapitel umfasst die folgenden Themen:

- Vorbereiten von Datenbanken für die Informatica-Domäne - Übersicht, 49
- Einrichten von Datenbankbenutzerkonten, 50
- Datenbankanforderungen des Domänen-Konfigurations-Repositorys, 50
- Anforderungen für Datenobjekt-Cache-Datenbank, 54
- Anforderungen an die Audit-Datenbank der Ausnahmeverwaltung, 55
- Metadata Manager Repository-Datenbankanforderungen, 56
- Modellrepository-Datenbankanforderungen, 60
- PowerCenter-Repository-Datenbankanforderungen, 62
- Anforderungen an das Profiling-Warehouse, 64
- Anforderungen des Referenzdaten-Warehouse, 65
- Anforderungen an Arbeitsablauf-Datenbanken, 67
- Konfigurieren der nativen Konnektivität auf dem Dienst-Computer, 68
- Verbindungszeichenfolge für eine sichere Datenbank, 71

Vorbereiten von Datenbanken für die Informatica-Domäne - Übersicht

Informatica speichert Daten und Metadaten in Repositorys in der Domäne. Richten Sie vor der Erstellung der Domäne und Anwendungsdienste die Datenbank und Datenbank-Benutzerkonten für die Repositorys ein.

Richten Sie eine Datenbank und ein Benutzerkonto für die folgenden Repositorys ein:

- Domänenkonfigurations-Repository
- Datenobjekt-Cache-Repository
- Ausnahmeverwaltungs-Audit-Datenbank
- Metadata Manager-Repository
- Modellrepository
- PowerCenter-Repository

- Profiling-Warehouse
- Referenzdaten-Warehouse
- Arbeitsablauf-Datenbank

Um die Datenbanken vorzubereiten, überprüfen Sie die Datenbankanforderungen und richten Sie die Datenbank ein. Die Datenbankanforderungen hängen von den Anwendungsdiensten, die Sie in der Domäne erstellen und von der Zahl der Datenintegrationsobjekte ab, die Sie in den Repositorys erstellen und speichern.

Einrichten von Datenbankbenutzerkonten

Richten Sie eine Datenbank und das Benutzerkonto für das Domänen-Konfigurations-Repository und für die Repository-Datenbanken ein, die mit den Anwendungsdiensten verbunden sind.

Beachten Sie beim Einrichten der Benutzerkonten die folgenden Richtlinien:

- Das Datenbankbenutzerkonto muss über Berechtigungen zum Erstellen und Ablegen von Tabellen, Indizes und Ansichten und zum Auswählen, Einfügen, Aktualisieren und Löschen von Daten in Tabellen verfügen.
- Verwenden Sie 7-Bit ASCII zum Erstellen des Passworts zum Konto
- Um zu vermeiden, dass Datenbankfehler in einem Repository auf andere Repositorys übergreifen, erstellen Sie jedes Repository in einem separaten Datenbankschema mit einem anderen Datenbankbenutzerkonto. Erstellen Sie das Repository nicht in demselben Datenbankschema wie das Domänen-Konfigurations-Repository oder die anderen Repositorys in der Domäne.
- Bei Erstellung mehrerer Domänen muss es für jedes Domänen-Konfigurations-Repository ein separates Benutzerkonto geben.

Datenbankanforderungen des Domänen-Konfigurations-Repositorys

Die Informatica-Komponenten speichern Metadaten in relationalen Datenbank-Repositories. In der Domäne werden Konfigurations- und Benutzerinformationen in einem Domänen-Konfigurations-Repository gespeichert.

Sie müssen eine Datenbank und ein Benutzerkonto für das Domänen-Konfigurations-Repository einrichten, bevor Sie die Installation ausführen. Die Datenbank muss allen Gateway-Knoten in der Informatica-Domäne zugänglich sein.

Bei der Installation von Informatica geben Sie die Datenbank- und Benutzerkontodaten für das Domänen-Konfigurations-Repository ein. Das Installationsprogramm kommuniziert mittels JDBC mit dem Domänen-Konfigurations-Repository.

Das Domänenkonfigurations-Repository unterstützt die folgenden Datenbanktypen:

- IBM DB2 UDB
- Microsoft SQL Server
- Oracle

- Sybase ASE

Zulassen von 200 MB Speicherplatz für die Datenbank.

IBM DB2-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository in IBM DB2 die folgenden Richtlinien:

- Wenn sich das Repository in einer IBM DB2 9.7-Datenbank befindet, stellen Sie sicher, dass IBM DB2 Version 9.7 Fix Pack 7 oder ein späteres Fixpack installiert ist.
- Setzen Sie die folgenden Parameter in der IBM DB2-Instanz, in der Sie die Datenbank erstellen, auf ON:
  - DB2_SKIPINSERTED
  - DB2_EVALUNCOMMITTED
  - DB2_SKIPDELETED
  - AUTO_RUNSTATS
- Legen Sie die Konfigurationsparameter in der Datenbank fest.

  In der folgenden Tabelle werden die Konfigurationsparameter aufgelistet, die Sie festlegen müssen:

Parameter	Wert
logfilsiz	8000
maxlocks	98
locklist	50000
auto_stmt_stats	ON

- Setzen Sie den Tablespace-Parameter pageSize auf 32768 Byte.

  Legen Sie in einer Datenbank mit einer einzigen Partition einen Tablespace fest, der die pageSize-Anforderungen erfüllt. Wenn Sie keinen Tablespace festlegen, muss der Standard-Tablespace die pageSize-Anforderungen erfüllen.

  Legen Sie in einer Datenbank mit mehreren Partitionen einen Tablespace fest, der die pageSize-Anforderungen erfüllt. Definieren Sie den Tablespace in der Katalogpartition der Datenbank.
- Legen Sie den NPAGES-Parameter auf mindestens 5000 fest. Der NPAGES-Parameter bestimmt die Anzahl der Seiten im Tabellenbereich.
- Stellen Sie sicher, dass der Datenbankbenutzer über die Berechtigungen CREATETAB, CONNECT und BINDADD verfügt.
- Informatica bietet keine Unterstützung für IBM DB2-Tabellenaliase für Repository-Tabellen. Stellen Sie sicher, dass für keine Tabellen in der Datenbank Tabellenaliase erstellt wurden.

- Aktualisieren Sie im Dienstprogramm DataDirect Connect for JDBC den Parameter DynamicSections auf 3000.

  Der Standardwert von DynamicSections ist zu niedrig für die Informatica-Repositorys. Für Informatica ist ein größeres DB2-Paket als das Standardpaket erforderlich. Beim Einrichten der DB2-Datenbank für das Domänenkonfigurations-Repository oder ein Modellrepository müssen Sie den Parameter DynamicSections auf einen Wert von mindestens 3000 einstellen. Wenn der Parameter DynamicSections auf einen niedrigeren Wert eingestellt ist, kann es beim Installieren oder Ausführen von Informatica-Diensten zu Problemen kommen.

  Weitere Informationen zur Aktualisierung des Parameters DynamicSections finden Sie unter Anhang D, “Aktualisieren des DynamicSections-Parameters einer DB2-Datenbank” auf Seite 285.

Microsoft SQL Server-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository in Microsoft SQL Server die folgenden Richtlinien:

- Legen Sie die Isolationsstufe "Allow Snapshot Isolation" und "Read Committed" auf ALLOW_SNAPSHOT_ISOLATION und READ_COMMITTED_SNAPSHOT fest, um Konflikte zu minimieren. Führen Sie zum Festlegen der Isolationsebene für die Datenbank die folgenden Befehle aus:

  ```
  ALTER DATABASE DatabaseName SET ALLOW_SNAPSHOT_ISOLATION ON
  ```

  ```
  ALTER DATABASE DatabaseName SET READ_COMMITTED_SNAPSHOT ON
  ```

  Führen Sie den folgenden Befehl aus, um zu überprüfen, ob die Isolationsebene für die Datenbank richtig ist:

  ```
  SELECT snapshot_isolation_state FROM sys.databases WHERE name=[Datenbankname]
  ```

  Hinweis: Um die Snapshot-Isolation zu aktivieren, legen Sie snapshot_isolation_state mit 1 fest. Beispiel: `snapshot_isolation_state=1`.

  ```
  SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name = DatabaseName
  ```

- Das Datenbankbenutzerkonto muss über die Berechtigungen CONNECT, CREATE TABLE und CREATE VIEW verfügen.

Oracle-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository in Oracle die folgenden Richtlinien:

- Setzen Sie den Parameter open_cursors auf 4000 oder höher.
- Legen Sie die Berechtigungen in der Ansicht `$parameter` für den Datenbankbenutzer fest.
- Legen Sie die Berechtigungen für den Datenbankbenutzer zum Ausführen von *show parameter open_cursors* in der Oracle-Datenbank fest.
  Wenn Sie das Vorinstallations-Systemprüfungstool (i10Pi) ausführen, führt i10Pi den Befehl in der Datenbank zur Identifizierung des Parameters OPEN_CURSORS mit den Anmeldedaten des Domänendatenbankbenutzers aus.

  Sie können die folgende Abfrage ausführen, um die Einstellung der offenen Cursor für das Domänendatenbank-Benutzerkonto zu bestimmen:

  ```
  SELECT VALUE OPEN_CURSORS FROM V$PARAMETER WHERE UPPER(NAME)=UPPER('OPEN_CURSORS')
  ```

- Stellen Sie sicher, dass der Datenbankbenutzer über die folgenden Berechtigungen verfügt:

  CREATE SEQUENCE

  CREATE SESSION

  CREATE SYNONYM

CREATE TABLE

CREATE VIEW

- Informatica bietet keine Unterstützung für öffentliche Oracle-Synonyme für Repository-Tabellen. Stellen Sie sicher, dass für keine der Tabellen in der Datenbank öffentliche Synonyme erstellt wurden.

Sybase ASE-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository in Sybase ASE die folgenden Richtlinien:

- Stellen Sie die Seitengröße des Datenbankservers auf 16 K oder höher ein. Sie müssen die Seitengröße auf 16 K einstellen, da Sie diese Konfiguration nur ein einziges Mal vornehmen und sie später nicht mehr ändern können.
- Legen Sie die Datenbank-Sperrkonfiguration für die Verwendung der Sperrung auf Zeilenebene fest.
  In der folgenden Tabelle wird die Datenbank-Sperrkonfiguration beschrieben, die Sie festlegen müssen:

Datenbankkonfiguration	Sybase-Systemprozedur	Wert
Sperrschema	sp_configure "Sperrschema"	0, datarows

- Legen Sie die Sybase-Datenbankoption „ddl in tran“ auf TRUE fest.
- Legen Sie „allow nulls by default“ auf TRUE fest.
- Aktivieren Sie die Sybase-Datenbankoption (ON) und wählen Sie into/bulkcopy/pllsort.
- Aktivieren Sie die select-Berechtigung für die sysobjects-Systemtabelle.
- Erstellen Sie das folgende Anmeldeskript zum Deaktivieren der Standard-VARCHAR-Kürzung:

```
create procedure dbo.sp_string_rtrunc_proc as set string_rtruncation on
sp_modifylogin "user_name", "login script", sp_string_rtrunc_proc
```

  Das Anmeldeskript wird jedes Mal ausgeführt, wenn sich der Benutzer bei der Sybase-Instanz anmeldet. Die gespeicherte Prozedur stellt den Parameter auf Sitzungsebene ein. Die Systemprozedur sp_modifylogin aktualisiert „user_name“ mit der gespeicherten Prozedur als „login script“. Der Benutzer muss zum Aufrufen der gespeicherten Prozedur berechtigt sein.

- Stellen Sie sicher, dass der Datenbankbenutzer über die Berechtigungen CREATE DEFAULT, CREATE PROCEDURE, CREATE RULE, CREATE TABLE und CREATE VIEW verfügt.
- Legen Sie die Datenbankkonfigurationen auf die empfohlenen Baseline-Werte fest.
  In der folgenden Tabelle werden die Konfigurationsparameter für den Datenbankspeicher aufgelistet, die Sie festlegen müssen:

Datenbankkonfiguration	Sybase-Systemprozedur	Wert
Maximale Gesamtmenge an physischem Speicher	sp_configure "max memory"	2097151
Cache-Größe der Prozedur	sp_configure "procedure cache size"	500000
Anzahl geöffneter Objekte	sp_configure "number of open objects"	5000
Anzahl geöffneter Indizes	sp_configure "number of open indexes"	5000
Anzahl geöffneter Partitionen	sp_configure "number of open partitions"	5000

Datenbankkonfiguration	Sybase-Systemprozedur	Wert
Heap-Speicher pro Benutzer	sp_configure "heap memory per user"	49152
Anzahl Sperren	sp_configure "number of locks"	100000

Anforderungen für Datenobjekt-Cache-Datenbank

Die Datenobjekt-Cache-Datenbank speichert zwischengespeicherte logische Datenobjekte und virtuelle Tabellen für den Datenintegrationsdienst. Beim Erstellen des Datenintegrationsdiensts geben Sie die Datenobjekt-Cache-Datenbankverbindung an.

Die Datenobjekt-Cache-Datenbank unterstützt die folgenden Datenbanktypen:

- IBM DB2 UDB
- Microsoft SQL Server
- Oracle

Zulassen von 200 MB Speicherplatz für die Datenbank.

Hinweis: Stellen Sie sicher, dass Sie den Datenbank-Client auf dem Computer installieren, auf dem Sie den Datenintegrationsdienst ausführen möchten.

IBM DB2-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository in IBM DB2 die folgenden Richtlinien:

- Stellen Sie sicher, dass das Datenbankbenutzerkonto über die Berechtigungen CREATETAB und CONNECT verfügt.
- Informatica bietet keine Unterstützung für IBM DB2-Tabellenaliase für Repository-Tabellen. Stellen Sie sicher, dass für keine Tabellen in der Datenbank Tabellenaliase erstellt wurden.
- Setzen Sie den Tablespace-Parameter pageSize auf 32768 Byte.
- Legen Sie den NPAGES-Parameter auf mindestens 5000 fest. Der NPAGES-Parameter bestimmt die Anzahl der Seiten im Tabellenbereich.

Microsoft SQL Server-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository in Microsoft SQL Server die folgenden Richtlinien:

- Stellen Sie sicher, dass das Datenbankbenutzerkonto über die Berechtigungen CONNECT und CREATE TABLE verfügt.

Oracle-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository in Oracle die folgenden Richtlinien:

- Stellen Sie sicher, dass der Datenbankbenutzer über die folgenden Berechtigungen verfügt:

  CREATE INDEX

  CREATE SESSION

  CREATE SYNONYM

  CREATE TABLE

  CREATE VIEW

  DROP TABLE

  INSERT INTO TABLE

  UPDATE TABLE
- Informatica bietet keine Unterstützung für öffentliche Oracle-Synonyme für Repository-Tabellen. Stellen Sie sicher, dass für keine der Tabellen in der Datenbank öffentliche Synonyme erstellt wurden.

Anforderungen an die Audit-Datenbank der Ausnahmeverwaltung

Bei der Audit-Datenbank der Ausnahmeverwaltung handelt es sich um ein einzelnes Repository für Daten, in dem die Arbeit beschrieben wird, die Benutzer des Analyst Tools für Instanzen von Human-Aufgaben durchführen. Der Analyst-Dienst gibt die Datenbankverbindung und den Schemanamen an. Der Datenintegrationsdienst schreibt die Audit-Daten in die Datenbank.

Wenn der Analyst-Dienst keine Audit-Datenbank der Ausnahmeverwaltung angibt, schreibt der Datenintegrationsdienst die Audit-Daten in die Datenbank, die die Datensätze der Aufgabeninstanz enthält.

Das Referenzdaten-Warehouse unterstützt die folgenden Datenbanktypen:

- IBM DB2 UDB
- Microsoft SQL Server
- Oracle

Zulassen von 200 MB Speicherplatz für die Datenbank.

Hinweis: Stellen Sie sicher, dass Sie den Datenbank-Client auf dem Computer installieren, auf dem der Content-Management-Dienst ausgeführt werden soll.

IBM DB2-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository in IBM DB2 die folgenden Richtlinien:

- Das Datenbankbenutzerkonto muss über die Berechtigungen CREATETAB, CONNECT, CREATE VIEW und CREATE FUNCTION verfügen.
- Informatica bietet keine Unterstützung für IBM DB2-Tabellenaliase für Repository-Tabellen. Stellen Sie sicher, dass für keine Tabellen in der Datenbank Tabellenaliase erstellt wurden.
- Setzen Sie den Tablespace-Parameter pageSize auf 32768 Byte.

- Legen Sie den NPAGES-Parameter auf mindestens 5000 fest. Der NPAGES-Parameter bestimmt die Anzahl der Seiten im Tabellenbereich.

Microsoft SQL Server-Datenbankanforderungen

Beachten Sie beim Einrichten des Repositorys in Microsoft SQL Server die folgenden Richtlinien:

- Das Datenbankbenutzerkonto muss über die Berechtigungen CONNECT, CREATE TABLE, CREATE VIEW und CREATE FUNCTION verfügen.

Oracle-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository in Oracle die folgenden Richtlinien:

- Stellen Sie sicher, dass der Datenbankbenutzer über die folgenden Berechtigungen verfügt:

  ALTER TABLE

  CREATE SESSION

  CREATE TABLE

  DROP TABLE

  UPDATE TABLE
- Informatica bietet keine Unterstützung für öffentliche Oracle-Synonyme für Repository-Tabellen. Stellen Sie sicher, dass für keine der Tabellen in der Datenbank öffentliche Synonyme erstellt wurden.
- Legen Sie den Tablespace-Parameter fest. Verwenden Sie die folgende Formel zur Bestimmung des Wertes: 2 MB x (Anzahl der Tabellen in jedem Scan x Anzahl gleichzeitiger Scans)
  Sie haben beispielsweise 1.000 Tabellen in jedem Scan und möchten 10 Scans gleichzeitig ausführen. Berechnen Sie den Wert des Tablespace-Parameters wie folgt: 2 MB x (100 x 10) = 20 GB

  Hinweis: Der Tablespace muss über mehrere Festplatten verteilt sein.
- Legen Sie die folgenden Parameter auf die von Informatica empfohlenen Werte fest:

Parameter	Empfohlener Wert
open_cursors	3000
Sitzungen	1000
Prozesse	1000

Metadata Manager Repository-Datenbankanforderungen

Das Metadata Manager-Repository enthält das Metadata Manager-Warehouse und Modelle. Das Metadata Manager-Warehouse ist ein zentralisiertes Metadaten-Warehouse, in dem die Metadaten aus Metadatenquellen gespeichert werden.

Geben Sie die Repository-Details beim Erstellen eines Metadata Manager-Diensts an.

Das Metadata Manager-Repository unterstützt die folgenden Datenbanktypen:

- IBM DB2 UDB
- Microsoft SQL Server
- Oracle

Zulassen von 1 GB Speicherplatz für die Datenbank.

Weitere Informationen zum Konfigurieren der Datenbank finden Sie in der Dokumentation zu Ihrem Datenbanksystem.

IBM DB2-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository in IBM DB2 die folgenden Richtlinien:

- Das Datenbankbenutzerkonto, das das Repository erstellt, muss über Berechtigungen zur Durchführung der folgenden Vorgänge verfügen:

  ALTER TABLE

  CREATE FUNCTION

  CREATE INDEX

  CREATE PROCEDURE

  CREATE TABLE

  CREATE VIEW

  DROP PROCEDURE

  DROP TABLE

  INSERT INTO
- Der Datenbankbenutzer, der das Repository erstellt, muss Tablespaces mit Seitengrößen von 32 KB erstellen können.
- Stellen Sie die temporären System-Tablespace größer als die Standard-Seitengröße von 4 KB ein und aktualisieren Sie die Heapgrößen.
  Abfragen gegen Tabellen in Tablespaces, die mit einer Seitengröße von über 4 KB definiert wurden, benötigen temporäre System-Tablespaces mit einer Seitengröße von über 4 KB. Wenn keine temporären System-Tablespaces mit einem höheren Wert für die Seitengröße definiert wurden, können die Abfragen fehlschlagen. Auf dem Server wird der folgende Fehler angezeigt:

  ```
  SQL 1585N A system temporary table space with sufficient page size does not exist.
  SQLSTATE=54048
  ```

  Erstellen Sie temporäre System-Tablespaces mit Seitengrößen von 8 KB, 16 KB und 32 KB. Führen Sie die folgenden SQL-Anweisungen in jeder Datenbank aus, um die temporären System-Tablespaces zu konfigurieren und die Heapgröße zu aktualisieren:

  ```
  CREATE Bufferpool RBF IMMEDIATE  SIZE 1000 PAGESIZE 32 K  EXTENDED STORAGE ;
  CREATE Bufferpool STBF IMMEDIATE  SIZE 2000 PAGESIZE 32 K  EXTENDED STORAGE ;
  CREATE REGULAR  TABLESPACE REGTS32 PAGESIZE 32 K  MANAGED BY SYSTEM  USING ('C:
  \DB2\NODE0000\reg32' ) EXTENTSIZE 16 OVERHEAD 10.5 PREFETCHSIZE 16 TRANSFERRATE 0.33
  BUFFERPOOL RBF;
  CREATE  SYSTEM TEMPORARY  TABLESPACE TEMP32 PAGESIZE 32 K  MANAGED BY SYSTEM  USING
  ('C:\DB2\NODE0000\temp32' ) EXTENTSIZE 16 OVERHEAD 10.5 PREFETCHSIZE 16 TRANSFERRATE
  0.33 BUFFERPOOL STBF;
  GRANT USE OF TABLESPACE REGTS32 TO USER <USERNAME>;
  UPDATE DB CFG FOR <DB NAME> USING APP_CTL_HEAP_SZ 16384
  UPDATE DB CFG FOR <DB NAME> USING APPLHEAPSZ 16384
  UPDATE DBM CFG USING QUERY_HEAP_SZ 8000
  UPDATE DB CFG FOR <DB NAME> USING LOGPRIMARY 100
  UPDATE DB CFG FOR <DB NAME> USING LOGFILSIZ 2000
  ```

```
UPDATE DB CFG FOR <DB NAME> USING LOCKLIST 1000
UPDATE DB CFG FOR <DB NAME> USING DBHEAP 2400
"FORCE APPLICATIONS ALL"
DB2STOP
DB2START
```

- Legen Sie die Sperrparameter fest, damit es beim Laden von Metadaten in das Metadata Manager-Repository in IBM DB2 nicht zu Deadlocks kommt.
  In der folgenden Tabelle werden die Sperrparameter aufgelistet, die Sie konfigurieren können:

Parametername	Wert	IBM DB2-Beschreibung
LOCKLIST	8192	Maximaler Speicher für Sperrliste (4 KB)
MAXLOCKS	10	Sperrlisten pro Anwendung in Prozent
LOCKTIMEOUT	300	Sperr-Zeitüberschreitung (Sek.)
DLCHKTIME	10000	Intervall für das Überprüfen eines Deadlocks (ms)

  Legen Sie außerdem für IBM DB2 9.7 und frühere Versionen den Parameter DB2_RR_TO_RS auf YES fest, um die Leserichtlinie von „Repeatable Read“ in „Read Stability“ zu ändern.

- Informatica bietet keine Unterstützung für IBM DB2-Tabellenaliase für Repository-Tabellen. Stellen Sie sicher, dass für keine Tabellen in der Datenbank Tabellenaliase erstellt wurden.

Hinweis: Bei Verwendung von IBM DB2 als Metadatenquelle gelten für die Quelldatenbank dieselben Konfigurationsanforderungen.

Microsoft SQL Server-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository in Microsoft SQL Server die folgenden Richtlinien:

- Das Datenbankbenutzerkonto, das das Repository erstellt, muss über Berechtigungen zur Durchführung der folgenden Vorgänge verfügen:

  ALTER TABLE

  CREATE CLUSTERED INDEX

  CREATE INDEX

  CREATE PROCEDURE

  CREATE TABLE

  CREATE VIEW

  DROP PROCEDURE

  DROP TABLE

  INSERT INTO

- Wenn im Repository Metadaten in einer Multibyte-Sprache gespeichert werden müssen, stellen Sie die Datenbank-Sortierreihenfolge bei der Installation von Microsoft SQL Server auf diese Multibyte-Sprache ein. Wenn im Repository beispielsweise Metadaten in Japanisch gespeichert werden müssen, setzen Sie bei der Installation von Microsoft SQL Server die Sortierreihenfolge der Datenbank auf eine japanische Sortierreihenfolge. Diese Konfiguration wird nur einmal vorgenommen und kann danach nicht mehr geändert werden.

Oracle-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository in Oracle die folgenden Richtlinien:

- Stellen Sie sicher, dass der Datenbankbenutzer über die folgenden Berechtigungen verfügt:

  ALTER TABLE

  CREATE CLUSTER

  CREATE INDEX

  CREATE OR REPLACE FORCE VIEW

  CREATE OR REPLACE PROCEDURE

  CREATE OR REPLACE VIEW

  CREATE SESSION

  CREATE TABLE

  DROP TABLE

  INSERT INTO TABLE

- Legen Sie die folgenden Parameter für den Tablespace unter Oracle fest:

  <Temporärer Tablespace>

  Größe auf mindestens 2 GB ändern.

  CURSOR_SHARING

  Auf FORCE festlegen.

  MEMORY_TARGET

  Mindestens auf 4 GB festlegen.

  Führen Sie `SELECT * FROM v$memory_target_advice ORDER BY memory_size;` aus, um die optimale Speichergröße (MEMORY_SIZE) festzulegen.

  MEMORY_MAX_TARGET

  Einen größeren Wert als die MEMORY_TARGET-Größe festlegen.

  Wenn MEMORY_MAX_TARGET nicht festgelegt ist, wird für MEMORY_MAX_TARGET standardmäßig die Einstellung MEMORY_TARGET festgelegt.

  OPEN_CURSORS

  Auf „3000 gemeinsam genutzt“ festlegen.

  Überwachen und Anpassen von offenen Cursorn. Abfragen von `v$sesstat`, um die Anzahl der aktuell offenen Cursor zu ermitteln. Wenn die Sitzungen nahe der Auslastungsgrenze ausgeführt werden, erhöhen Sie den Wert für OPEN_CURSORS.

  UNDO_MANAGEMENT

  Auf AUTO festlegen.

- Wenn im Repository Metadaten in einer Multibyte-Sprache gespeichert werden müssen, setzen Sie den Parameter NLS_LENGTH_SEMANTICS in der Datenbankinstanz auf CHAR. Die Standardeinstellung lautet BYTE.
- Informatica bietet keine Unterstützung für öffentliche Oracle-Synonyme für Repository-Tabellen. Stellen Sie sicher, dass für keine der Tabellen in der Datenbank öffentliche Synonyme erstellt wurden.

Modellrepository-Datenbankanforderungen

Informatica-Dienste und Clients speichern Daten und Metadaten im Modellrepository. Richten Sie vor der Erstellung des Modellrepository-Diensts eine Datenbank und ein Datenbank-Benutzerkonto für das Modellrepository ein.

Das Modellrepository unterstützt die folgenden Datenbanktypen:

- IBM DB2 UDB
- Microsoft SQL Server
- Oracle

Zulassen von 3 GB Speicherplatz für DB2. Lassen Sie 200 MB Festplattenspeicher für alle anderen Datenbanktypen zu.

Weitere Informationen zum Konfigurieren der Datenbank finden Sie in der Dokumentation zu Ihrem Datenbanksystem.

IBM DB2-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository in IBM DB2 die folgenden Richtlinien:

- Wenn sich das Repository in einer IBM DB2 9.7-Datenbank befindet, stellen Sie sicher, dass IBM DB2 Version 9.7 Fix Pack 7 oder ein späteres Fixpack installiert ist.
- Setzen Sie die folgenden Parameter in der IBM DB2-Instanz, in der Sie die Datenbank erstellen, auf ON:
  - DB2_SKIPINSERTED
  - DB2_EVALUNCOMMITTED
  - DB2_SKIPDELETED
  - AUTO_RUNSTATS
- Legen Sie die Konfigurationsparameter in der Datenbank fest.

  In der folgenden Tabelle werden die Konfigurationsparameter aufgelistet, die Sie festlegen müssen:

Parameter	Wert
logfilsiz	8000
maxlocks	98
locklist	50000
auto_stmt_stats	ON

- Setzen Sie den Tablespace-Parameter pageSize auf 32768 Byte.

  Legen Sie in einer Datenbank mit einer einzigen Partition einen Tablespace fest, der die pageSize-Anforderungen erfüllt. Wenn Sie keinen Tablespace festlegen, muss der Standard-Tablespace die pageSize-Anforderungen erfüllen.

  Legen Sie in einer Datenbank mit mehreren Partitionen einen Tablespace fest, der die pageSize-Anforderungen erfüllt. Definieren Sie den Tablespace in der Katalogpartition der Datenbank.
- Legen Sie den NPAGES-Parameter auf mindestens 5000 fest. Der NPAGES-Parameter bestimmt die Anzahl der Seiten im Tabellenbereich.

- Stellen Sie sicher, dass der Datenbankbenutzer über die Berechtigungen CREATETAB, CONNECT und BINDADD verfügt.
- Informatica bietet keine Unterstützung für IBM DB2-Tabellenaliase für Repository-Tabellen. Stellen Sie sicher, dass für keine Tabellen in der Datenbank Tabellenaliase erstellt wurden.
- Aktualisieren Sie im Dienstprogramm DataDirect Connect for JDBC den Parameter DynamicSections auf 3000.

  Der Standardwert von DynamicSections ist zu niedrig für die Informatica-Repositorys. Für Informatica ist ein größeres DB2-Paket als das Standardpaket erforderlich. Beim Einrichten der DB2-Datenbank für das Domänenkonfigurations-Repository oder ein Modellrepository müssen Sie den Parameter DynamicSections auf einen Wert von mindestens 3000 einstellen. Wenn der Parameter DynamicSections auf einen niedrigeren Wert eingestellt ist, kann es beim Installieren oder Ausführen von Informatica-Diensten zu Problemen kommen.

  Weitere Informationen zur Aktualisierung des Parameters DynamicSections finden Sie unter Anhang D, “Aktualisieren des DynamicSections-Parameters einer DB2-Datenbank” auf Seite 285.

Microsoft SQL Server-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository in Microsoft SQL Server die folgenden Richtlinien:

- Legen Sie die Isolationsstufe "Allow Snapshot Isolation" und "Read Committed" auf ALLOW_SNAPSHOT_ISOLATION und READ_COMMITTED_SNAPSHOT fest, um Konflikte zu minimieren. Führen Sie zum Festlegen der Isolationsebene für die Datenbank die folgenden Befehle aus:

  ```
  ALTER DATABASE DatabaseName SET ALLOW_SNAPSHOT_ISOLATION ON
  ```

  ```
  ALTER DATABASE DatabaseName SET READ_COMMITTED_SNAPSHOT ON
  ```

  Führen Sie den folgenden Befehl aus, um zu überprüfen, ob die Isolationsebene für die Datenbank richtig ist:

  ```
  SELECT snapshot_isolation_state FROM sys.databases WHERE name=[Datenbankname]
  ```

  Hinweis: Um die Snapshot-Isolation zu aktivieren, legen Sie snapshot_isolation_state mit 1 fest. Beispiel: `snapshot_isolation_state=1`.

  ```
  SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name = DatabaseName
  ```

- Das Datenbankbenutzerkonto muss über die Berechtigungen CONNECT, CREATE TABLE und CREATE VIEW verfügen.

Oracle-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository in Oracle die folgenden Richtlinien:

- Setzen Sie den Parameter „open_cursors“ auf 2000 oder höher.
- Stellen Sie sicher, dass der Datenbankbenutzer über die folgenden Berechtigungen verfügt:

  CREATE SEQUENCE

  CREATE SESSION

  CREATE SYNONYM

  CREATE TABLE

  CREATE VIEW

- Informatica bietet keine Unterstützung für öffentliche Oracle-Synonyme für Repository-Tabellen. Stellen Sie sicher, dass für keine der Tabellen in der Datenbank öffentliche Synonyme erstellt wurden.

PowerCenter-Repository-Datenbankanforderungen

Ein PowerCenter-Repository ist eine Zusammenstellung von Datenbanktabellen mit Metadaten. Ein PowerCenter-Repository-Dienst verwaltet das Repository und führt alle Metadaten-Transaktionen zwischen der Repository-Datenbank und Repository-Clients aus.

Das PowerCenter-Repository unterstützt die folgenden Datenbanktypen:

- IBM DB2 UDB
- Microsoft SQL Server
- Oracle
- Sybase ASE

Zulassen von 35 MB Speicherplatz für die Datenbank.

Hinweis: Stellen Sie sicher, dass Sie den Datenbank-Client auf dem Computer installieren, auf dem Sie den PowerCenter-Repository-Dienst ausführen möchten.

Weitere Informationen zum Konfigurieren der Datenbank finden Sie in der Dokumentation zu Ihrem Datenbanksystem.

IBM DB2-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository in IBM DB2 die folgenden Richtlinien:

- Richten Sie die Datenbank zur Optimierung der Repository-Leistung mit dem Tabellenbereich auf einem Einzelknoten ein. Wenn sich der Tabellenbereich auf einem einzigen Knoten befindet, greifen PowerCenter Client und PowerCenter-Integrationsdienst schneller auf das Repository zu, als wenn sich die Repository-Tabellen auf unterschiedlichen Datenbankknoten befinden.

  Legen Sie den Einzelknoten-Tabellenbereich-Namen beim Erstellen, Kopieren oder Wiederherstellen eines Repository fest. Wenn Sie keinen Tabellenbereich-Namen angeben, verwendet DB2 den Standard-Tabellenbereich.
- Informatica bietet keine Unterstützung für IBM DB2-Tabellenaliase für Repository-Tabellen. Stellen Sie sicher, dass für keine Tabellen in der Datenbank Tabellenaliase erstellt wurden.

Microsoft SQL Server-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository in Microsoft SQL Server die folgenden Richtlinien:

- Stellen Sie die Seitengröße des Datenbankservers auf mindestens 8 K ein. Diese Konfiguration wird nur einmal vorgenommen und kann später nicht mehr geändert werden.
- Stellen Sie sicher, dass das Datenbankbenutzerkonto über die Berechtigungen CONNECT, CREATE TABLE und CREATE VIEW verfügt.

Oracle-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository in Oracle die folgenden Richtlinien:

- Halten Sie die Speichergröße für den Tabellenbereich gering, damit das Repository nicht zu viel Speicherplatz in Anspruch nimmt. Überprüfen Sie, ob die Größe des Standard-Tabellenbereichs des Eigentümers der Repository-Tabellen auf einen niedrigen Wert eingestellt ist.

Das nachfolgende Beispiel demonstriert, wie der empfohlene Speicherparameter für einen Tablespace namens REPOSITORY festgelegt wird:

```
ALTER TABLESPACE "REPOSITORY" DEFAULT STORAGE ( INITIAL 10K NEXT 10K MAXEXTENTS
UNLIMITED PCTINCREASE 50 );
```

Überprüfen oder ändern Sie die Speicherparameter für den Tabellenbereich, bevor Sie das Repository erstellen.

- Stellen Sie sicher, dass der Datenbankbenutzer über die folgenden Berechtigungen verfügt:

  CREATE SEQUENCE

  CREATE SESSION

  CREATE SYNONYM

  CREATE TABLE

  CREATE VIEW

- Informatica bietet keine Unterstützung für öffentliche Oracle-Synonyme für Repository-Tabellen. Stellen Sie sicher, dass für keine der Tabellen in der Datenbank öffentliche Synonyme erstellt wurden.

Sybase ASE-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository in Sybase ASE die folgenden Richtlinien:

- Stellen Sie die Seitengröße des Datenbankservers auf mindestens 8 K ein. Diese Konfiguration wird nur einmal vorgenommen und kann später nicht mehr geändert werden.
- Legen Sie die Sybase-Datenbankoption „ddl in tran“ auf TRUE fest.
- Legen Sie „allow nulls by default“ auf TRUE fest.
- Stellen Sie sicher, dass der Datenbankbenutzer über die Berechtigungen CREATE TABLE und CREATE VIEW verfügt.
- Legen Sie die Konfigurationsanforderungen für den Datenbankspeicher fest.
  In der folgenden Tabelle sind die Konfigurationsanforderungen für den Speicher und die empfohlenen Baseline-Werte aufgeführt:

Datenbankkonfiguration	Sybase-Systemprozedur	Wert
Anzahl geöffneter Objekte	sp_configure "number of open objects"	5000
Anzahl geöffneter Indizes	sp_configure "number of open indexes"	5000
Anzahl geöffneter Partitionen	sp_configure "number of open partitions"	8000
Anzahl Sperren	sp_configure "number of locks"	100000

Anforderungen an das Profiling-Warehouse

In der Profiling-Warehouse-Datenbank werden Profiling- und Scorecard-Ergebnisse gespeichert. Beim Erstellen des Datenintegrationsdiensts geben Sie die Profiling-Warehouse-Verbindung an.

Das Profiling-Warehouse unterstützt die folgenden Datenbanktypen:

- IBM DB2 UDB
- Microsoft SQL Server
- Oracle

Zulassen von 10 GB Speicherplatz für die Datenbank.

Hinweis: Stellen Sie sicher, dass Sie den Datenbank-Client auf dem Computer installieren, auf dem Sie den Datenintegrationsdienst ausführen möchten. Sie können eine JDBC-Verbindung oder Hive-Verbindung als Profiling-Warehouse-Verbindung für IBM DB2 UDB, Microsoft SQL Server und Oracle-Datenbanktypen festlegen.

Weitere Informationen zum Konfigurieren der Datenbank finden Sie in der Dokumentation zu Ihrem Datenbanksystem.

IBM DB2-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository in IBM DB2 die folgenden Richtlinien:

- Das Datenbankbenutzerkonto muss über die Berechtigungen CREATETAB, CONNECT, CREATE VIEW und CREATE FUNCTION verfügen.
- Informatica bietet keine Unterstützung für IBM DB2-Tabellenaliase für Repository-Tabellen. Stellen Sie sicher, dass für keine Tabellen in der Datenbank Tabellenaliase erstellt wurden.
- Setzen Sie den Tablespace-Parameter pageSize auf 32768 Byte.
- Legen Sie den NPAGES-Parameter auf mindestens 5000 fest. Der NPAGES-Parameter bestimmt die Anzahl der Seiten im Tabellenbereich.

Hinweis: Informatica unterstützt die partitionierte Datenbankumgebung für IBM DB2-Datenbanken nicht, wenn Sie eine JDBC-Verbindung als Profiling-Warehouse-Verbindung verwenden.

Microsoft SQL Server-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository in Microsoft SQL Server die folgenden Richtlinien:

- Das Datenbankbenutzerkonto muss über die Berechtigungen CONNECT, CREATE TABLE, CREATE VIEW und CREATE FUNCTION verfügen.

Oracle-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository in Oracle die folgenden Richtlinien:

- Stellen Sie sicher, dass der Datenbankbenutzer über die folgenden Berechtigungen verfügt:

  ALTER TABLE

  CREATE ANY INDEX

  CREATE PROCEDURE

  CREATE SESSION

  CREATE TABLE

  CREATE VIEW

  DROP TABLE

  UPDATE TABLE
- Informatica bietet keine Unterstützung für öffentliche Oracle-Synonyme für Repository-Tabellen. Stellen Sie sicher, dass für keine der Tabellen in der Datenbank öffentliche Synonyme erstellt wurden.
- Legen Sie den Tablespace-Parameter fest. Verwenden Sie die folgende Formel zur Bestimmung des Wertes: 2 MB x (Anzahl der Tabellen in jedem Scan x Anzahl gleichzeitiger Scans)
  Sie haben beispielsweise 1.000 Tabellen in jedem Scan und möchten 10 Scans gleichzeitig ausführen. Berechnen Sie den Wert des Tablespace-Parameters wie folgt: 2 MB x (100 x 10) = 20 GB

  Hinweis: Tablespace muss über mehrere Festplatten verteilt sein.
- Legen Sie die folgenden Parameter auf die von Informatica empfohlenen Werte fest:

Parameter	Empfohlener Wert
open_cursors	3000
Sitzungen	1000
Prozesse	1000

Anforderungen des Referenzdaten-Warehouse

Das Referenzdaten-Warehouse speichert die Datenwerte für die Referenztabellenobjekte, die Sie in einem Modellrepository definieren. Konfigurieren Sie einen Content Management Service, um das Referenzdaten-Warehouse und das Modellrepository zu identifizieren.

Sie verbinden ein Referenzdaten-Warehouse mit einem einzigen Modellrepository. Sie können ein gemeinsames Referenzdaten-Warehouse auf mehreren Content-Management-Diensten auswählen, wenn die Content-Management-Dienste ein gemeinsames Modellrepository identifizieren. Das Referenzdaten-Warehouse muss Spaltennamen mit Groß- und Kleinbuchstaben unterstützen.

Das Referenzdaten-Warehouse unterstützt die folgenden Datenbanktypen:

- IBM DB2 UDB
- Microsoft SQL Server
- Oracle

Zulassen von 200 MB Speicherplatz für die Datenbank.

Hinweis: Stellen Sie sicher, dass Sie den Datenbank-Client auf dem Computer installieren, auf dem der Content-Management-Dienst ausgeführt werden soll.

IBM DB2-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository in IBM DB2 die folgenden Richtlinien:

- Stellen Sie sicher, dass das Datenbankbenutzerkonto über die Berechtigungen CREATETAB und CONNECT verfügt.
- Stellen Sie sicher, dass der Datenbankbenutzer über SELECT-Berechtigungen für die Tabellen SYSCAT.DBAUTH und SYSCAT.DBTABAUTH verfügt.
- Informatica bietet keine Unterstützung für IBM DB2-Tabellenaliase für Repository-Tabellen. Stellen Sie sicher, dass für keine Tabellen in der Datenbank Tabellenaliase erstellt wurden.
- Setzen Sie den Tablespace-Parameter pageSize auf 32768 Byte.
- Legen Sie den NPAGES-Parameter auf mindestens 5000 fest. Der NPAGES-Parameter bestimmt die Anzahl der Seiten im Tabellenbereich.

Microsoft SQL Server-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository in Microsoft SQL Server die folgenden Richtlinien:

- Stellen Sie sicher, dass das Datenbankbenutzerkonto über die Berechtigungen CONNECT und CREATE TABLE verfügt.

Oracle-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository in Oracle die folgenden Richtlinien:

- Stellen Sie sicher, dass der Datenbankbenutzer über die folgenden Berechtigungen verfügt:

  ALTER SEQUENCE

  ALTER TABLE

  CREATE SEQUENCE

  CREATE SESSION

  CREATE TABLE

  CREATE VIEW

  DROP SEQUENCE

  DROP TABLE
- Informatica bietet keine Unterstützung für öffentliche Oracle-Synonyme für Repository-Tabellen. Stellen Sie sicher, dass für keine der Tabellen in der Datenbank öffentliche Synonyme erstellt wurden.

Anforderungen an Arbeitsablauf-Datenbanken

Der Datenintegrationsdienst speichert Laufzeitmetadaten für Arbeitsabläufe in der Arbeitsablauf-Datenbank. Bevor Sie die Arbeitsablauf-Datenbank erstellen, richten Sie eine Datenbank und ein Datenbankbenutzerkonto für die Arbeitsablauf-Datenbank ein.

Beim Erstellen des Datenintegrationsdiensts geben Sie die Arbeitsablauf-Datenbankverbindung an.

Die Arbeitsablauf-Datenbank unterstützt die folgenden Datenbanktypen:

- IBM DB2 UDB
- Microsoft SQL Server
- Oracle

Zulassen von 200 MB Speicherplatz für die Datenbank.

Hinweis: Stellen Sie sicher, dass Sie den Datenbank-Client auf dem Computer installieren, auf dem Sie den Datenintegrationsdienst ausführen möchten.

IBM DB2-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository in IBM DB2 die folgenden Richtlinien:

- Stellen Sie sicher, dass das Datenbankbenutzerkonto über die Berechtigungen CREATETAB und CONNECT verfügt.
- Informatica bietet keine Unterstützung für IBM DB2-Tabellenaliase für Repository-Tabellen. Stellen Sie sicher, dass für keine Tabellen in der Datenbank Tabellenaliase erstellt wurden.
- Setzen Sie den Tablespace-Parameter pageSize auf 32768 Byte.
- Legen Sie den NPAGES-Parameter auf mindestens 5000 fest. Der NPAGES-Parameter bestimmt die Anzahl der Seiten im Tabellenbereich.
- Legen Sie die Verbindungspooling-Parameter fest.

  In der folgenden Tabelle werden die Verbindungspooling-Parameter aufgelistet, die Sie festlegen müssen:

Parameter	Wert
Die maximale Verbindungspoolgröße	128
Minimale Verbindungspoolgröße	0
Maximale Leerlaufzeit	120 Sekunden

Microsoft SQL Server-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository in Microsoft SQL Server die folgenden Richtlinien:

- Stellen Sie sicher, dass das Datenbankbenutzerkonto über die Berechtigungen CONNECT und CREATE TABLE verfügt.
- Aktivieren Sie die JTA- und XA-Datenquellenfunktionalität in der Datenbank.
- Legen Sie die Verbindungspooling-Parameter fest.

In der folgenden Tabelle werden die Verbindungspooling-Parameter aufgelistet, die Sie festlegen müssen:

Parameter	Wert
Die maximale Verbindungspoolgröße	128
Minimale Verbindungspoolgröße	0
Maximale Leerlaufzeit	120 Sekunden

Oracle-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository in Oracle die folgenden Richtlinien:

- Stellen Sie sicher, dass der Datenbankbenutzer über die folgenden Berechtigungen verfügt:

  ALTER TABLE

  ALTER VIEW

  CREATE SEQUENCE

  CREATE SESSION

  CREATE SYNONYM

  CREATE TABLE

  CREATE VIEW

  DROP TABLE

  DROP VIEW
- Informatica bietet keine Unterstützung für öffentliche Oracle-Synonyme für Repository-Tabellen. Stellen Sie sicher, dass für keine der Tabellen in der Datenbank öffentliche Synonyme erstellt wurden.
- Legen Sie die Verbindungspooling-Parameter fest.

  In der folgenden Tabelle werden die Verbindungspooling-Parameter aufgelistet, die Sie festlegen müssen:

Parameter	Wert
Die maximale Verbindungspoolgröße	128
Minimale Verbindungspoolgröße	0
Maximale Leerlaufzeit	120 Sekunden

Konfigurieren der nativen Konnektivität auf dem Dienst-Computer

Um die native Konnektivität zwischen einem Anwendungsdienst und einer Datenbank einzurichten, installieren Sie die Datenbank-Client-Software für die Datenbank, auf die Sie zugreifen möchten.

Native Treiber werden mit dem Datenbankserver und der Clientsoftware geliefert. Konfigurieren Sie die Konnektivität auf den Computern, die auf die Datenbanken zugreifen müssen. Um die Kompatibilität zwischen

dem Anwendungsdienst und der Datenbank zu gewährleisten, installieren Sie eine Client-Software, die mit der Datenbankversion kompatibel ist, und verwenden Sie die entsprechenden Bibliotheken des Datenbank-Client.

Weitere Informationen zum Konfigurieren der Konnektivität finden Sie im Anhang C, “Verbinden zu Datenbanken unter UNIX” auf Seite 260 und Anhang B, “Verbinden zu Datenbanken unter Windows” auf Seite 250.

Die folgenden Dienste verwenden native Konnektivität für eine Verbindung zu anderen Datenbanken:

Datenintegrationsdienst

Der Datenintegrationsdienst verwendet native Datenbanktreiber zum Verbinden mit den folgenden Datenbanken:

- Quell- und Zieldatenbanken. Liest Daten aus Quelldatenbanken und schreibt Daten in Zieldatenbanken.
- Datenobjekt-Cache-Datenbank. Speichert den Datenobjekt-Cache.
- Profiling-Quelldatenbanken. Liest aus relationalen Quelldatenbanken zum Ausführen von Profilen für die Quellen.
- Profiling warehouse. Schreibt die Profiling-Ergebnisse in das Profiling Warehouse.
- Referenztabellen. Führt Mappings zum Übertragen von Daten zwischen den Referenztabellen und den externen Datenquellen aus.

Wenn der Datenintegrationsdienst auf einem einzigen Knoten bzw. auf primären Knoten und Backup-Knoten ausgeführt wird, installieren Sie Datenbank-Client-Software und konfigurieren Sie die Konnektivität auf den Computern, auf denen der Datenintegrationsdienst ausgeführt wird.

Wird der Datenintegrationsdienst in einem Gitter ausgeführt, so installieren Sie die Datenbank-Client-Software und konfigurieren Sie die Konnektivität auf jedem Computer, der einen Knoten mit der Berechnungsrolle bzw. einen Knoten darstellt, der sowohl über die Dienst- als auch über die Berechnungsrolle verfügt.

PowerCenter-Repository-Dienst

Der PowerCenter-Repository-Dienst verwendet native Datenbanktreiber zum Herstellen einer Verbindung mit der PowerCenter-Repository-Datenbank.

Installieren Sie die Datenbank-Client-Software und konfigurieren Sie die Konnektivität auf den Computern, auf denen der PowerCenter-Repository-Dienst und die PowerCenter-Repository-Dienstprozesse ausgeführt werden.

PowerCenter-Integrationsdienst

Der PowerCenter-Integrationsdienst verwendet native Datenbanktreiber zum Verbinden mit den folgenden Datenbanken:

- Quell- und Zieldatenbanken. Liest aus den Quelldatenbanken und schreibt in Zieldatenbanken.
- Metadata Manager-Quelldatenbanken. Lädt die relationalen Datenquellen in Metadata Manager.

Installieren Sie die Datenbank-Client-Software für die relationalen Datenquellen und die Repository-Datenbank auf den Computern, auf denen der PowerCenter-Integrationsdienst ausgeführt wird.

Installieren der Datenbank-Client-Software

Sie müssen die Datenbank-Clients auf den erforderlichen Computern basierend auf den Datenbanktypen installieren, auf die die Anwendungsdienste zugreifen.

Um die Kompatibilität zwischen dem Anwendungsdienst und der Datenbank zu gewährleisten, verwenden Sie die entsprechenden Datenbank-Client-Bibliotheken, und installieren Sie eine Client-Software, die mit der Datenbankversion kompatibel ist.

Installieren Sie die folgende Datenbank-Client-Software basierend auf dem Typ der Datenbank, auf den der Anwendungsdienst zugreift:

IBM DB2 Client Application Enabler (CAE)

Konfigurieren Sie die Konnektivität auf den erforderlichen Computern, indem Sie sich beim Computer als der Benutzer anmelden, der die Informatica-Dienste startet.

Microsoft SQL Server 2012 Native Client

Laden Sie den Client von der folgenden Microsoft-Website herunter: http://www.microsoft.com/en-in/download/details.aspx?id=29065.

Oracle-Client

Installieren Sie die kompatiblen Versionen des Oracle-Client und Oracle-Datenbankservers. Außerdem müssen Sie dieselbe Version des Oracle-Client auf allen Computern installieren, die ihn benötigen. Informationen zur Überprüfung der Kompatibilität erhalten Sie von Oracle.

Sybase Open Client (OCS)

Installieren Sie eine mit dem Sybase ASE-Datenbankserver kompatible Version von Open Client Sie müssen dieselbe Version von Open Client auf den Computern installieren, auf denen sich die Sybase ASE-Datenbank und Informatica befinden. Informationen zur Überprüfung der Kompatibilität erhalten Sie von Sybase.

Konfigurieren von Datenbank-Client-Umgebungsvariablen auf UNIX

Konfigurieren Sie die Datenbank-Client-Umgebungsvariablen auf den Computern, auf denen Datenintegrationsdienst-, PowerCenter-Integrationsdienst- und PowerCenter-Repository-Dienst-Prozesse ausgeführt werden.

Pfad-Variablenname und Anforderungen des Datenbank-Client hängen von der UNIX-Plattform und der Datenbank ab.

Nach dem Konfigurieren der Datenbank-Umgebungsvariablen können Sie die Verbindung zur Datenbank über den Datenbank-Client testen.

In der nachstehenden Tabelle sind die Datenbank-Umgebungsvariablen aufgelistet, die Sie unter UNIX festlegen müssen:

Datenbank	Name der Umgebungsvariable	Datenbank-Dienstprogramm	Wert
Oracle	ORACLE_HOME PATH	sqlplus	Setzen Sie sie auf: <*DatabasePath*> Fügen Sie hinzu: <*DatabasePath*>/bin
IBM DB2	DB2DIR DB2INSTANCE PATH	db2connect	Setzen Sie sie auf: <*DatabasePath*> Setzen Sie sie auf: <*DB2InstanceName*> Fügen Sie hinzu: <*DatabasePath*>/bin
Sybase ASE	SYBASE15 SYBASE_ASE SYBASE_OCS PATH	isql	Setzen Sie sie auf: <*DatabasePath*>/sybase<*version*> Setzen auf: ${SYBASE15}/ASE-<*version*> Setzen auf: ${SYBASE15}/OCS-<*version*> Fügen Sie hinzu: ${SYBASE_ASE}/bin:${SYBASE_OCS}/bin:$PATH

Verbindungszeichenfolge für eine sichere Datenbank

Wenn Sie ein Repository auf einer sicheren Datenbank erstellen, müssen Sie die Truststore-Informationen für die Datenbank und eine JDBC-Verbindungszeichenfolge bereitstellen, die die Sicherheitsparameter für die Datenbank enthält.

Während der Installation können Sie das Domänenkonfigurations-Repository in einer sicheren Datenbank erstellen. Sie können auch das Modellrepository in einer sicheren Datenbank erstellen.

Sie können eine sichere Verbindung für die folgenden Datenbanken konfigurieren:

- IBM DB2 UDB
- Microsoft SQL Server
- Oracle

Hinweis: Sie können keine sichere Verbindung zu einer Sybase-Datenbank konfigurieren.

Beim Konfigurieren der Verbindung für die sichere Datenbank müssen Sie die Verbindungsinformationen in einer JDBC-Verbindungszeichenfolge angeben. Neben dem Hostnamen und der Portnummer für den Datenbankserver muss die Verbindungszeichenfolge auch Sicherheitsparameter enthalten.

In der folgenden Tabelle werden die Sicherheitsparameter beschrieben, die in die JDBC-Verbindungszeichenfolge aufgenommen werden müssen:

Parameter	Beschreibung
EncryptionMethod	Erforderlich. Gibt an, ob Daten bei der Netzwerkübertragung verschlüsselt werden. Dieser Parameter muss auf `SSL` festgelegt werden.
ValidateServerCertificate	Optional. Gibt an, ob Informatica das Zertifikat validiert, das vom Datenbankserver gesendet wird. Wenn dieser Parameter auf TRUE festgelegt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat. Wenn Sie den HostNameInCertificate-Parameter angeben, validiert Informatica ebenfalls den Hostnamen im Zertifikat. Wenn dieser Parameter auf "false" festgelegt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat nicht. Informatica ignoriert alle Truststore-Informationen, die Sie angeben.
HostNameInCertificate	Optional. Hostname des Computers, auf dem die sichere Datenbank gehostet wird. Wenn Sie einen Hostnamen angeben, validiert Informatica den Hostnamen in der Verbindungszeichenfolge mit dem Hostnamen im SSL-Zertifikat. Wenn SSL-Verschlüsselung und Validierung aktiviert sind und diese Eigenschaft nicht angegeben wurde, verwendet der Treiber den in der Verbindungs-URL oder der Datenquelle der Verbindung angegebenen Servernamen, um das Zertifikat zu validieren.
cryptoProtocolVersion	Erforderlich. Gibt das Kryptografieprotokoll an, das für die Verbindung mit einer sicheren Datenbank verwendet werden soll. Sie können je nach dem vom Datenbankserver verwendeten Kryptografieprotokoll den Parameter auf `cryptoProtocolVersion=TLSv1.1` oder `cryptoProtocolVersion=TLSv1.2` festlegen.

Sie können folgende Syntax in der JDBC-Verbindungszeichenfolge verwenden, um eine Verbindung zu einer sicheren Datenbank herzustellen:

IBM DB2

```
jdbc:Informatica:db2://
host_name:port_no;DatabaseName=database_name;EncryptionMethod=SSL;HostNameInCertificate=D
B_host_name;ValidateServerCertificate=true_or_false
```

Oracle

```
jdbc:Informatica:oracle://
host_name:port_no;ServiceName=service_name;EncryptionMethod=SSL;HostNameInCertificate=DB_
host_name;ValidateServerCertificate=true_or_false
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://
host_name:port_no;SelectMethod=cursor;DatabaseName=database_name;EncryptionMethod=SSL;Hos
tNameInCertificate=DB_host_name;ValidateServerCertificate=true_or_false
```

Hinweis: Die Verbindungszeichenfolge wird vom Installationsprogramm nicht überprüft. Stellen Sie sicher, dass die Verbindungszeichenfolge alle von der Datenbank benötigten Verbindungs- und Sicherheitsparameter enthält.

KAPITEL 4

Vorbereiten der Einrichtung der Kerberos-Authentifizierung

Dieses Kapitel umfasst die folgenden Themen:

- Vorbereiten der Einrichtung der Kerberos-Authentifizierung - Übersicht, 73
- Einrichten der Kerberos-Konfigurationsdatei, 74
- Generieren des Namensformats für Dienstprinzipale und Keytab-Dateien, 75
- Überprüfen der SPN- und Keytab-Format-Textdatei, 80
- Erstellen der Dienstprinzipalnamen und Keytab-Dateien, 82

Vorbereiten der Einrichtung der Kerberos-Authentifizierung - Übersicht

Sie können die Informatica-Domäne für die Verwendung der Kerberos-Netzwerkauthentifizierung konfigurieren, um Benutzer, Dienste und Knoten zu authentifizieren.

Kerberos ist ein Netzwerkauthentifizierungsprotokoll, das Tickets zur Authentifizierung des Zugriffs auf Dienste und Knoten in einem Netzwerk verwendet. Kerberos verwendet ein KDC (Key Distribution Center), um die Identität von Benutzern und Diensten zum Gewähren von Tickets für authentifizierte Benutzer- und Dienstkonten zu validieren. Im Kerberos-Protokoll werden Benutzer und Dienste als Prinzipale bezeichnet. Das KDC verfügt über eine Datenbank mit Prinzipalen und deren zugeordneten Geheimschlüssel, die als Beweis für ihre Identität verwendet werden. Kerberos kann einen LDAP-Verzeichnisdienst als eine Prinzipaldatenbank verwenden.

Um die Kerberos-Authentifizierung zu verwenden, müssen Sie die Informatica-Domäne in einem Netzwerk installieren und ausführen, das die Kerberos-Netzwerk-Authentifizierung verwendet. Informatica kann in einem Netzwerk ausgeführt werden, das die Kerberos-Authentifizierung mit dem Microsoft Active Directory-Verzeichnisdienst als Prinzipaldatenbank verwendet.

Die Informatica-Domäne benötigt Keytab-Dateien zur Authentifizierung von Knoten und Diensten in der Domäne, ohne Passwörter über das Netzwerk zu übertragen. Die Keytab-Dateien enthalten SPNs und zugeordnete verschlüsselte Schlüssel. Erstellen Sie die Keytab-Dateien, bevor Sie Knoten und Dienste in der Informatica-Domäne erstellen.

Führen Sie vor der Konfiguration von Kerberos-Authentifizierung für die Domäne die folgenden Aufgaben durch:

- Einrichten der Kerberos-Konfigurationsdatei.

- Generieren der Namen für Dienstprinzipale und Keytab-Dateien im Informatica-Format.
- Überprüfen der SPN- und Keytab-Format-Textdatei
- Bitten Sie den Kerberos-Administrator, den SPN zur Kerberos-Prinzipaldatenbank hinzuzufügen und die Keytab-Dateien zu erstellen.

Einrichten der Kerberos-Konfigurationsdatei

Kerberos speichert Konfigurationsinformationen in einer Datei mit der Bezeichnung *krb5.conf*. Für Informatica müssen in der Kerberos-Konfigurationsdatei bestimmte Eigenschaften eingerichtet werden, damit Kerberos-Authentifizierung in der Informatica-Domäne ordnungsgemäß verwendet werden kann. Sie müssen die Eigenschaften in der krb5.conf-Konfigurationsdatei festlegen.

Die Konfigurationsdatei enthält die Informationen über den Kerberos-Server, einschließlich des Kerberos-Bereichs und der KDC-Adresse. Sie können den Kerberos-Administrator bitten, die Eigenschaften in der Konfigurationsdatei einzurichten und Ihnen eine Kopie der Datei zu senden.

1. Sichern Sie die Datei „krb5.conf“, bevor Sie Änderungen vornehmen.
2. Bearbeiten Sie die Datei „krb5.conf“.
3. Legen Sie im Abschnitt *libdefaults* die von Informatica benötigten Eigenschaften fest oder fügen Sie sie hinzu.

   In der folgenden Tabelle werden die Werte aufgelistet, für die im Abschnitt „libdefaults“ Eigenschaften festgelegt werden müssen:

Parameter	Wert
default_realm	Name des Dienstbereichs für die Informatica-Domäne.
forwardable	Ermöglicht es einem Dienst, Client-Benutzeranmeldedaten an einen anderen Dienst zu delegieren. Legen Sie diesen Parameter auf TRUE fest. Für die Informatica-Domäne müssen Anwendungsdienste die Client-Benutzeranmeldedaten bei anderen Diensten authentifizieren.
default_tkt_enctypes	Verschlüsselungstyp für den Sitzungsschlüssel im TGT (Ticket-Granting Ticket). Legen Sie diesen Parameter auf *rc4-hmac* fest. Informatica unterstützt nur den Verschlüsselungstyp *rc4-hmac*.
udp_preference_limit	Legt das Protokoll fest, das Kerberos beim Senden einer Meldung an den KDC verwendet. Setzen Sie „udp_preference_limit = 1“ fest, damit TCP immer verwendet wird. Die Informatica-Domäne unterstützt nur das TCP-Protokoll. Wenn für „udp_preference_limit“ ein anderer Wert gesetzt wurde, kann die Informatica-Domäne unerwartet heruntergefahren werden.

4. Schließen Sie im Abschnitt *Bereiche* die Portnummer in die Adresse des KDC, getrennt durch einen Doppelpunkt, ein.

   Beispiel: Wenn die KDC-Adresse „kerberos.example.com“ lautet und die Portnummer „88“ ist, legen Sie den Parameter *kdc* wie folgt fest:

   ```
   kdc = kerberos.example.com:88
   ```

5. Speichern Sie die Datei „krb5.conf“.

6. Speichern Sie die Datei „krb5.conf“ in einem Verzeichnis, das auf dem Rechner zugänglich ist, wenn Sie vorhaben, die Informatica-Dienste zu installieren.

Im folgenden Beispiel wird der Inhalt einer krb5.conf-Datei mit den erforderlichen Eigenschaften angezeigt:

```
[libdefaults]
default_realm = AFNIKRB.AFNIDEV.COM
forwardable = true
default_tkt_enctypes = rc4-hmac
udp_preference_limit = 1

[realms]
AFNIKRB.AFNIDEV.COM = {
  admin_server = SMPLKERDC01.AFNIKRB.AFNIDEV.COM
  kdc = SMPLKERDC01.AFNIKRB.AFNIDEV.COM:88
 }

[domain_realm]
afnikrb.afnidev.com = AFNIKRB.AFNIDEV.COM
.afnikrb.afnidev.com = AFNIKRB.AFNIDEV.COM
```

Weitere Informationen über die Kerberos-Konfigurationsdatei finden Sie in der Dokumentation zur Kerberos-Netzwerkauthentifizierung.

Generieren des Namensformats für Dienstprinzipale und Keytab-Dateien

Wenn Sie die Informatica-Domäne mit Kerberos-Authentifizierung ausführen, müssen Sie Kerberos-Dienstprinzipalnamen (SPN) und Keytab-Dateien mit den Knoten und Diensten in der Domäne verknüpfen. Informatica benötigt Keytab-Dateien zum Authentifizieren von Diensten, ohne Passwörter anzufragen.

Je nach den Sicherheitsanforderungen für die Domäne können Sie eine der folgenden beiden Ebenen als Dienstprinzipalebene festlegen:

Knotenebene

Wenn die Domäne zum Testen oder für die Entwicklung verwendet wird und keine hohe Sicherheitsstufe erfordert, können Sie die Knotenebene als Dienstprinzipalebene festlegen. Sie können einen SPN und eine Keytab-Datei für den Knoten und für alle Dienstprozesse auf dem Knoten verwenden. Außerdem müssen Sie einen separaten SPN und eine separate Keytab-Datei für die HTTP-Prozesse auf dem Knoten festlegen.

Prozessebene

Wenn die Domäne zur Produktion verwendet wird und eine hohe Sicherheitsstufe erfordert, können Sie die Prozessebene als Dienstprinzipalebene festlegen. Erstellen Sie einen eindeutigen SPN und eine eigene Keytab-Datei für jeden Knoten und für jeden Prozess auf dem Knoten. Außerdem müssen Sie einen separaten SPN und eine separate Keytab-Datei für die HTTP-Prozesse auf dem Knoten festlegen.

Für die Informatica-Domäne müssen der Dienstprinzipal und die Keytab-Dateinamen ein bestimmtes Format aufweisen. Um sicherzustellen, dass Sie das korrekte Format für die Namen des Dienstprinzipals und der Keytab-Dateien berücksichtigen, verwenden Sie den Informatica-Kerberos-SPN-Formatgenerator für die Generierung einer Liste von Dienstprinzipal- und Keytab-Dateinamen im von der Informatica-Domäne geforderten Format.

Der Kerberos SPN-Formatgenerator von Informatica ist im Lieferumfang des Installationsprogramms für die Informatica-Dienste enthalten.

Dienstprinzipalanforderungen auf der Knotenebene

Wenn die Informatica-Domäne keine hohe Sicherheitsstufe erfordert, können die Knoten- und Dienstprozesse gemeinsam dieselben SPNs und Keytab-Dateien nutzen. Die Domäne erfordert keinen separaten SPN für jeden Dienstprozess in einem Knoten.

Die Informatica-Domäne erfordert SPNs und Keytab-Dateien für die folgenden Komponenten auf der Knotenebene:

Prinzipal-DN (Distinguished Name) für den LDAP-Verzeichnisdienst

Prinzipalname für den Benutzer-DN der Bindung, der zur Suche des LDAP-Verzeichnisdienstes verwendet wird. Der Name der Keytab-Datei muss `infa_ldapuser.keytab` lauten.

Knotenprozess

Prinzipalname für den Informatica-Knoten, der Authentifizierungsaufrufe initiiert oder annimmt. Derselbe Prinzipalname wird für die Authentifizierung der Dienste in dem Knoten verwendet. Jeder Gateway-Knoten in der Domäne erfordert einen eigenen Prinzipalnamen.

HTTP-Prozesse in der Domäne

Prinzipalname für alle Webanwendungsdienste in der Informatica-Domäne, einschließlich Informatica Administrator. Der Browser verwendet diesen Prinzipalnamen für die Authentifizierung mit allen HTTP-Prozessen in der Domäne. Der Name der Keytab-Datei muss `webapp_http.keytab` lauten.

Dienstprinzipalanforderungen auf Prozessebene

Wenn die Informatica-Domäne einen hohen Grad an Sicherheit erfordert, erstellen Sie eine separate SPN- und Keytab-Datei für jeden Knoten und jeden Anwendungsdienst in dem Knoten.

Die Informatica-Domäne erfordert SPNs und Keytab-Dateien für die folgenden Komponenten auf der Prozessebene:

Prinzipal-DN (Distinguished Name) für den LDAP-Verzeichnisdienst

Prinzipalname für den Benutzer-DN der Bindung, der zur Suche des LDAP-Verzeichnisdienstes verwendet wird. Der Name der Keytab-Datei muss `infa_ldapuser.keytab` lauten.

Knotenprozess

Prinzipalname für den Informatica-Knoten, der die Authentifizierung initiiert oder akzeptiert.

Informatica Administrator-Dienst

Prinzipalname für den Informatica Administrator-Dienst, der den Dienst mit anderen Diensten in der Informatica-Domäne authentifiziert. Der Name der Keytab-Datei muss *_AdminConsole.keytab* lauten.

HTTP-Prozesse in der Domäne

Prinzipalname für alle Webanwendungsdienste in der Informatica-Domäne, einschließlich Informatica Administrator. Der Browser verwendet diesen Prinzipalnamen für die Authentifizierung mit allen HTTP-Prozessen in der Domäne. Der Name der Keytab-Datei muss `webapp_http.keytab` lauten.

Dienstprozess

Prinzipalname für den Dienst, der auf einem Knoten in der Informatica-Domäne ausgeführt wird. Jeder Dienst erfordert einen eindeutigen Dienstprinzipal- und Keytab-Datei-Namen.

Sie brauchen die SPNs und Keytab-Dateien für die Dienste nicht vor dem Ausführen des Installationsprogramms zu erstellen. Sie können den SPN und die Keytab-Datei für einen Dienst beim Erstellen des Diensts in der Domäne erstellen. Der SPN und die Keytab-Datei für einen Dienst müssen verfügbar sein, wenn Sie den Dienst aktivieren.

Ausführen des Kerberos SPN-Formatgenerators von Informatica unter Windows

Sie können den Kerberos SPN-Formatgenerator von Informatica zum Generieren einer Datei verwenden, die das korrekte Format für die in der Informatica-Domäne erforderlichen Namen der SPNs und Keytab-Dateien anzeigt.

Sie können den SPN-Formatgenerator von der Befehlszeile oder über das Informatica-Installationsprogramm ausführen. Der SPN-Formatgenerator generiert eine Datei mit dem Namen der Dienstprinzipal- und Keytab-Dateien basierend auf den von Ihnen eingegebenen Parametern.

Hinweis: Stellen Sie sicher, dass die von Ihnen eingegebenen Informationen korrekt sind. Der SPN-Formatgenerator validiert nicht die von Ihnen eingegebenen Werte.

Zum Ausführen des SPN-Formatgenerators führen Sie folgende Schritte aus:

1. Melden Sie sich mit einem Systembenutzerkonto am Computer an.
2. Schließen Sie alle anderen Anwendungen.
3. Gehen Sie auf dem Computer, auf dem Sie die Installationsdateien entpackt haben, zu folgendem Verzeichnis: `<Informatica installation files directory>/Server/Kerberos`
4. Führen Sie die Datei SPNFormatGenerator.bat aus.

   Die **Begrüßungsseite** des Kerberos SPN-Formatgenerators von Informatica wird geöffnet.
5. Klicken Sie auf **Weiter**.

   Die Seite **Dienstprinzipalebene** wird angezeigt.
6. Wählen Sie die Ebene aus, auf die die Kerberos-Dienstprinzipale für die Domäne festgelegt werden.

   In der folgenden Tabelle werden die Ebenen beschrieben, die Sie festlegen können:

Ebene	Beschreibung
Prozessebene	Konfiguriert die Domäne für die Verwendung eines eindeutigen SPN und einer Keytab-Datei für jeden Knoten und jeden Anwendungsdienst auf einem Knoten. Die Anzahl der pro Knoten erforderlichen SPNs und Keytab-Dateien hängt von der Anzahl der Anwendungsdienstprozesse ab, die auf dem Knoten ausgeführt werden. Verwenden Sie die Prozessebenenoption für Datendomänen, die einen hohen Grad an Sicherheit erfordern, wie z. B. Produktionsdomänen.
Knotenebene	Konfiguriert die Domäne zur gemeinsamen Nutzung von SPNs und Keytab-Dateien auf einem Knoten. Diese Option erfordert jeweils einen SPN und eine Keytab-Datei für den Knoten und alle Anwendungsdienste, die auf dem Knoten ausgeführt werden. Sie erfordert außerdem einen separaten SPN und eine separate Keytab-Datei für alle HTTP-Prozesse auf dem Knoten. Verwenden Sie die Knotenebenenoption für Domänen, die keinen hohen Grad an Sicherheit erfordern, wie z. B. Test- und Entwicklungsdomänen.

7. Klicken Sie auf **Weiter**.

   Die Seite **Authentifizierungsparameter – Kerberos-Authentifizierung** wird angezeigt.
8. Geben Sie die Domänen- und Knotenparameter zum Generieren des SPN-Formats ein.

Die folgende Tabelle beschreibt die Parameter, die Sie angeben müssen:

Eingabeaufforderung	Beschreibung
Domänenname	Name der Domäne. Der Name darf nicht länger als 128 Zeichen sein und muss im 7-Bit-ASCII-Format vorliegen. Er darf weder Leerzeichen noch die folgenden Zeichen enthalten: ` % * + ; " ? , < > \ /
Knotenname	Name des Informatica-Knotens
Knoten-Hostname	Vollständig qualifizierter Hostname oder die IP-Adresse des Computers, auf dem der Knoten erstellt werden soll. Der Hostname für den Knoten darf keinen Unterstrich (_) enthalten. **Hinweis:** Verwenden Sie nicht *localhost*. Der Hostname muss den Computer eindeutig kennzeichnen.
Dienstbereichsname	Name des Kerberos-Bereichs für die Informatica-Domänendienste. Der Bereichsname muss aus Großbuchstaben bestehen.

Wenn Sie den Dienstprinzipal auf die Knotenebene festlegen, zeigt das Dienstprogramm die Schaltfläche **+Knoten** an. Wenn Sie den Dienstprinzipal auf die Prozessebene festlegen, zeigt das Dienstprogramm die Schaltflächen **+Knoten** und **+Dienst** an.

9. Zum Generieren des SPN-Formats für einen zusätzlichen Knoten klicken Sie auf **+Knoten**, und geben Sie den Knotennamen und Hostnamen an.

   Sie können mehrere Knoten für eine Domäne eingeben.

10. Zum Generieren des SPN-Formats für einen Dienst klicken Sie auf **+Dienst**, und geben Sie den Dienstnamen im Feld **Dienst auf Knoten** ein.

    Das Feld **Dienst auf Knoten** wird nur angezeigt, wenn Sie den Dienstprinzipal auf Prozessebene festlegen und auf **+Dienst** klicken. Sie können mehrere Dienste für einen Knoten eingeben. Die Dienste werden direkt unterhalb des Knotens angezeigt, auf dem sie ausgeführt werden.

11. Klicken Sie zum Entfernen eines Knotens aus der Liste auf **-Knoten**.

    Der SPN-Formatgenerator von Informatica löscht den Knoten. Wenn Sie Dienste zu dem Knoten hinzugefügt haben, werden die Dienste mit dem Knoten gelöscht.

12. Zum Entfernen eines Diensts aus einem Knoten löschen Sie das Feld für den Dienstnamen.

13. Klicken Sie auf **Weiter**.

    Der SPN-Formatgenerator zeigt den Pfad und Namen der Datei an, die die Liste der Namen für die Dienstprinzipale und Keytab-Dateien enthält.

14. Klicken Sie auf **Fertig**, um den SPN-Formatgenerator zu beenden.

Der SPN-Formatgenerator generiert eine Textdatei, die die Namen des SPN und der Keytab-Dateien in dem für die Informatica-Domäne erforderlichen Format enthält.

Ausführen des Kerberos SPN-Formatgenerators von Informatica unter UNIX

Sie können den Kerberos SPN-Formatgenerator von Informatica zum Generieren einer Datei verwenden, die das korrekte Format für die in der Informatica-Domäne erforderlichen Namen der SPNs und Keytab-Dateien anzeigt.

Sie können den SPN-Formatgenerator von der Befehlszeile oder über das Informatica-Installationsprogramm ausführen. Der SPN-Formatgenerator generiert eine Datei mit dem Namen der Dienstprinzipal- und Keytab-Dateien basierend auf den von Ihnen eingegebenen Parametern.

Hinweis: Stellen Sie sicher, dass die von Ihnen eingegebenen Informationen korrekt sind. Der SPN-Formatgenerator validiert nicht die von Ihnen eingegebenen Werte.

1. Gehen Sie auf dem Computer, auf dem Sie die Installationsdateien entpackt haben, zu folgendem Verzeichnis: `<Informatica installation files directory>/Server/Kerberos`
2. Führen Sie in einer Shell-Befehlszeile die Datei SPNFormatGenerator.sh aus.
3. Drücken Sie zur Fortsetzung die **Eingabetaste**.
4. Wählen Sie im Abschnitt **Dienstprinzipalebene** die Ebene aus, auf die Sie die Kerberos-Dienstprinzipale für die Domäne festlegen möchten.

   In der folgenden Tabelle werden die Ebenen beschrieben, die Sie festlegen können:

Ebene	Beschreibung
Prozessebene	Konfiguriert die Domäne für die Verwendung eines eindeutigen SPN und einer Keytab-Datei für jeden Knoten und jeden Anwendungsdienst auf einem Knoten. Die Anzahl der pro Knoten erforderlichen SPNs und Keytab-Dateien hängt von der Anzahl der Anwendungsdienstprozesse ab, die auf dem Knoten ausgeführt werden. Verwenden Sie die Prozessebenenoption für Datendomänen, die einen hohen Grad an Sicherheit erfordern, wie z. B. Produktionsdomänen.
Knotenebene	Konfiguriert die Domäne zur gemeinsamen Nutzung von SPNs und Keytab-Dateien auf einem Knoten. Diese Option erfordert jeweils einen SPN und eine Keytab-Datei für den Knoten und alle Anwendungsdienste, die auf dem Knoten ausgeführt werden. Sie erfordert außerdem einen separaten SPN und eine separate Keytab-Datei für alle HTTP-Prozesse auf dem Knoten. Verwenden Sie die Knotenebenenoption für Domänen, die keinen hohen Grad an Sicherheit erfordern, wie z. B. Test- und Entwicklungsdomänen.

5. Geben Sie die Domänen- und Knotenparameter zum Generieren des SPN-Formats ein.

   Die folgende Tabelle beschreibt die Parameter, die Sie angeben müssen:

Eingabeaufforderung	Beschreibung
Domänenname	Name der Domäne. Der Name darf nicht länger als 128 Zeichen sein und muss im 7-Bit-ASCII-Format vorliegen. Er darf weder Leerzeichen noch die folgenden Zeichen enthalten: ` % * + ; " ? , < > \ /
Knotenname	Name des Informatica-Knotens

Eingabeaufforderung	Beschreibung
Knoten-Hostname	Vollständig qualifizierter Hostname oder die IP-Adresse des Computers, auf dem der Knoten erstellt werden soll. Der Hostname für den Knoten darf keinen Unterstrich (_) enthalten. **Hinweis:** Verwenden Sie nicht *localhost*. Der Hostname muss den Computer eindeutig kennzeichnen.
Dienstbereichsname	Name des Kerberos-Bereichs für die Informatica-Domänendienste. Der Bereichsname muss aus Großbuchstaben bestehen.

Wenn Sie den Dienstprinzipal auf die Knotenebene festlegen, wird die Eingabeaufforderung **Knoten hinzufügen?** angezeigt. Wenn Sie den Dienstprinzipal auf die Prozessebene festlegen, wird die Eingabeaufforderung**Dienst hinzufügen?** angezeigt.

6. Geben Sie in der Eingabeaufforderung **Knoten hinzufügen?** „1“ zum Generieren des SPN-Formats für einen zusätzlichen Knoten ein. Geben Sie dann den Knotennamen und Hostnamen des Knotens ein.

   Zum Generieren der SPN-Formate für mehrere Knoten geben Sie „1“ in jeder Eingabeaufforderung **Knoten hinzufügen?** ein, und geben Sie einen Knotennamen und Hostnamen des Knotens ein.
7. Geben Sie in der Eingabeaufforderung **Dienst hinzufügen?** „1“ zum Generieren des SPN-Formats für einen Dienst ein, der auf dem vorigen Knoten ausgeführt wird. Geben Sie dann den Dienstnamen ein.

   Zum Generieren der SPN-Formate für mehrere Dienste geben Sie „1“ in jeder Eingabeaufforderung **Dienst hinzufügen?** ein, und geben Sie dann einen Dienstnamen ein.
8. Geben Sie „2“ zum Beenden der Eingabeaufforderung **Dienst hinzufügen?** oder **Knoten hinzufügen?** ein.

   Der SPN-Formatgenerator zeigt den Pfad und Namen der Datei an, die die Liste der Namen für die Dienstprinzipale und Keytab-Dateien enthält.
9. Drücken Sie zum Beenden des SPN-Formatgenerators die Eingabetaste.

Der SPN-Formatgenerator generiert eine Textdatei, die die Namen des SPN und der Keytab-Dateien in dem für die Informatica-Domäne erforderlichen Format enthält.

Überprüfen der SPN- und Keytab-Format-Textdatei

Der Kerberos SPN-Formatgenerator generiert eine Textdatei mit dem Namen SPNKeytabFormat.txt, die das von der Informatica-Domäne benötigte Format für die Namen der Dienstprinzipale und Keytab-Dateien auflistet. Die Liste enthält die SPN- und Keytab-Datei-Namen basierend auf der ausgewählten Dienstprinzipalebene.

Überprüfen Sie die Textdatei und stellen Sie sicher, dass keine Fehlermeldungen enthalten sind.

Die Textdatei enthält die folgenden Informationen:

Entitätsname

Identifiziert den Knoten oder Dienst, der mit dem Prozess verknüpft ist.

SPN

Format für den SPN in der Kerberos-Prinzipaldatenbank. Beim SPN wird die Groß- und Kleinschreibung beachtet. Jeder SPN-Typ hat ein anderes Format.

Ein SPN kann eines der folgenden Formate aufweisen:

Schlüsseltabellentyp	SPN-Format
NODE_SPN	isp/<*NodeName*>/<*DomainName*>@<*REALMNAME*>
NODE_AC_SPN	_AdminConsole/<*NodeName*>/<*DomainName*>@<*REALMNAME*>
NODE_HTTP_SPN	HTTP/<*NodeHostName*>@<*REALMNAME*> **Hinweis:** Der Kerberos SPN-Formatgenerator validiert den Knoten-Hostnamen. Wenn der Knoten-Hostname nicht gültig ist, generiert das Dienstprogramm keinen SPN. Stattdessen zeigt es die folgende Meldung an: Fehler beim Auflösen des Hostnamens.
SERVICE_PROCESS_SPN	<*ServiceName*>/<*NodeName*>/<*DomainName*>@<*REALMNAME*>

Keytab-Dateiname

Format für den Namen der Keytab-Datei, die für den zugehörigen SPN in der Kerberos-Prinzipaldatenbank erstellt werden soll. Beim Keytab-Dateinamen ist die Groß- und Kleinschreibung zu berücksichtigen.

Die Keytab-Dateinamen verwenden die folgenden Formate:

Schlüsseltabellentyp	Keytab-Dateiname
NODE_SPN	<*NodeName*>.keytab
NODE_AC_SPN	_AdminConsole.keytab
NODE_HTTP_SPN	webapp_http.keytab
SERVICE_PROCESS_SPN	<*ServiceName*>.keytab

Schlüsseltabellentyp

Der Typ der Schlüsseltabelle. Folgende Schlüsseltabellentypen sind möglich:

- NODE_SPN. Die Keytab-Datei für einen Knotenprozess.
- NODE_AC_SPN. Die Keytab-Datei für den Informatica Administrator-Dienstprozess.
- NODE_HTTP_SPN. Die Keytab-Datei für HTTP-Prozesse in einem Knoten.
- SERVICE_PROCESS_SPN. Die Keytab-Datei für einen Dienstprozess.

Dienstprinzipale auf der Knotenebene

Das folgende Beispiel zeigt den Inhalt der Datei SPNKeytabFormat.txt, die für Dienstprinzipale auf der Knotenebene generiert wurde:

```
ENTITY_NAME   SPN                                                KEY_TAB_NAME
KEY_TAB_TYPE
Node01        isp/Node01/InfaDomain@MY.SVCREALM.COM              Node01.keytab
NODE_SPN
Node01        HTTP/NodeHost01.enterprise.com@MY.SVCREALM.COM     webapp_http.keytab
NODE_HTTP_SPN
Node02        isp/Node02/InfaDomain@MY.SVCREALM.COM              Node02.keytab
NODE_SPN
Node02        HTTP/NodeHost02.enterprise.com@MY.SVCREALM.COM     webapp_http.keytab
NODE_HTTP_SPN
Node03        isp/Node03/InfaDomain@MY.SVCREALM.COM              Node03.keytab
```

```
NODE_SPN
Node03        HTTP/NodeHost03.enterprise.com@MY.SVCREALM.COM     webapp_http.keytab
NODE_HTTP_SPN
```

Dienstprinzipale auf der Prozessebene

Das folgende Beispiel zeigt den Inhalt der Datei SPNKeytabFormat.txt, die für Dienstprinzipale auf der Prozessebene generiert wurde:

```
ENTITY_NAME        SPN
KEY_TAB_NAME           KEY_TAB_TYPE
Node01             isp/Node01/InfaDomain@MY.SVCREALM.COM
Node01.keytab          NODE_SPN
Node01             _AdminConsole/Node01/InfaDomain@MY.SVCREALM.COM
_AdminConsole.keytab   NODE_AC_SPN
Node01             HTTP/NodeHost01.enterprise.com@MY.SVCREALM.COM
webapp_http.keytab     NODE_HTTP_SPN
Node02             isp/Node02/InfaDomain@MY.SVCREALM.COM
Node02.keytab          NODE_SPN
Node02             _AdminConsole/Node02/InfaDomain@MY.SVCREALM.COM
_AdminConsole.keytab   NODE_AC_SPN
Node02             HTTP/NodeHost02.enterprise.com@MY.SVCREALM.COM
webapp_http.keytab     NODE_HTTP_SPN
Service10:Node01   Service10/Node01/InfaDomain@MY.SVCREALM.COM
Service10.keytab       SERVICE_PROCESS_SPN
Service100:Node02  Service100/Node02/InfaDomain@MY.SVCREALM.COM
Service100.keytab      SERVICE_PROCESS_SPN
Service200:Node02  Service200/Node02/InfaDomain@MY.SVCREALM.COM
Service200.keytab      SERVICE_PROCESS_SPN
```

Erstellen der Dienstprinzipalnamen und Keytab-Dateien

Senden Sie nach dem Generieren der Liste der SPN- und Keytab-Datei-Namen im Informatica-Format eine Anfrage an den Kerberos-Administrator, um die SPNs zur Kerberos-Prinzipaldatenbank hinzuzufügen und Keytab-Dateien zu erstellen.

Verwenden Sie die folgenden Richtlinien, wenn Sie den SPN und die Keytab-Dateien erstellen:

Der Benutzerprinzipalname (UPN, User Prinicipal Name) muss identisch sein mit dem SPN.

Wenn Sie ein Benutzerkonto für den Dienstprinzipal erstellen, müssen Sie den UPN auf den gleichen Namen festlegen wie den SPN. Die Anwendungsdienste in der Informatica-Domäne können je nach Vorgang als Dienst oder Client agieren. Sie müssen den Dienstprinzipal so konfigurieren, dass er durch den gleichen UPN und SPN identifiziert werden kann.

Ein Benutzerkonto darf nur einem SPN zugeordnet sein. Legen Sie nicht mehrere SPNs für ein Benutzerkonto fest.

Aktivieren Sie die Delegierung in Microsoft Active Directory.

Sie müssen die Delegierung für alle Benutzerkonten mit Dienstprinzipalen aktivieren, die in der Informatica-Domäne verwendet werden. Legen Sie im Microsoft Active Directory Service die Option **Diesem Benutzer für die Delegierung eines Dienstes (nur Kerberos) vertrauen** für jedes Benutzerkonto fest, für das Sie einen SPN festlegen.

Delegierte Authentifizierung tritt ein, wenn ein Benutzer mit einem Dienst authentifiziert wird und dieser Dienst die Anmeldedaten des authentifizierten Benutzers zum Herstellen einer Verbindung zu einem anderen Dienst verwendet. Da Dienste in der Informatica-Domäne eine Verbindung zu anderen Diensten

herstellen müssen, um einen Vorgang abzuschließen, muss für die Informatica-Domäne die Delegierungsoption in Microsoft Active Directory aktiviert sein.

Wenn beispielsweise ein PowerCenter Client eine Verbindung zum PowerCenter-Repository-Dienst herstellt, so wird das Client-Benutzerkonto mit dem PowerCenter-Repository-Dienst-Prinzipal authentifiziert. Wenn der PowerCenter-Repository-Dienst eine Verbindung zum PowerCenter-Integrationsdienst herstellt, kann der PowerCenter Repository-Dienst-Prinzipal die Benutzerzugangsdaten für die Authentifizierung mit dem PowerCenter-Integrationsdienst verwenden. Eine zusätzliche Authentifizierung des Client-Benutzerkontos mit dem PowerCenter-Integrationsdienst ist nicht erforderlich.

Verwenden Sie das ktpass-Dienstprogramm zum Erstellen der Dienstprinzipal-Keytab-Dateien.

Microsoft Active Directory stellt das ktpass-Dienstprogramm zum Erstellen von Keytab-Dateien zur Verfügung. Informatica unterstützt die Kerberos-Authentifizierung nur auf Microsoft Active Directory und zertifiziert ausschließlich Keytab-Dateien, die mit dem ktpass-Dienstprogramm erstellt werden.

Die Keytab-Dateien für einen Knoten müssen auf dem Rechner verfügbar sein, auf dem sich der Knoten befindet. Standardmäßig werden Keytab-Dateien im folgenden Verzeichnis gespeichert: `<Informatica-Installationsverzeichnis>/isp/config/keys`. Während der Installation können Sie ein Verzeichnis auf dem Knoten zum Speichern der Keytab-Dateien angeben.

Wenn Sie die Keytab-Dateien von dem Kerberos-Administrator erhalten, kopieren Sie sie in ein Verzeichnis, das für den Computer zugänglich ist, auf dem die Informatica-Dienste installiert werden sollen. Geben Sie beim Ausführen des Informatica-Installationsprogramms den Speicherort der Keytab-Dateien an. Das Informatica-Installationsprogramm kopiert die Keytab-Dateien in das Verzeichnis für Keytab-Dateien auf dem Informatica-Knoten.

Fehlerbehebung bei den Dienstprinzipalnamen und Keytab-Dateien

Mit Kerberos-Dienstprogrammen können Sie überprüfen, ob die vom Kerberos-Administrator erstellten Dienstprinzipal- und Keytab-Dateinamen mit den von Ihnen angeforderten Dienstprinzipal- und Keytab-Dateienamen übereinstimmen. Mit den Dienstprogrammen können Sie außerdem den Status des Kerberos-Schlüsselverteilungscenters (KDC) ermitteln.

Mit Kerberos-Dienstprogrammen wie *setspn*, *kinit* und *klist* können Sie die SPNs und Keytab-Dateien anzeigen und überprüfen. Stellen Sie zum Verwenden der Dienstprogramme sicher, dass die Umgebungsvariable KRB5_CONFIG den Pfad und den Dateinamen der Kerberos-Konfigurationsdatei enthält.

Hinweis: Die folgenden Beispiele zeigen Möglichkeiten, wie Sie mit den Kerberos-Dienstprogrammen die Gültigkeit der SPNs und Keytab-Dateien überprüfen können. Die Beispiele könnten von der Art und Weise abweichen, in der der Kerberos-Administrator die Dienstprogramme zum Erstellen der für die Informatica-Domäne erforderlichen SPNs und Keytab-Dateien verwendet. Weitere Informationen über die Ausführung der Kerberos-Dienstprogramme finden Sie in der Kerberos-Dokumentation.

Verwenden Sie die folgenden Dienstprogramme zum Überprüfen der SPNs und Keytab-Dateien:

klist

Mit *klist* können Sie die Kerberos-Prinzipale und Schlüssel in einer Keytab-Datei auflisten. Führen Sie zum Auflisten der Schlüssel in der Keytab-Datei und des Zeitstempels für den Keytab-Eintrag den folgenden Befehl aus:

```
klist -k -t <keytab_file>
```

Das folgende Ausgabebeispiel zeigt die Prinzipale in einer Keytab-Datei:

```
Keytab name: FILE:int_srvc01.keytab
KVNO Timestamp         Principal
---- ----------------- -------------------------------------------------------
   3 12/31/69 19:00:00 int_srvc01/node01_vMPE/Domn96_vMPE@REALM
```

```
   3 12/31/69 19:00:00 int_srvc01/node01_vMPE/Domn96_vMPE@REALM
   3 12/31/69 19:00:00 int_srvc01/node01_vMPE/Domn96_vMPE@REALM
   3 12/31/69 19:00:00 int_srvc01/node01_vMPE/Domn96_vMPE@REALM
   3 12/31/69 19:00:00 int_srvc01/node01_vMPE/Domn96_vMPE@REALM
```

kinit

Mit *kinit* können Sie ein TGT (Ticket-Granting-Ticket) für ein Benutzerkonto anfordern, um zu überprüfen, ob der KDC ausgeführt wird und Tickets gewähren kann. Führen Sie zum Anfordern eines Ticket-Granting-Ticket für ein Benutzerkonto den folgenden Befehl aus:

```
kinit <user_account>
```

Sie können auch mit *kinit* ein Ticket-Granting-Ticket anfordern und überprüfen, ob mithilfe der Keytab-Datei eine Kerberos-Verbindung hergestellt werden kann. Führen Sie zum Anfordern eines Ticket-Granting-Tickets für einen SPN den folgenden Befehl aus:

```
kinit -V -k -t <keytab_file> <SPN>
```

Das folgende Ausgabebeispiel zeigt das Ticket-Granting-Ticket, das im Standard-Cache für eine angegebene Keytab-Datei und einen SPN erstellt wurde:

```
Using default cache: /tmp/krb5cc_10000073
Using principal: int_srvc01/node01_vMPE/Domn96_vMPE@REALM
Using keytab: int_srvc01.keytab
Authenticated to Kerberos v5
```

setspn

Mit *setspn* können Sie den SPN für ein Active Directory-Dienstkonto anzeigen, ändern oder löschen. Öffnen Sie auf dem Rechner, auf dem sich der Active Directory-Dienst befindet, ein Befehlszeilenfenster und führen Sie den Befehl aus.

Führen Sie zum Anzeigen der SPNs, die einem Benutzerkonto zugeordnet sind, den folgenden Befehl an:

```
setspn -L <user_account>
```

Das folgende Ausgabebeispiel zeigt den SPN, der dem Benutzerkonto `is96svc` zugeordnet ist:

```
Registered ServicePrincipalNames for CN=is96svc,OU=AllSvcAccts,OU=People,
DC=ds,DC=intrac0rp,DC=zec0rp:
       int_srvc01/node02_vMPE/Domn96_vMPE
```

Führen Sie zum Anzeigen der Benutzerkonten, die einem SPN zugeordnet sind, den folgenden Befehl aus:

```
setspn -Q <SPN>
```

Die folgende Ausgabebeispiel zeigt das Benutzerkonto, das dem SPN `int_srvc01/node02_vMPE/Domn96_vMPE` zugeordnet ist:

```
Checking domain DC=ds,DC=intrac0rp,DC=zec0rp
CN=is96svc,OU=AllSvcAccts,OU=People,DC=ds,DC=intrac0rp,DC=zec0rp
        int_srvc01/node02_vMPE/Domn96_vMPE

Existing SPN found!
```

Führen Sie für die Suche nach duplizierten SPNs den folgenden Befehl aus:

```
setspn -X
```

Das folgende Ausgabebeispiel zeigt mehrere Benutzerkonten, die einem SPN zugeordnet sind:

```
Checking domain DC=ds,DC=intrac0rp,DC=zec0rp
Processing entry 1125
HOST/mtb01.REALM is registered on these accounts:
        CN=Team1svc,OU=AllSvcAccts,OU=People,DC=ds,DC=intrac0rp,DC=zec0rp
        CN=MTB1svc,OU=IIS,OU=WPC960K3,OU=WINServers,DC=ds,DC=intrac0rp,DC=zec0rp
```

Hinweis: Die Suche nach duplizierten SPNs kann recht viel Zeit und Arbeitsspeicherkapazität in Anspruch nehmen.

kdestroy

Mit *kdestroy* können Sie die aktiven Kerberos-Autorisierungstickets und den Cache für Benutzeranmeldedaten löschen, der diese Tickets enthält. Wenn Sie *kdestroy* ohne Parameter ausführen, löschen Sie den Standardcache für Anmeldedaten.

KAPITEL 5

Vor der Installation der Dienste unter Windows

Dieses Kapitel umfasst die folgenden Themen:

- Vor der Installation der Dienste unter Windows - Übersicht, 86
- Lesen der Versionshinweise, 86
- Überprüfen Sie die Patch Anforderungen, 87
- Data Transformation-Dateien sichern, 87
- Überprüfen der Umgebungsvariablen, 87
- Erstellen eines Systembenutzerkontos, 88
- Einrichten von Schlüsselspeicher- und Truststore-Dateien, 88
- Extrahieren der Dateien des Installationsprogramms, 90
- Überprüfen Sie den Lizenzschlüssel, 91
- Ausführen des Vorinstallations-Systemprüfungstools (i10Pi), 91

Vor der Installation der Dienste unter Windows - Übersicht

Bevor Sie die Informatica-Dienste installieren, richten Sie den Computer so ein, dass er die Anforderungen für das Installieren und Ausführen der Informatica-Plattform erfüllt. Wenn der Computer, auf dem Sie die Informatica-Dienste installieren möchten, nicht ordnungsgemäß konfiguriert ist, kann die Installation fehlschlagen.

Lesen der Versionshinweise

Lesen Sie die Versionshinweise, um mehr über Aktualisierungen der Installation und den Upgradeprozess zu erfahren. Außerdem können Sie Informationen über bekannte und behobene Einschränkungen für die Version finden.

Überprüfen Sie die Patch Anforderungen

Bevor Sie die Informatica-Dienste installieren, stellen Sie sicher, dass der Computer über die erforderlichen Betriebssystem-Patches und -Bibliotheken verfügt.

In der folgenden Tabelle finden Sie eine Auflistung der Patches und Bibliotheken, die die Informatica-Dienste auf einer Windows-Plattform benötigen:

Plattform	Betriebssystem	Betriebssystem-Patch
Windows x64	2012 R2 64 Bit	Nicht erforderlich
Windows x64	2008 R2 64 Bit	Nicht erforderlich

Data Transformation-Dateien sichern

Vor der Installation müssen Sie die unter früheren Versionen erstellten Data Transformation-Dateien sichern. Kopieren Sie nach Abschluss der Installation die Dateien in die neuen Installationsverzeichnisse, damit Repository und benutzerdefinierte globale Komponenten die gleichen sind wie in der vorherigen Version.

In der folgenden Tabelle sind die Dateien und Verzeichnisse aufgeführt, die gesichert werden müssen:

Datei oder Verzeichnis	Standardspeicherort
Repository	<Informatica-Installationsverzeichnis>\DataTransformation\ServiceDB
Custom Global Components-Verzeichnis (TGP-Dateien)	<Informatica-Installationsverzeichnis>\DataTransformation\autoInclude\user
Custom Global Components-Verzeichnis (DLL- und JAR-Dateien)	<Informatica-Installationsverzeichnis>\DataTransformation\externLibs\user
Konfigurationsdatei	<Informatica-Installationsverzeichnis>\DataTransformation\CMConfig.xml
Lizenzdatei	<Informatica-Installationsverzeichnis>\DataTransformation\CDELicense.cfg

Kopieren Sie die Data Transformation-Bibliotheksdateien nicht. Installieren Sie stattdessen die Data Transformation-Bibliotheken erneut.

Überprüfen der Umgebungsvariablen

Konfigurieren Sie die Umgebungsvariablen so, dass sie mit der Installation von Informatica funktionieren.

In der nachstehenden Tabellen sind die unter Windows zu überprüfenden Umgebungsvariablen aufgeführt:

Variable	Beschreibung
%TEMP%	Der Speicherort der während der Installation erstellten temporären Dateien. Informatica benötigt 1 GB Speicherplatz auf der Festplatte für temporäre Dateien. Konfigurieren Sie die Umgebungsvariable, wenn auf dem Standardlaufwerk keine temporären Dateien erstellt werden sollen.
PATH	Das Installationsprogramm hängt von Informatica benötigte Dateipfade an die Umgebungsvariable PATH an. Stellen Sie sicher, dass die Länge der Umgebungsvariable PATH nicht die Systemobergrenze überschreitet.

Erstellen eines Systembenutzerkontos

Erstellen Sie ein Systembenutzerkonto, um die Installation durchzuführen und den Informatica-Dienst auszuführen. Vergewissern Sie sich, dass das Benutzerkonto, das Sie zum Installieren der Informatica-Dienste verwenden, über Schreibberechtigung für das Installationsverzeichnis verfügt.

Sie können Informatica mit dem Benutzerkonto installieren, mit dem Sie beim Rechner angemeldet sind, und es später unter einem anderen Benutzerkonto ausführen. Sie können ein lokales Konto oder ein Domänenkonto erstellen, um Informatica zu installieren oder den Informatica-Windows-Dienst auszuführen.

Hinweis: Für den Zugriff auf ein Repository in Microsoft SQL Server, das eine vertrauenswürdige Windows-Verbindung verwendet, erstellen Sie ein Domänenkonto.

Die Benutzerkonten benötigen die folgenden Berechtigungen zum Ausführen des Installationsprogramms oder des Informatica-Windows-Dienstes:

- **Ein angemeldetes Benutzerkonto** Das Benutzerkonto muss Mitglied der Administratorengruppe sein und über die Berechtigung *Als Dienst anmelden* verfügen. Melden Sie sich vor dem Installieren von Informatica mit diesem Benutzerkonto an.
- **Ein anderes Benutzerkonto** Das Benutzerkonto muss Mitglied der Administratorengruppe sein und über die Berechtigungen "Als Dienst anmelden" und "Als Betriebssystem fungieren" verfügen. Vor dem Installieren von Informatica brauchen Sie sich mit diesem Benutzerkonto nicht anzumelden. Während der Installation können Sie das Benutzerkonto angeben, über das der Informatica-Windows-Dienst ausgeführt werden soll.

Einrichten von Schlüsselspeicher- und Truststore-Dateien

Wenn Sie die Informatica-Dienste installieren, können Sie die sichere Kommunikation für die Domäne konfigurieren und eine sichere Verbindung zu Informatica Administrator einrichten. Wenn Sie diese Sicherheitsoptionen konfigurieren, müssen Sie Schlüsselspeicher- und Truststore-Dateien einrichten.

Bevor Sie die Informatica-Dienste installieren, richten Sie die Dateien für die sichere Kommunikation innerhalb der Informatica-Domäne oder für eine sichere Verbindung zum Administrator Tool ein. Sie können die folgenden Programme verwenden, um die erforderlichen Dateien zu erstellen:

Keytool

Sie können Keytool zum Erstellen eines SSL-Zertifikats oder eines CSR (Certificate Signing Request) sowie als Schlüsselspeicherdateien und Truststore-Dateien im JKS-Format verwenden.

Weitere Informationen zur Verwendung von Keytool finden Sie in der Dokumentation auf der folgenden Website: http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html

OpenSSL

Sie können OpenSSL verwenden, um ein SSL-Zertifikat oder eine Zertifikatssignieranfrage zu erstellen und einen Schlüsselspeicher im JKS-Format in das PEM-Format zu konvertieren.

Weitere Informationen zu OpenSSL finden Sie in der Dokumentation auf der folgenden Website: https://www.openssl.org/docs/

Damit Sie eine höhere Sicherheitsebene erzielen, senden Sie Ihr CSR an eine Zertifizierungsstelle, um ein signiertes Zertifikat zu erhalten.

Die über die angegebenen Links zum Download verfügbare Software wird nicht von Informatica LLC angeboten, sondern ist Eigentum eines oder mehrerer Drittanbieter. Eventuelle Fehler oder Änderungen bei den Download-Links können nicht ausgeschlossen werden. Informatica übernimmt keinerlei Verantwortung für diese Links und/oder Software, lehnt jegliche ausdrückliche oder stillschweigende Garantien ab, einschließlich jedweder stillschweigenden Garantien in Bezug auf Handelsüblichkeit, Eignung zu einem bestimmten Zweck, Eigentumsrechte und Nichtverletzung von Rechten Dritter, und schließt jedwede damit verbundene Haftungsansprüche aus.

Sichere Kommunikation innerhalb der Informatica-Domäne

Bevor Sie die sichere Kommunikation innerhalb der Informatica-Domäne aktivieren, überprüfen Sie, ob die folgenden Anforderungen erfüllt sind:

Sie haben eine Zertifikatssignieranfrage und einen privaten Schlüssel erstellt.

Sie können keytool oder OpenSSL zum Erstellen der Zertifikatssignieranfrage und des privaten Schlüssels verwenden.

Bei Verwendung von RSA-Verschlüsselung müssen Sie mehr als 512 Bit verwenden.

Sie haben ein signiertes SSL-Zertifikat.

Das Zertifikat kann selbstsigniert oder von einer Zertifizierungsstelle signiert sein. Informatica empfiehlt ein von einer Zertifizierungsstelle signiertes Zertifikat.

Sie haben das Zertifikat in Schlüsselspeicher importiert.

Sie müssen über einen Schlüsselspeicher im PEM-Format mit der Bezeichnung `infa_keystore.pem` sowie über einen Schlüsselspeicher im JKS-Format mit der Bezeichnung `infa_keystore.jks` verfügen.

Hinweis: Das Passwort für den Schlüsselspeicher im JKS-Format muss mit der Passphrase des privaten Schlüssels übereinstimmen, die zum Erzeugen des SSL-Zertifikats verwendet wurde.

Sie haben das Zertifikat in Truststores importiert.

Sie müssen über einen Truststore im PEM-Format mit der Bezeichnung `infa_keystore.pem` sowie über einen Schlüsselspeicher im JKS-Format mit der Bezeichnung `infa_keystore.jks` verfügen.

Die Schlüsselspeicher und Truststores befinden sich im richtigen Verzeichnis.

Der Schlüsselspeicher und der Truststore müssen sich in einem Verzeichnis befinden, auf das das Installationsprogramm zugreifen kann.

Weitere Informationen zum Erstellen eines benutzerdefinierten Schlüsselspeichers und Truststores finden Sie im Artikel „How to Create Keystore and Truststore Files for Secure Communication in the Informatica

Domain“ in der Informatica How-To Library:
https://kb.informatica.com/h2l/HowTo%20Library/1/0700-CreateKeystoresAndTruststores-H2L.pdf

Sichere Verbindung zum Administrator Tool

Bevor Sie die Verbindung zum Administrator Tool sichern, stellen Sie sicher, dass die folgende Anforderungen erfüllt sind:

Sie haben eine Zertifikatssignieranfrage und einen privaten Schlüssel erstellt.

Sie können keytool oder OpenSSL zum Erstellen der Zertifikatssignieranfrage und des privaten Schlüssels verwenden.

Bei Verwendung von RSA-Verschlüsselung müssen Sie mehr als 512 Bit verwenden.

Sie haben ein signiertes SSL-Zertifikat.

Das Zertifikat kann selbstsigniert oder von einer Zertifizierungsstelle signiert sein. Informatica empfiehlt ein von einer Zertifizierungsstelle signiertes Zertifikat.

Sie haben das Zertifikat in einen Schlüsselspeicher im JKS-Format importiert.

Ein Schlüsselspeicher muss nur ein Zertifikat enthalten. Wenn Sie ein eindeutiges Zertifikat für jeden Webanwendungsdienst verwenden, erstellen Sie einen separaten Schlüsselspeicher für jedes Zertifikat. Alternativ können Sie ein gemeinsam genutztes Zertifikat und einen gemeinsam genutzten Schlüsselspeicher verwenden.

Wenn Sie das vom Installationsprogramm erzeugte SSL-Zertifikat für das Administrator-Tool verwenden, müssen Sie das Zertifikat nicht in einen Schlüsselspeicher im JKS-Format importieren.

Der Schlüsselspeicher befindet sich im richtigen Verzeichnis.

Der Schlüsselspeicher muss sich in einem Verzeichnis befinden, auf das das Installationsprogramm zugreifen kann.

Extrahieren der Dateien des Installationsprogramms

Die Installationsprogrammdateien sind komprimiert und werden als ZIP-Datei verteilt.

Verwenden Sie ein ZIP-Dienstprogramm zum Extrahieren der Installationsprogrammdateien in ein Verzeichnis auf Ihrem Computer. Stellen Sie sicher, dass die ZIP-Dienstprogrammversion mit der Version des Betriebssystems Windows kompatibel ist. Wenn Sie die Datei entpacken, stellen Sie sicher, dass das ZIP-Dienstprogramm auch leere Ordner extrahiert.

Sie können die Installationsprogrammdateien folgendermaßen extrahieren:

- Installations-DVD. Laden Sie die Informatica-ZIP-Datei aus der Installations-DVD in ein Verzeichnis auf Ihrem Computer und extrahieren Sie die Installationsprogrammdateien; oder extrahieren Sie die Installationsprogrammdateien direkt aus der DVD in ein Verzeichnis auf Ihrem Computer. Wenn Sie die ZIP-Datei in ein Verzeichnis auf Ihrem Computer laden, vergewissern Sie sich, dass die Länge des gesamten Installationsverzeichnispfads, einschließlich des Namens der Zip-Datei, 60 Zeichen nicht überschreitet.
- FTP-Download. Laden Sie die ZIP-Installationsdatei von Informatica aus der Informatica Electronic Software Download-Site in ein Verzeichnis auf Ihrem Computer herunter und extrahieren Sie die Installationsprogrammdateien.

Hinweis: Stellen Sie sicher, dass Sie die Datei in ein lokales Verzeichnis oder ein gemeinsam genutztes Netzlaufwerk herunterladen, das auf Ihrem Computer zugeordnet ist. Sie können dann die Dateien des

Installationsprogramms extrahieren. Sie können jedoch das Installationsprogramm nicht aus einer zugeordneten Datei ausführen. Kopieren Sie die extrahierten Dateien in ein lokales Laufwerk, und führen Sie anschließend das Installationsprogramm aus.

Überprüfen Sie den Lizenzschlüssel

Vergewissern Sie sich vor dem Installieren der Software, dass Sie über einen Lizenzschlüssel verfügen.

Sie können sich den Lizenzschlüssel folgendermaßen besorgen:

- Installations-DVD. Wenn Ihnen die Installationsdateien auf DVD vorliegen, finden Sie die Lizenzschlüsseldatei auf der Informatica-Lizenzschlüssel-CD.
- HTTP-Download. Wenn Sie die Installationsdateien von der Electronic Software Download (ESD)-Site von Informatica heruntergeladen haben, erhalten Sie den Lizenzschlüssel in einer E-Mail-Nachricht von Informatica. Kopieren Sie die Lizenzschlüsseldatei in ein Verzeichnis, worauf das Benutzerkonto, das Informatica installiert, zugreifen kann.

Wenden Sie sich an den globalen Kundensupport von Informatica, wenn Ihnen kein Lizenzschlüssel vorliegt oder Sie über einen inkrementellen Lizenzschlüssel verfügen und eine Domäne erstellen möchten.

Ausführen des Vorinstallations-Systemprüfungstools (i10Pi)

Führen Sie das Vorinstallations-Systemprüfungstool (i10Pi) aus, um sicherzustellen, dass der Computer die Systemanforderungen für die Installation oder das Upgrade erfüllt.

Stellen Sie sicher, dass Sie die Systemanforderungen überprüft und die Datenbank des Domänen-Konfigurations-Repository vorbereitet haben.

1. Melden Sie sich mit einem Systembenutzerkonto am Computer an.
2. Schließen Sie alle anderen Anwendungen.
3. Navigieren Sie zu dem Root-Verzeichnis, das die Installationsdateien enthält, und führen Sie die Datei „install.bat“ als Administrator aus.
4. Wählen Sie **Informatica 10.1.1 HotFix 1 installieren** aus.
5. Wählen Sie **Ausführen des Vorinstallations-Systemprüfungstools (i10Pi)**, um zu überprüfen, ob der Computer die Systemanforderungen für die Installation oder das Upgrade erfüllt.
6. Klicken Sie auf **Start**.

   Die Seite **Willkommen** im Vorinstallations-Systemprüfungstool (i10Pi) wird angezeigt.
7. Klicken Sie auf **Weiter**.

   Die Seite **Systeminformationen** wird angezeigt.
8. Geben Sie den absoluten Pfad für das Installationsverzeichnis an.

   Die Verzeichnisnamen in dem Pfad dürfen weder Leerzeichen noch die folgenden Sonderzeichen enthalten: @|* $ # ! % ( ) { } [ ] , ; '

Hinweis: Informatica empfiehlt die Verwendung alphanumerischer Zeichen im Installationsverzeichnispfad. Wenn Sie ein Sonderzeichen wie zum Beispiel á oder € verwenden, können unerwartete Ergebnisse während der Laufzeit auftreten.

9. Geben Sie die Start-Portnummer für den Knoten ein, den Sie auf dem Computer erstellen oder aktualisieren möchten. Die Standard-Portnummer für den Knoten lautet 6005.
10. Klicken Sie auf **Weiter**.

    Die Seite **Datenbank- und JDBC-Verbindungsinformationen** wird eingeblendet.
11. Geben Sie die Daten für die Datenbank des Domänen-Konfigurations-Repositorys ein.

    In der folgenden Tabelle sind die Eigenschaften beschrieben, die Sie für die Datenbank und das Benutzerkonto festlegen:

Eigenschaft	Beschreibung
Datenbanktyp	Datenbank für das Repository. Wählen Sie eine der folgenden Datenbanken aus: - Oracle - IBM DB2 - Microsoft SQL Server - Sybase ASE
Datenbankbenutzer-ID	Benutzerkonto für die Repository-Datenbank.
Benutzerpasswort	Das Passwort für das Datenbankbenutzerkonto.

    Das Domänen-Konfigurations-Repository muss allen Gateway-Knoten in der Domäne zugänglich sein.

12. Wenn Sie eine sichere Datenbank für das Domänen-Konfigurations-Repository verwenden, wählen Sie die Option **Sichere Datenbank** aus.
13. Geben Sie die Verbindungsinformationen für die Datenbank ein.
    - Um die Verbindungsinformationen unter Verwendung der JDBC-URL-Informationen einzugeben, wählen Sie **JDBC-URL** aus und geben die JDBC-URL-Eigenschaften an.
      In der folgenden Tabelle werden die JDBC-URL-Eigenschaften beschrieben, die Sie festlegen:

Eigenschaft	Beschreibung
Datenbankadresse	Der Hostname und die Portnummer für die Datenbank im Format `host_name:port`.
Datenbankdienstname	Dienst- oder Datenbankname: - Oracle: Geben Sie den Dienstnamen ein. - Microsoft SQL Server: Geben Sie den Datenbanknamen ein. - IBM DB2: Geben Sie den Dienstnamen ein. - Sybase ASE: Geben Sie den Datenbanknamen ein.
JDBC-Parameter	Optionale Parameter, die in der Datenbank-Verbindungszeichenfolge aufgenommen werden können. Mit den Parametern können die Datenbankvorgänge für die Datenbank optimiert werden. Überprüfen Sie die Gültigkeit der Parameterzeichenfolge. Das Installationsprogramm führt vor dem Hinzufügen der Parameterzeichenfolge zur JDBC-URL keine Überprüfung der Zeichenfolge durch. Ist diese Option nicht aktiviert, erstellt das Installationsprogramm die JDBC-URL ohne zusätzliche Parameter.

- Um die Verbindungsdaten mithilfe einer benutzerdefinierten JDBC-Verbindungszeichenfolge einzugeben, wählen Sie **Benutzerdefinierte JDBC-Verbindungszeichenfolge** aus und geben Sie die Verbindungszeichenfolge ein.
  Verwenden Sie die folgende Syntax in der JDBC-Verbindungszeichenfolge:
  IBM DB2

  ```
  jdbc:Informatica:db2://host_name:port_no;DatabaseName=
  ```

  Oracle

  ```
  jdbc:Informatica:oracle://host_name:port_no;ServiceName=
  ```

  Microsoft SQL Server

  ```
  jdbc:Informatica:sqlserver://host_name:port_no;SelectMethod=cursor;DatabaseName=
  ```

  Sybase

  ```
  jdbc:Informatica:sybase://host_name:port_no;DatabaseName=
  ```

  Stellen Sie sicher, dass die Verbindungszeichenfolge alle vom Datenbanksystem benötigten Verbindungsparameter enthält.
- Wenn Sie die Option **Sichere Datenbank** auswählen, wählen Sie **Benutzerdefinierte JDBC-Verbindungszeichenfolge** und geben Sie die Verbindungszeichenfolge ein.
  Neben den Verbindungsparametern müssen die Sicherheitsparameter berücksichtigt werden. Informationen zu den Sicherheitsparametern, die in die JDBC-Verbindung für eine sichere Datenbank aufgenommen werden müssen, finden Sie unter "Verbindungszeichenfolge für eine sichere Datenbank" auf Seite 71.

14. Klicken Sie auf **Verbindung testen**, um zu überprüfen, ob Sie eine Verbindung zur Datenbank herstellen können, und anschließend auf **OK**, um fortzufahren.
15. Klicken Sie auf **Weiter**, um die Systemprüfung zu starten.

    Das Tool prüft die Einstellungen der Festplatte, die Verfügbarkeit der Ports und die Konfiguration der Datenbank. Nach abgeschlossener Systemprüfung wird die Seite **Systemprüfungsübersicht** angezeigt, auf der Sie die Ergebnisse der Systemprüfung sehen.
16. Kontrollieren Sie die Ergebnisse der Systemprüfung.

    Die Liste enthält sämtliche Anforderungen mit jeweils einem der folgenden Prüfstatusangaben:

    - [Erfolg] - Die Anforderung erfüllt die Kriterien für die Installation oder Aktualisierung von Informatica.
    - [Fehler] - Die Anforderung erfüllt die Kriterien für die Installation oder Aktualisierung von Informatica nicht. Beheben Sie dieses Problem, bevor Sie die Installation oder das Upgrade fortsetzen.
    - [Information]: Prüfen Sie die Informationen und führen Sie weitere Aufgaben wie beschrieben aus.

    Die Ergebnisse der Systemprüfung werden in der folgenden Datei gespeichert: `.../Server/I10PI/I10PI/en/i10Pi_summary.txt`
17. Klicken Sie auf **Fertig**, um das Vorinstallations-Systemprüfungstool (i10Pi) zu schließen.

Wenn das Vorinstallations-Systemprüfungstool (i10Pi) nicht erfüllte Anforderungen ermittelt hat, prüfen Sie die fehlgeschlagenen Anforderungen und führen Sie das Vorinstallations-Systemprüfungstool (i10Pi) erneut aus.

Hinweis: Die Installation oder Aktualisierung von Informatica kann auch dann ausgeführt werden, wenn das Vorinstallations-Systemprüfungstool (i10Pi) nicht erfüllte Anforderungen ermittelt hat. Informatica empfiehlt jedoch dringend, sämtliche Probleme vor dem Fortsetzen der Installation oder des Upgrades zu beheben.

KAPITEL 6

Vor der Installation von Diensten unter UNIX

Dieses Kapitel umfasst die folgenden Themen:

- Vor der Installation von Diensten unter UNIX - Übersicht, 94
- Lesen der Versionshinweise, 95
- Überprüfen Sie die Patch Anforderungen, 95
- Installieren der Java-Laufzeitumgebung, 95
- Data Transformation-Dateien sichern, 96
- Überprüfen der Umgebungsvariablen, 97
- Erstellen eines Systembenutzerkontos, 97
- Einrichten von Schlüsselspeicher- und Truststore-Dateien, 98
- Festlegen des Grenzwerts für den Dateideskriptor, 99
- Konfigurieren von POSIX Asynchronous I/O, 100
- Extrahieren der Dateien des Installationsprogramms, 100
- Überprüfen Sie den Lizenzschlüssel, 101
- Ausführen des Vorinstallations-Systemprüfungstools (i10Pi), 101

Vor der Installation von Diensten unter UNIX - Übersicht

Bevor Sie die Informatica-Dienste installieren, richten Sie den Computer so ein, dass er die Anforderungen für das Installieren und Ausführen der Informatica-Plattform erfüllt. Wenn der Computer, auf dem Sie die Informatica-Dienste installieren möchten, nicht ordnungsgemäß konfiguriert ist, kann die Installation fehlschlagen.

Lesen der Versionshinweise

Lesen Sie die Versionshinweise, um mehr über Aktualisierungen der Installation und den Upgradeprozess zu erfahren. Außerdem können Sie Informationen über bekannte und behobene Einschränkungen für die Version finden.

Überprüfen Sie die Patch Anforderungen

Bevor Sie die Informatica-Dienste installieren, stellen Sie sicher, dass der Computer über die erforderlichen Betriebssystem-Patches und -Bibliotheken verfügt.

In der folgenden Tabelle finden Sie eine Auflistung der Patches und Bibliotheken, die die Informatica-Dienste auf einer UNIX-Plattform benötigen:

Plattform	Betriebssystem	Betriebssystem-Patch
AIX	7.1 TL2	Betriebssystemebene: 7100-02 bos.adt.debug Version 7.1.2.0
AIX	6.1 TL8	Betriebssystemebene: 6100-08 bos.adt.debug Version 6.1.8.0
Linux-x64	Red Hat Enterprise Linux 6.5	Alle folgenden Pakete, in denen <version> eine beliebige Version des Pakets ist: - e2fsprogs-libs-<version>.el6 - keyutils-libs-<version>.el6 - libselinux-<version>.el6 - libsepol-<version>.el6
Linux-x64	Red Hat Enterprise Linux 7	Alle folgenden Pakete, in denen <version> eine beliebige Version des Pakets ist: - e2fsprogs-libs-<version>.el7 - keyutils-libs-<version>.el7 - libselinux-<version>.el7 - libsepol-<version>.el7
Linux-x64	SUSE Linux Enterprise Server 11	Service Pack 3
Solaris	11	-

Installieren der Java-Laufzeitumgebung

Informatica stellt standardmäßig die Java-Bibliotheken für Linux bereit. Die Java-Bibliotheken für AIX befinden sich nicht im Lieferumfang von Informatica. Bevor Sie Informatica unter AIX installieren, müssen Sie die Java-Laufzeitumgebung (JRE) herunterladen. Die erforderliche JRE-Version hängt von der Plattform ab, auf der Sie Informatica installieren.

Informatica-Dienste unter AIX sind für die folgende Version zertifiziert:

Java(TM) SE-Laufzeitumgebung pap6480sr4fp2-20170322_01(SR4 FP2)

Laden Sie die folgende Datei herunter: `Java8_64.jre.8.0.0.402.tar.gz`

Wenn Probleme bei der Installation von JRE auftreten, wenden Sie sich an den JRE-Anbieter.

Hinweis: Optional können Sie zum Aktivieren der Unterstützung für Cipher-Suites, die AES-256 verwenden, die Java Cryptography Extension (JCE) installieren. Die JCE-Richtliniendateien sind nicht im Lieferumfang von Informatica enthalten. Weitere Informationen zum Herunterladen und Installieren der JCE-Richtliniendateien finden Sie unter den JCE-Richtliniendateien auf http://www.ibm.com/support/knowledgecenter/SS8JFY_7.5.0/com.ibm.lmt75.doc/com.ibm.license.mgmt.security.doc/lmt_scr_downloading_installing_jce_policyfiles.html.

Die über die angegebenen Links zum Download verfügbare Software wird nicht von Informatica LLC angeboten, sondern ist Eigentum eines oder mehrerer Drittanbieter. Eventuelle Fehler, Auslassungen oder Änderungen bei den Download-Links können nicht ausgeschlossen werden. Informatica übernimmt keinerlei Verantwortung für diese Links und/oder Software, lehnt jegliche ausdrückliche oder stillschweigende Garantie ab, einschließlich jedweder stillschweigenden Garantie in Bezug auf Handelsüblichkeit, Eignung zu einem bestimmten Zweck, Eigentumsrechte und Nichtverletzung von Rechten Dritter, und schließt jedweden damit verbundenen Haftungsanspruch aus.

Data Transformation-Dateien sichern

Vor der Installation müssen Sie die unter früheren Versionen erstellten Data Transformation-Dateien sichern. Kopieren Sie nach Abschluss der Installation die Dateien in die neuen Installationsverzeichnisse, damit Repository und benutzerdefinierte globale Komponenten die gleichen sind wie in der vorherigen Version.

In der folgenden Tabelle sind die Dateien und Verzeichnisse aufgeführt, die gesichert werden müssen:

Datei oder Verzeichnis	Standardspeicherort
Repository	<Informatica-Installationsverzeichnis>\DataTransformation\ServiceDB
Custom Global Components-Verzeichnis (TGP-Dateien)	<Informatica-Installationsverzeichnis>\DataTransformation\autoInclude\user
Custom Global Components-Verzeichnis (DLL- und JAR-Dateien)	<Informatica-Installationsverzeichnis>\DataTransformation\externLibs\user
Konfigurationsdatei	<Informatica-Installationsverzeichnis>\DataTransformation\CMConfig.xml
Lizenzdatei	<Informatica-Installationsverzeichnis>\DataTransformation\CDELicense.cfg

Kopieren Sie die Data Transformation-Bibliotheksdateien nicht. Installieren Sie stattdessen die Data Transformation-Bibliotheken erneut.

Überprüfen der Umgebungsvariablen

Konfigurieren Sie die Umgebungsvariablen so, dass sie mit der Installation von Informatica funktionieren.

In der folgenden Tabelle werden die unter UNIX zu überprüfenden Umgebungsvariablen beschrieben:

Variable	Beschreibung
IATEMPDIR	Der Speicherort der während der Installation erstellten temporären Dateien. Informatica benötigt 1 GB Speicherplatz auf der Festplatte für temporäre Dateien. Konfigurieren Sie die Umgebungsvariable, wenn keine temporären Dateien im Verzeichnis /tmp erstellt werden sollen.
INFA_JRE_HOME	Speicherort des Ordners, der die unterstützte Java-Laufzeitumgebung (JRE) enthält. Wenn Sie Informatica auf AIX installieren, legen Sie die INFA_JRE_HOME-Umgebungsvariable fest. In der Konfigurationsdatei für Ihre Shell, etwa der .bashrc-Datei, setzen Sie die Umgebungsvariable INFA_JRE_HOME auf das Verzeichnis mit JRE. Stellen Sie sicher, dass die Login-Shell auf die Umgebungsvariable INFA_JRE_HOME zugreifen kann.
JRE_HOME	Wenn Sie die Informatica-Dienste auf einem UNIX-Computer installieren, löschen Sie die Umgebungsvariable JRE_HOME vor dem Beginn der Installation.
LANG und LC_ALL	Ändern Sie das Gebietsschema, um die entsprechende Zeichenkodierung für die Terminalsitzung festzulegen. Legen Sie zum Beispiel die Kodierung auf `Latin1` oder `ISO-8859-1` für Französisch; `EUC-JP` oder `UMSCHALT JIS` für Japanisch; oder `UTF-8` für Chinesisch oder Koreanisch fest. Die Zeichenkodierung legt die Arten von Zeichen fest, die auf dem UNIX-Terminal angezeigt werden.
DISPLAY	Löschen Sie die DISPLAY-Umgebung, bevor Sie das Installationsprogramm ausführen. Die Installation schlägt möglicherweise fehl, wenn die DISPLAY-Umgebungsvariable einen Wert aufweist.

Erstellen eines Systembenutzerkontos

Erstellen Sie ein Benutzerkonto speziell für das Ausführen des Informatica-Dämons.

Vergewissern Sie sich, dass das Benutzerkonto, das Sie zum Installieren von Informatica verwenden, über Schreibberechtigung im Installationsverzeichnis verfügt.

Einrichten von Schlüsselspeicher- und Truststore-Dateien

Wenn Sie die Informatica-Dienste installieren, können Sie die sichere Kommunikation für die Domäne konfigurieren und eine sichere Verbindung zu Informatica Administrator einrichten. Wenn Sie diese Sicherheitsoptionen konfigurieren, müssen Sie Schlüsselspeicher- und Truststore-Dateien einrichten.

Bevor Sie die Informatica-Dienste installieren, richten Sie die Dateien für die sichere Kommunikation innerhalb der Informatica-Domäne oder für eine sichere Verbindung zum Administrator Tool ein. Sie können die folgenden Programme verwenden, um die erforderlichen Dateien zu erstellen:

Keytool

Sie können Keytool zum Erstellen eines SSL-Zertifikats oder eines CSR (Certificate Signing Request) sowie als Schlüsselspeicherdateien und Truststore-Dateien im JKS-Format verwenden.

Weitere Informationen zur Verwendung von Keytool finden Sie in der Dokumentation auf der folgenden Website: http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html

OpenSSL

Sie können OpenSSL verwenden, um ein SSL-Zertifikat oder eine Zertifikatssignieranfrage zu erstellen und einen Schlüsselspeicher im JKS-Format in das PEM-Format zu konvertieren.

Weitere Informationen zu OpenSSL finden Sie in der Dokumentation auf der folgenden Website: https://www.openssl.org/docs/

Damit Sie eine höhere Sicherheitsebene erzielen, senden Sie Ihr CSR an eine Zertifizierungsstelle, um ein signiertes Zertifikat zu erhalten.

Die über die angegebenen Links zum Download verfügbare Software wird nicht von Informatica LLC angeboten, sondern ist Eigentum eines oder mehrerer Drittanbieter. Eventuelle Fehler oder Änderungen bei den Download-Links können nicht ausgeschlossen werden. Informatica übernimmt keinerlei Verantwortung für diese Links und/oder Software, lehnt jegliche ausdrückliche oder stillschweigende Garantien ab, einschließlich jedweder stillschweigenden Garantien in Bezug auf Handelsüblichkeit, Eignung zu einem bestimmten Zweck, Eigentumsrechte und Nichtverletzung von Rechten Dritter, und schließt jedwede damit verbundene Haftungsansprüche aus.

Sichere Kommunikation innerhalb der Informatica-Domäne

Bevor Sie die sichere Kommunikation innerhalb der Informatica-Domäne aktivieren, überprüfen Sie, ob die folgenden Anforderungen erfüllt sind:

Sie haben eine Zertifikatssignieranfrage und einen privaten Schlüssel erstellt.

Sie können keytool oder OpenSSL zum Erstellen der Zertifikatssignieranfrage und des privaten Schlüssels verwenden.

Bei Verwendung von RSA-Verschlüsselung müssen Sie mehr als 512 Bit verwenden.

Sie haben ein signiertes SSL-Zertifikat.

Das Zertifikat kann selbstsigniert oder von einer Zertifizierungsstelle signiert sein. Informatica empfiehlt ein von einer Zertifizierungsstelle signiertes Zertifikat.

Sie haben das Zertifikat in Schlüsselspeicher importiert.

Sie müssen über einen Schlüsselspeicher im PEM-Format mit der Bezeichnung `infa_keystore.pem` sowie über einen Schlüsselspeicher im JKS-Format mit der Bezeichnung `infa_keystore.jks` verfügen.

Hinweis: Das Passwort für den Schlüsselspeicher im JKS-Format muss mit der Passphrase des privaten Schlüssels übereinstimmen, die zum Erzeugen des SSL-Zertifikats verwendet wurde.

Sie haben das Zertifikat in Truststores importiert.

Sie müssen über einen Truststore im PEM-Format mit der Bezeichnung `infa_keystore.pem` sowie über einen Schlüsselspeicher im JKS-Format mit der Bezeichnung `infa_keystore.jks` verfügen.

Die Schlüsselspeicher und Truststores befinden sich im richtigen Verzeichnis.

Der Schlüsselspeicher und der Truststore müssen sich in einem Verzeichnis befinden, auf das das Installationsprogramm zugreifen kann.

Weitere Informationen zum Erstellen eines benutzerdefinierten Schlüsselspeichers und Truststores finden Sie im Artikel „How to Create Keystore and Truststore Files for Secure Communication in the Informatica Domain“ in der Informatica How-To Library:
https://kb.informatica.com/h2l/HowTo%20Library/1/0700-CreateKeystoresAndTruststores-H2L.pdf

Sichere Verbindung zum Administrator Tool

Bevor Sie die Verbindung zum Administrator Tool sichern, stellen Sie sicher, dass die folgende Anforderungen erfüllt sind:

Sie haben eine Zertifikatssignieranfrage und einen privaten Schlüssel erstellt.

Sie können keytool oder OpenSSL zum Erstellen der Zertifikatssignieranfrage und des privaten Schlüssels verwenden.

Bei Verwendung von RSA-Verschlüsselung müssen Sie mehr als 512 Bit verwenden.

Sie haben ein signiertes SSL-Zertifikat.

Das Zertifikat kann selbstsigniert oder von einer Zertifizierungsstelle signiert sein. Informatica empfiehlt ein von einer Zertifizierungsstelle signiertes Zertifikat.

Sie haben das Zertifikat in einen Schlüsselspeicher im JKS-Format importiert.

Ein Schlüsselspeicher muss nur ein Zertifikat enthalten. Wenn Sie ein eindeutiges Zertifikat für jeden Webanwendungsdienst verwenden, erstellen Sie einen separaten Schlüsselspeicher für jedes Zertifikat. Alternativ können Sie ein gemeinsam genutztes Zertifikat und einen gemeinsam genutzten Schlüsselspeicher verwenden.

Wenn Sie das vom Installationsprogramm erzeugte SSL-Zertifikat für das Administrator-Tool verwenden, müssen Sie das Zertifikat nicht in einen Schlüsselspeicher im JKS-Format importieren.

Der Schlüsselspeicher befindet sich im richtigen Verzeichnis.

Der Schlüsselspeicher muss sich in einem Verzeichnis befinden, auf das das Installationsprogramm zugreifen kann.

Festlegen des Grenzwerts für den Dateideskriptor

Stellen Sie sicher, dass das Betriebssystem die Anforderung des Dateideskriptors erfüllt.

Informatica-Dienstprozesse können eine hohe Anzahl an Dateien verwenden. Zur Vermeidung von Fehlern, die sich aus der hohen Anzahl an Dateien und Prozessen ergeben, können Sie Systemeinstellungen mithilfe des Limit-Befehls ändern, wenn Sie eine C-Shell verwenden, oder mithilfe des Ulimit-Befehls, wenn Sie eine Bash-Shell verwenden.

Zum Abrufen einer Liste der Betriebssystemeinstellungen, einschließlich des Dateideskriptorgrenzwerts, führen Sie den folgenden Befehl aus:
C-Shell

```
Limit
```

Bash-Shell

```
ulimit -a
```

Informatica-Dienstprozesse können eine hohe Anzahl an Dateien verwenden. Stellen Sie den Grenzwert für den Dateideskriptor pro Vorgang auf mindestens 16.000 ein. Der empfohlene Grenzwert ist 32.000 Dateideskriptoren pro Vorgang.

Zum Ändern der Systemeinstellungen führen Sie den Limit- oder Ulimit-Befehl mit dem entsprechenden Flag und Wert aus. Führen Sie beispielsweise zum Einrichten des Dateideskriptorgrenzwerts folgenden Befehl durch:

C-Shell

```
limit -h filesize <value>
```

Bash-Shell

```
ulimit -n <value>
```

Informatica-Dienste verwenden zahlreiche Benutzerprozesse. Verwenden Sie den Befehl „ulimit -u“, um die Einstellung der maximalen Benutzerprozesse hoch genug für alle für Blaze erforderlichen Prozesse einzustellen. Abhängig von der Anzahl der Mappings und Umwandlungen, die gleichzeitig ausgeführt werden können, legen Sie die Einstellung vom Standardwert 1024 auf mindestens 4096 fest.

Führen Sie folgenden Befehl aus, um die Einstellung der maximalen Benutzerprozesse festzulegen:

C-Shell

```
limit -u processes <Wert>
```

Bash-Shell

```
ulimit -u <Wert>
```

Konfigurieren von POSIX Asynchronous I/O

Machen Sie POSIX Asynchronous I/O bei der Installation von Informatica auf IBM AIX auf allen Konten verfügbar, auf denen Sie einen PowerCenter Integration Service ausführen möchten. Wenn POSIX Asynchronous I/O nicht verfügbar ist, kann ein auf einem IBM AIX-Rechner ausgeführter PowerCenter Integration Service möglicherweise nicht gestartet werden.

Extrahieren der Dateien des Installationsprogramms

Die Installationsprogrammdateien sind komprimiert und werden als Tar-Datei verteilt.

Verwenden Sie ein natives Tar- oder GNU-Tar-Dienstprogramm zum Extrahieren der Installationsprogrammdateien in ein Verzeichnis auf Ihrem Computer. Der Benutzer, der das Installationsprogramm ausführt, muss über Lese- und Schreibberechtigungen für das Verzeichnis der Installationsdateien sowie über Ausführungsberechtigungen in „install.sh“ verfügen.

Sie können die Installationsprogrammdateien folgendermaßen extrahieren:

- Installations-DVD. Laden Sie die Informatica-Tar-Datei aus der Installations-DVD in ein Verzeichnis auf Ihrem Computer und extrahieren Sie die Installationsprogrammdateien; oder extrahieren Sie die Installationsprogrammdateien direkt aus der DVD in ein Verzeichnis auf Ihrem Computer.

- FTP-Download. Laden Sie die Tar-Datei der Informatica-Installation von der Informatica Electronic Software Download-Site in ein Verzeichnis auf Ihrem Computer herunter und extrahieren Sie die Installationsprogrammdateien.

Hinweis: Achten Sie darauf, die Datei in ein lokales Verzeichnis oder ein gemeinsam genutztes Netzlaufwerk herunterzuladen, das auf Ihrem Computer zugeordnet ist. Sie können dann die Dateien des Installationsprogramms extrahieren. Sie können jedoch das Installationsprogramm nicht aus einer zugeordneten Datei ausführen. Kopieren Sie die extrahierten Dateien in ein lokales Laufwerk und führen Sie anschließend das Installationsprogramm aus.

Überprüfen Sie den Lizenzschlüssel

Vergewissern Sie sich vor dem Installieren der Software, dass Sie über einen Lizenzschlüssel verfügen.

Sie können sich den Lizenzschlüssel folgendermaßen besorgen:

- Installations-DVD. Wenn Ihnen die Installationsdateien auf DVD vorliegen, finden Sie die Lizenzschlüsseldatei auf der Informatica-Lizenzschlüssel-CD.
- HTTP-Download. Wenn Sie die Installationsdateien von der Electronic Software Download (ESD)-Site von Informatica heruntergeladen haben, erhalten Sie den Lizenzschlüssel in einer E-Mail-Nachricht von Informatica. Kopieren Sie die Lizenzschlüsseldatei in ein Verzeichnis, worauf das Benutzerkonto, das Informatica installiert, zugreifen kann.

Wenden Sie sich an den globalen Kundensupport von Informatica, wenn Ihnen kein Lizenzschlüssel vorliegt oder Sie über einen inkrementellen Lizenzschlüssel verfügen und eine Domäne erstellen möchten.

Ausführen des Vorinstallations-Systemprüfungstools (i10Pi)

Führen Sie das Vorinstallations-Systemprüfungstool (i10Pi) aus, um sicherzustellen, dass der Computer die Systemanforderungen für die Installation oder das Upgrade erfüllt.

Stellen Sie sicher, dass Sie die Systemanforderungen überprüft und die Datenbank des Domänen-Konfigurations-Repository vorbereitet haben.

1. Melden Sie sich mit einem Systembenutzerkonto am Computer an.
2. Schließen Sie alle anderen Anwendungen.
3. Führen Sie über eine Shell-Befehlszeile die Datei „install.sh“ im Root-Verzeichnis aus.

   Der Installer zeigt die Nachricht an, um sicherzustellen, dass die Gebietsschema-Umgebungsvariablen gesetzt sind.
4. Wurden die Umgebungsvariablen nicht eingestellt, drücken Sie **n**, um den Installer zu beenden. Stellen Sie sie anschließend entsprechend den Anforderungen ein.

   Wenn die Umgebungsvariablen eingestellt sind, drücken Sie **y**, um fortzufahren.
5. Drücken Sie **1**, um die Installation oder das Upgrade von Informatica durchzuführen.
6. Drücken Sie **1**, um das Vorinstallations-Systemprüfungstool (i10Pi) auszuführen, mit dem sichergestellt wird, dass der Computer die Systemanforderungen für die Installation oder das Upgrade erfüllt.

7. Klicken Sie unter **Willkommen** im Vorinstallations-Systemprüfungstool (i10Pi) auf **Weiter**.

   Der Abschnitt **Systeminformationen** wird angezeigt.

8. Geben Sie den absoluten Pfad für das Installationsverzeichnis ein.

   Die Verzeichnisnamen in dem Pfad dürfen weder Leerzeichen noch die folgenden Sonderzeichen enthalten: @|* $ # ! % ( ) { } [ ] , ; '

   Hinweis: Informatica empfiehlt die Verwendung alphanumerischer Zeichen im Installationsverzeichnispfad. Wenn Sie ein Sonderzeichen wie zum Beispiel á oder € verwenden, können unerwartete Ergebnisse während der Laufzeit auftreten.

9. Drücken Sie die **Eingabetaste**.

10. Geben Sie die Start-Portnummer für den Knoten ein, den Sie auf dem Computer erstellen oder aktualisieren möchten. Die Standard-Portnummer für den Knoten lautet 6005.

11. Drücken Sie die **Eingabetaste**.

    Der Abschnitt **Datenbank- und Verbindungsinformationen** wird angezeigt.

12. Um die JDBC-Verbindungsdaten mithilfe einer benutzerdefinierten JDBC-Verbindungszeichenfolge einzugeben, drücken Sie **1**. Um die JDBC-Verbindungsdaten mithilfe der JDBC-URL-Daten einzugeben, drücken Sie **2**.

    Zum Herstellen einer Verbindung zu einer sicheren Datenbank müssen Sie die JDBC-Verbindung mithilfe einer benutzerdefinierten JDBC-Verbindungszeichenfolge eingeben.

13. Geben Sie die JDBC-Verbindungsdaten ein.

    - Um die Verbindungsdaten mithilfe einer benutzerdefinierten JDBC-Verbindungszeichenfolge einzugeben, geben Sie die Verbindungszeichenfolge ein und legen Sie die Verbindungsparameter fest.
      Verwenden Sie die folgende Syntax in der JDBC-Verbindungszeichenfolge:
      IBM DB2

      ```
      jdbc:Informatica:db2://host_name:port_no;DatabaseName=
      ```

      Oracle

      ```
      jdbc:Informatica:oracle://host_name:port_no;ServiceName=
      ```

      Microsoft SQL Server

      ```
      jdbc:Informatica:sqlserver://host_name:port_no;SelectMethod=cursor;DatabaseName=
      ```

      Sybase

      ```
      jdbc:Informatica:sybase://host_name:port_no;DatabaseName=
      ```

      Stellen Sie sicher, dass die Verbindungszeichenfolge alle vom Datenbanksystem benötigten Verbindungsparameter enthält.

    - Um die Verbindungsdaten mithilfe der JDBC-URL-Daten einzugeben, legen Sie die JDBC-URL-Eigenschaften fest.

In der folgenden Tabelle werden die Verbindungsinformationen beschrieben:

Eingabeaufforderung	Beschreibung
Datenbanktyp	Der Datenbanktyp für das Domänen-Konfigurations-Repository. Treffen Sie eine Auswahl aus den folgenden Datenbanktypen: - 1 – Oracle - 2 – Microsoft SQL Server - 3 – IBM DB2 - 4 – Sybase ASE
Datenbankbenutzer-ID	Benutzer-ID des Datenbankbenutzerkontos für das Domänen-Konfigurations-Repository.
Passwort des Datenbankbenutzers	Das Passwort für das Datenbankbenutzerkonto.
Datenbank-Hostname	Hostname für den Datenbankserver.
Datenbank-Portnummer	Portnummer der Datenbank.
Datenbankdienstname	Der Dienstname für Oracle- und IBM DB2-Datenbanken bzw. der Datenbankname für Microsoft SQL Server und Sybase ASE.

- Wenn Sie eine Verbindung zu einer sicheren Datenbank herstellen möchten, wählen Sie **1** aus, um eine benutzerdefinierte Zeichenfolge zu verwenden und die Verbindungszeichenfolge einzugeben. Neben den Verbindungsparametern müssen die Sicherheitsparameter berücksichtigt werden. Informationen zu den Sicherheitsparametern, die in die JDBC-Verbindung für eine sichere Datenbank aufgenommen werden müssen, finden Sie unter "Verbindungszeichenfolge für eine sichere Datenbank" auf Seite 71.

Das Tool prüft die Einstellungen der Festplatte, die Verfügbarkeit der Ports und die Konfiguration der Datenbank. Nach abgeschlossener Systemprüfung werden im Abschnitt **Systemprüfungsübersicht** die Ergebnisse der Systemprüfung angezeigt.

14. Kontrollieren Sie die Ergebnisse der Systemprüfung.

    Die Liste enthält sämtliche Anforderungen mit jeweils einem der folgenden Prüfstatusangaben:

    - [Erfolg] - Die Anforderung erfüllt die Kriterien für die Installation oder Aktualisierung von Informatica.
    - [Fehler] - Die Anforderung erfüllt die Kriterien für die Installation oder Aktualisierung von Informatica nicht. Beheben Sie dieses Problem, bevor Sie die Installation oder das Upgrade fortsetzen.
    - [Information]: Prüfen Sie die Informationen und führen Sie weitere Aufgaben wie beschrieben aus.

    Die Ergebnisse der Systemprüfung werden in der folgenden Datei gespeichert: `.../Server/I10PI/I10PI/en/i10Pi_summary.txt`

15. Drücken Sie die **Eingabetaste**, um das Vorinstallations-Systemprüfungstool (i10Pi) zu schließen.

    Sie können sofort mit der Installation oder dem Upgrade der Informatica-Dienste fortfahren oder die Systemprüfung beenden und zu einem späteren Zeitpunkt mit der Installation oder dem Upgrade fortfahren. Wenn Sie sofort mit der Installation oder dem Upgrade fortfahren, müssen Sie das Installationsprogramm nicht erneut starten.

16. Um die Informatica Service-Installation fortzusetzen, drücken Sie **y**.

    Um die Systemprüfung zu beenden und mit der Installation fortzufahren, drücken Sie **n**.

Wenn das Vorinstallations-Systemprüfungstool (i10Pi) nicht erfüllte Anforderungen ermittelt hat, prüfen Sie die fehlgeschlagenen Anforderungen und führen Sie das Vorinstallations-Systemprüfungstool (i10Pi) erneut aus.

Hinweis: Die Installation oder Aktualisierung von Informatica kann auch dann ausgeführt werden, wenn das Vorinstallations-Systemprüfungstool (i10Pi) nicht erfüllte Anforderungen ermittelt hat. Informatica empfiehlt jedoch dringend, sämtliche Probleme vor dem Fortsetzen der Installation oder des Upgrades zu beheben.

Teil III: Installation von Diensten

Dieser Teil enthält die folgenden Kapitel:

- Installation von Informatica-Diensten, 106
- Fehlerbehebung , 169

KAPITEL 7

Installation von Informatica-Diensten

Dieses Kapitel umfasst die folgenden Themen:

- Installation von Informatica-Diensten - Übersicht, 106
- Installieren der Informatica-Dienste im Grafikmodus, 108
- Installieren der Informatica-Dienste im Konsolenmodus, 131
- Automatisches Installieren der Informatica-Dienst, 154

Installation von Informatica-Diensten - Übersicht

Sie können die Informatica-Dienste sowohl auf einem Windows- als auch auf einem UNIX-Computer installieren. Unter Windows können Sie das Installationsprogramm im Grafikmodus oder im automatischen Modus installieren. Unter UNIX können Sie das Installationsprogramm im Konsolen- oder automatischen Modus ausführen.

Führen Sie die Vorinstallationsaufgaben zur Vorbereitung auf die Installation durch. Sie können die Informatica-Dienste auf mehreren Computern installieren. Beim Installationsvorgang wird ein Dienst mit dem Namen Informatica erstellt, der unter Windows als Dienst und unter UNIX als Dämon ausgeführt wird. Beim Starten des Informatica-Diensts wird der Dienstmanager gestartet; dieser verwaltet alle Domänenvorgänge.

Sie können optional während der Installation einen Modellrepository-Dienst und einen Datenintegrationsdienst erstellen.

Melden Sie sich nach der Installation mithilfe von Informatica Administrator bei der Domäne an und erstellen und konfigurieren Sie die Anwendungsdienste.

Erstellen oder Anfügen einer Domäne

Bei der Erstinstallation müssen Sie eine Domäne erstellen. Stellen Sie eine Verknüpfung zu einer Domäne her, wenn Sie auf mehreren Computern installieren und eine Domäne auf einem anderen Computer erstellt haben.

Die Informatica-Domäne stellt die grundlegende Verwaltungseinheit für Dienste, Benutzer und Ressourcen dar. Ein Knoten entspricht der logischen Darstellung eines einzelnen Rechners. Eine Domäne enthält einen oder mehrere Knoten.

Erfolgt die Installation auf mehreren Rechnern, können Sie mehrere Domänen erstellen. Beim Erstellen einer Domäne übernimmt der Knoten auf dem Computer, der zur Installation verwendet wird, die Funktion eines

Gateway-Knotens in der Domäne. Sie können die Option „Sichere Kommunikation aktivieren“ auswählen, um sichere Kommunikation zwischen Diensten innerhalb der Domäne einzurichten.

Bei der Installation der Informatica-Dienste wird ein Knoten auf dem Rechner erstellt. Sie können eine Domäne erstellen und den Knoten dieser neuen Domäne hinzufügen. Wenn Sie keine neue Domäne erstellen möchten, können Sie den Knoten einer anderen Domäne hinzufügen.

Wenn Sie eine Domäne anfügen, können Sie den von Ihnen erstellten Knoten als Gateway-Knoten konfigurieren. Beim Erstellen eines Gateway-Knotens können Sie die Option zum Aktivieren einer sicheren HTTPS-Verbindung zu Informatica Administrator auswählen.

Systemprüfungstool (i10Pi) und SPN-Formatgenerator

Informatica stellt Dienstprogramme bereit, um die Installation der Informatica-Dienste zu vereinfachen. Sie können das Informatica-Installationsprogramm zum Ausführen von Dienstprogrammen verwenden.

Führen Sie die folgenden Dienstprogramme vor der Installation von Informatica-Diensten aus:

Vorinstallations-Systemprüfungstool (i10Pi)

Das Vorinstallations-Systemprüfungstool (i10Pi) überprüft, ob ein Computer die Systemanforderungen für die Informatica-Installation erfüllt. Informatica empfiehlt die Überprüfung der Mindestsystemanforderungen vor dem Starten der Installation.

Kerberos SPN-Formatgenerator von Informatica

Der Kerberos SPN-Formatgenerator von Informatica generiert eine Liste von Kerberos-SPNs (Dienstprinzipalnamen) und Keytab-Dateinamen in dem von Informatica benötigten Format. Wenn Sie Informatica auf einem Netzwerk installieren, das die Kerberos-Authentifizierung verwendet, führen Sie das Dienstprogramm zum Generieren der Dienstprinzipalnamen und Keytab-Dateinamen im Informatica Format aus. Bitten Sie anschließend den Kerberos-Administrator, die SPNs zur Kerberos-Prinzipaldatenbank hinzuzufügen und die Keytab-Dateien zu erstellen. Beginnen Sie erst dann mit der Installation.

Sichere Dateien und Verzeichnisse

Wenn Sie Informatica installieren oder aktualisieren, erstellt das Installationsprogramm Verzeichnisse zum Speichern von Informatica-Dateien, die eingeschränkten Zugriff benötigen, wie z. B. die Verschlüsselungsschlüsseldatei der Domäne und die Datei „nodemeta.xml“. Das Installationsprogramm weist unter UNIX verschiedene Berechtigungen für die Verzeichnisse und Dateien in den Verzeichnissen zu.

Standardmäßig erstellt das Installationsprogramm die folgenden Verzeichnisse im Informatica-Installationsverzeichnis:

<Informatica-Installationsverzeichnis>/isp/config

Enthält die Datei nodemeta.xml. Enthält außerdem das Verzeichnis „/keys“, in dem die Verschlüsselungsschlüsseldatei gespeichert ist. Wenn Sie die Domäne konfigurieren, um die Kerberos-Authentifizierung zu verwenden, enthält das Verzeichnis „/keys“ auch die Kerberos-Keytab-Dateien. Sie können ein anderes Verzeichnis festlegen, in dem die Dateien gespeichert werden sollen. Das Installationsprogramm weist dieselben Berechtigungen für das angegebene Verzeichnis wie das Standardverzeichnis zu.

<Informatica-Installationsverzeichnis>/services/shared/security

Wenn Sie die sichere Kommunikation für die Domäne aktivieren, enthält das Verzeichnis /secret den Schlüsselspeicher und die Truststore-Dateien für die standardmäßigen SSL-Zertifikate.

Zum Gewährleisten der Sicherheit der Verzeichnisse und Dateien beschränkt das Installationsprogramm den Zugriff auf die Verzeichnisse und die Dateien in den Verzeichnissen. Unter UNIX weist das

Installationsprogramm der Gruppe und dem Benutzerkonto, die als Eigentümer der Verzeichnisse und Dateien fungieren, bestimmte Berechtigungen zu.

Weitere Informationen über die den Verzeichnissen und Dateien zugewiesenen Berechtigungen finden Sie im *Informatica-Sicherheitshandbuch*.

Installieren der Informatica-Dienste im Grafikmodus

Sie können die Informatica-Dienste im Grafikmodus unter Windows installieren.

Wenn Sie das Vorinstallations-Systemprüfungstool (i10Pi) vor der Installation ausführen, legt das Installationsprogramm die Werte für bestimmte Felder (beispielsweise die Datenbankverbindung und die Domänenportnummern) basierend auf den während der Systemüberprüfung eingegebenen Daten fest.

Wenn unter Windows beim Ausführen der Datei „install.bat“ im Root-Verzeichnis Probleme auftreten, führen Sie folgende Datei aus: `<Verzeichnis der Installationsdateien>\server\install.exe`

Hinweis: Informatica empfiehlt, dass Sie die Informatica Services und den PowerCenter Client in verschiedenen Verzeichnissen installieren, weil bei einer Installation von Informatica Services und PowerCenter Client im selben Verzeichnis die Programmdateien deinstalliert werden, wenn Sie den PowerCenter Client deinstallieren.

Erstellen einer Domäne

Erstellen Sie eine Domäne, wenn Sie zum ersten Mal installieren oder Knoten in separaten Domänen verwalten möchten.

1. Melden Sie sich mit einem Systembenutzerkonto am Computer an.
2. Schließen Sie alle anderen Anwendungen.
3. Wechseln Sie in das Stammverzeichnis für die Installationsdateien und führen Sie die Datei „install.bat“ als Administrator aus.

   Klicken Sie zum Ausführen der Datei als Administrator mit der rechten Maustaste auf die Datei „install.bat“ und wählen Sie **Als Administrator ausführen** aus.

   Hinweis: Wenn Sie das Installationsprogramm nicht als Administrator ausführen, meldet der Windows-Systemadministrator möglicherweise Probleme, wenn Sie auf die Dateien im Informatica-Installationsverzeichnis zugreifen.

   Die Seite **Informatica 10.1.1 HotFix 1** wird angezeigt.
4. Wählen Sie **Informatica 10.1.1 HotFix 1 installieren** aus.

   Informatica stellt Dienstprogramme bereit, um die Installation der Informatica-Dienste zu vereinfachen. Führen Sie die folgenden Dienstprogramme vor der Installation von Informatica-Diensten aus:

   - Vorinstallations-Systemprüfungstool (i10Pi) Stellt sicher, dass der Computer, auf dem die Informatica-Dienste installiert werden, die Systemanforderungen für die Installation erfüllt.

     Weitere Informationen zum Ausführen des Vorinstallations-Systemprüfungstools (i10Pi) finden Sie unter “Ausführen des Vorinstallations-Systemprüfungstools (i10Pi)” auf Seite 91.

- Kerberos SPN-Formatgenerator von Informatica. Erstellt eine Liste der Kerberos-Dienstprinzipalnamen und Keytab-Dateinamen, die zum Ausführen von Informatica-Diensten in einem Netzwerk mit Kerberos-Authentifizierung benötigt werden.

  Weitere Informationen zum Ausführen des Kerberos SPN-Formatgenerators von Informatica finden Sie unter "Ausführen des Kerberos SPN-Formatgenerators von Informatica unter Windows" auf Seite 77.

Sie können das Installationsprogramm zum Ausführen der Dienstprogramme verwenden, bevor Sie die Informatica-Dienste installieren. Starten Sie nach dem Beenden eines Dienstprogramms das Installationsprogramm erneut, um das nächste Dienstprogramm auszuführen oder die Informatica-Dienste zu installieren.

5. Klicken Sie auf **Start**.
6. Lesen Sie die Bedingungen für die Informatica-Installation und das Toolkit zur Produktverwendung und wählen Sie **Ich stimme den Bedingungen zu** aus.

   Informatica DiscoveryIQ ist ein Produktnutzungstool, das Routineberichte über Datennutzung und Systemstatistiken an Informatica sendet. Nach der Installation und Konfiguration der Informatica-Domäne lädt Informatica DiscoveryIQ alle 15 Minuten Daten an Informatica hoch. Danach sendet die Domäne die Daten alle 30 Tage. Sie können die Verwendung von Statistiken im Administrator-Tool deaktivieren.
7. Klicken Sie auf **Weiter**.

   Auf der Seite **Installationsvoraussetzungen** werden die Installationsanforderungen angezeigt. Stellen Sie sicher, dass alle Voraussetzungen erfüllt sind, bevor Sie die Installation fortsetzen.
8. Klicken Sie auf **Weiter**.

   Die Seite **Lizenz- und Installationsverzeichnis** wird angezeigt.
9. Geben Sie den Informatica-Lizenzschlüssel und das Installationsverzeichnis ein.

   In der folgenden Tabelle werden der Lizenzschlüssel und das Verzeichnis beschrieben, die für die Installation der Informatica-Dienste angegeben werden:

Eigenschaft	Beschreibung
Lizenzschlüsseldatei	Pfad und Dateinamen des Informatica-Lizenzschlüssels.
Installationsverzeichnis	Absoluter Pfad für das Installationsverzeichnis. Das Installationsverzeichnis muss sich auf dem Computer befinden, auf dem Informatica installiert wird. Die Verzeichnisnamen im Pfad dürfen weder Leerzeichen noch die folgenden Sonderzeichen enthalten: `@ | * $ # ! % ( ) { } [ ]` **Hinweis:** Informatica empfiehlt die Verwendung alphanumerischer Zeichen im Installationsverzeichnispfad. Wenn Sie ein Sonderzeichen wie zum Beispiel á oder € verwenden, können unerwartete Ergebnisse während der Laufzeit auftreten.

10. Zum Konfigurieren der Informatica-Domäne für die Ausführung in einem Netzwerk mit Kerberos-Authentifizierung wählen Sie **Kerberos-Netzwerkauthentifizierung aktivieren** aus.
11. Klicken Sie auf **Weiter**.

    Wenn Sie die Kerberos-Netzwerkauthentifizierung aktiviert haben, wird die Seite **Netzwerksicherheit – Dienstprinzipalebene** angezeigt.
    Wenn Sie die Kerberos-Netzwerkauthentifizierung nicht aktivieren, wird die Seite **Vorinstallationsübersicht** angezeigt. Fahren Sie mit 16 fort

12. Wählen Sie auf der Seite **Netzwerksicherheit - Dienstprinzipalebene** die Ebene aus, auf die Sie die Kerberos-Dienstprinzipale für die Domäne festlegen möchten.

    In der folgenden Tabelle werden die Dienstprinzipalebenen beschrieben, die Sie auswählen können:

Ebene	Beschreibung
Prozessebene	Konfiguriert die Domäne für die Verwendung eines eindeutigen SPN und einer Keytab-Datei für jeden Knoten und jeden Anwendungsdienst auf einem Knoten. Die Anzahl der pro Knoten erforderlichen SPNs und Keytab-Dateien hängt von der Anzahl der Anwendungsdienstprozesse ab, die auf dem Knoten ausgeführt werden. Verwenden Sie die Prozessebenenoption für Datendomänen, die einen hohen Grad an Sicherheit erfordern, wie z. B. Produktionsdomänen.
Knotenebene	Konfiguriert die Domäne zur gemeinsamen Nutzung von SPNs und Keytab-Dateien auf einem Knoten. Diese Option erfordert jeweils einen SPN und eine Keytab-Datei für den Knoten und alle Anwendungsdienste, die auf dem Knoten ausgeführt werden. Sie erfordert außerdem einen separaten SPN und eine separate Keytab-Datei für alle HTTP-Prozesse auf dem Knoten. Verwenden Sie die Knotenebenenoption für Domänen, die keinen hohen Grad an Sicherheit erfordern, wie z. B. Test- und Entwicklungsdomänen.

13. Klicken Sie auf **Weiter**.

    Die Seite **Netzwerksicherheit – Kerberos-Authentifizierung** wird angezeigt.

14. Geben Sie die Domäne und die Keytab-Informationen ein, die für die Kerberos-Authentifizierung notwendig sind.

    In der folgenden Tabelle werden die Informatica-Domänen- und die Knoteninformationen beschrieben, die bereitgestellt werden müssen:

Eigenschaft	Beschreibung
Domänenname	Der Name der zu erstellenden Domäne. Der Name darf maximal 128 Zeichen umfassen und muss im 7-Bit-ASCII-Format vorliegen. Der Name darf weder Leerzeichen noch folgende Zeichen enthalten: ` % * + ; " ? , < > \ /
Knotenname	Name des zu erstellenden Knotens.
Knoten-Hostname	Vollständig qualifizierter Hostname oder die IP-Adresse des Computers, auf dem der Knoten erstellt werden soll. **Hinweis:** Der Hostname des Knotens darf keine Unterstriche (_) enthalten. Verwenden Sie nicht localhost. Der Hostname muss den Computer eindeutig kennzeichnen.

In der folgenden Tabelle werden der Kerberos-Bereich und die Keytab-Informationen beschrieben, die bereitgestellt werden müssen:

Eigenschaft	Beschreibung
Dienstbereichsname	Name des Kerberos-Bereichs, zu dem die Informatica-Domänendienste gehören. Der Bereichsname muss aus Großbuchstaben bestehen. Die Namen des Dienst- und Benutzerbereichs müssen übereinstimmen.
Benutzerbereichsname	Name des Kerberos-Bereichs, zu dem die Informatica-Domänenbenutzer gehören. Der Bereichsname muss aus Großbuchstaben bestehen. Die Namen des Dienst- und Benutzerbereichs müssen übereinstimmen.
Keytab-Verzeichnis	Verzeichnis, in dem alle Keytab-Dateien für die Informatica-Domäne gespeichert werden. Der Name einer Keytab-Datei in der Informatica-Domäne muss einem von Informatica festgelegten Format entsprechen.
Kerberos-Konfigurationsdatei	Pfad und Dateiname der Kerberos-Konfigurationsdatei. Informatica benötigt folgenden Namen für die Kerberos-Konfigurationsdatei: *krb5.conf*

Wichtig: Wenn Sie die Domäne zur Ausführung mit Kerberos-Authentifizierung konfigurieren, müssen der Domänen- und Knotenname sowie der Knoten-Hostname mit den Namen übereinstimmen, die beim Ausführen des Kerberos SPN-Formatgenerators von Informatica zum Erzeugen der SPNs und Keytab-Dateinamen angegeben wurden. Wenn Sie einen anderen Domänen-, Knoten- oder Hostnamen verwenden, erzeugen Sie den SPN und die Keytab-Dateinamen erneut und bitten Sie den Kerberos-Administrator, den neuen SPN zur Kerberos-Prinzipaldatenbank hinzuzufügen und die Keytab-Dateien zu erstellen.

15. Klicken Sie auf **Weiter**.

    Die Seite **Vorinstallationsübersicht** wird angezeigt.

16. Überprüfen Sie die Installationsinformationen und klicken Sie auf **Installieren**, um fortzufahren.

    Der Installer kopiert die Informatica-Dateien in das Installationsverzeichnis. Nach dem Kopieren der Dateien durch das Installationsprogramm wird die Seite **Domänenauswahl** angezeigt.

17. Wählen Sie **Eine Domäne erstellen** aus.

    Beim Erstellen einer Domäne übernimmt der zugehörige Knoten die Funktion eines Gateway-Knotens in der Domäne. Der Gateway-Knoten enthält einen Dienstmanager, der alle Domänenvorgänge verwaltet.

18. Um sichere Kommunikation zwischen den Diensten in der Domäne einzurichten, wählen Sie **Sichere Kommunikation für die Domäne aktivieren** aus.

    Wenn Sie sichere Kommunikation für die Domäne aktivieren, richtet das Installationsprogramm standardmäßig eine HTTPS-Verbindung für Informatica Administrator ein. Sie können auch ein Domänen-Konfigurations-Repository in einer sicheren Datenbank erstellen.

19. Wählen Sie zum Sichern der Verbindung zu Informatica Administrator **HTTPS für Informatica Administrator aktivieren** aus.

In der folgenden Tabelle werden die Eigenschaften beschrieben, die Sie für eine sichere Verbindung zum Administrator Tool einrichten:

Eigenschaft	Beschreibung
HTTPS für Informatica Administrator aktivieren	Wählen Sie diese Option zum Sichern der Verbindung zu Informatica Administrator. Deaktivieren Sie diese Option, um eine ungesicherte HTTP-Verbindung zu verwenden. Wenn sichere Kommunikation für die Domäne aktiviert ist, wird diese Option vom Installationsprogramm aktiviert. Sie können diese Option auch verwenden, wenn für die Domäne keine sichere Kommunikation aktiviert wurde.
Port	Der für die Kommunikation zwischen Informatica Administrator und dem Dienstmanager zu verwendende Port.
Vom Installer generierte Schlüsselspeicherdatei verwenden	Verwendung einer vom Installationsprogramm generierten selbstsignierten Schlüsselspeicherdatei. Das Installationsprogramm erstellt eine Schlüsselspeicherdatei mit dem Namen „Default.keystore“ am folgenden Speicherort: `<Informatica-Installationsverzeichnis>\tomcat\conf\`
Schlüsselspeicherdatei und Passwort eingeben	Verwendung einer von Ihnen erstellten Schlüsselspeicherdatei. Sie können eine Schlüsselspeicherdatei mit einem selbstsignierten Zertifikat oder einem von einer Zertifizierungsbehörde signierten Zertifikat verwenden.
Schlüsselspeicherpasswort	Ein Klartext-Passwort für die Schlüsselspeicherdatei. Bei Verwendung einer von Ihnen erstellten Schlüsselspeicherdatei erforderlich.
Schlüsselspeicherdatei	Pfad und Dateiname der Schlüsselspeicherdatei. Bei Verwendung einer von Ihnen erstellten Schlüsselspeicherdatei erforderlich.

20. Klicken Sie auf **Weiter**.

    Wenn Sie die Option **Sichere Kommunikation für die Domäne aktivieren** ausgewählt haben, wird die Seite **Domänensicherheit - Sichere Kommunikation** angezeigt.
    Wenn sichere Kommunikation für die Domäne nicht aktiviert wurde, wird die Seite **Domänen-Konfigurations-Repository** angezeigt. Fahren Sie mit Schritt 24 fort.

21. Geben Sie auf der Seite **Domänensicherheit – Sichere Kommunikation** an, ob die standardmäßigen SSL-Zertifikate von Informatica oder eigene SSL-Zertifikate zum Aktivieren sicherer Kommunikation in der Domäne verwendet werden sollen.

In der folgenden Tabelle werden die SSL-Zertifikatsoptionen zum Sichern der Informatica-Domäne beschrieben:

Option	Beschreibung
SSL-Standardzertifikatsdateien von Informatica verwenden	Verwenden Sie die von Informatica bereitgestellten SSL-Standardzertifikate. **Hinweis:** Wenn Sie kein SSL-Zertifikat bereitstellen, verwendet Informatica denselben privaten Standardschlüssel für alle Informatica-Installationen. Wenn Sie die von Informatica bereitgestellten standardmäßigen Schlüsselspeicher- und Truststore-Dateien verwenden, wird die Sicherheit Ihrer Domäne unter Umständen gefährdet. Um ein hohes Maß an Sicherheit für die Domäne zu gewährleisten, wählen Sie die Option zum Angeben des Speicherorts der SSL-Zertifikatsdateien aus.
Speicherort der SSL-Zertifikatsdateien angeben	Verwenden Sie von Ihnen bereitgestellte SSL-Zertifikate. Sie müssen den Speicherort der Schlüsselspeicher- und Truststore-Dateien angeben. Sie können ein selbstsigniertes Zertifikat oder ein von einer Zertifizierungsstelle ausgegebenes Zertifikat verwenden. Sie müssen SSL-Zertifikate im PEM-Format und in Java-Schlüsselspeicherdateien (JKS) bereitstellen. Informatica benötigt bestimmte Namen für die SSL-Zertifikatsdateien in der Informatica-Domäne. Sie müssen für alle Knoten in der Domäne dieselben SSL-Zertifikate verwenden. Speichern Sie die Truststore- und Schlüsselspeicherdateien in einem Verzeichnis, auf das alle Knoten in der Domäne zugreifen können, und geben Sie für alle Knoten in derselben Domäne dasselbe Schlüsselspeicherdatei- und Truststore-Datei-Verzeichnis an.

22. Wenn Sie die Sicherheitszertifikate bereitstellen, geben Sie den Speicherort und die Passwörter der Schlüsselspeicher- und Truststore-Dateien an.

    In der folgenden Tabelle werden die Parameter beschrieben, die für die SSL-Zertifikatsdateien eingegeben werden müssen:

Eigenschaft	Beschreibung
Schlüsselspeicherdatei-Verzeichnis	Verzeichnis, das die Schlüsselspeicherdateien enthält. Das Verzeichnis muss Dateien mit der Bezeichnung "infa_keystore.jks" und "infa_keystore.pem" enthalten.
Schlüsselspeicherpasswort	Passwort für den Schlüsselspeicher „infa_keystore.jks“.
Verzeichnis der Truststore-Datei	Verzeichnis, das die Truststore-Dateien enthält. Das Verzeichnis muss Dateien mit der Bezeichnung "infa_truststore.jks" und "infa_truststore.pem" enthalten.
Truststore-Passwort	Passwort für die Datei infa_truststore.jks.

23. Klicken Sie auf **Weiter**.

    Die Seite **Domänen-Konfigurations-Repository** wird angezeigt.

24. Geben Sie auf der Seite **Domänen-Konfigurations-Repository** die entsprechenden Datenbank- und Benutzerkontodaten für das Domänen-Konfigurations-Repository ein.

    Im Domänen-Konfigurations-Repository werden Metadaten für Domänenvorgänge und die Benutzerauthentifizierung gespeichert. Die Datenbank muss allen Gateway-Knoten in der Domäne zugänglich sein.

In der folgenden Tabelle sind die Eigenschaften beschrieben, die Sie für die Datenbank und das Benutzerkonto festlegen:

Eigenschaft	Beschreibung
Datenbanktyp	Datenbank für das Repository. Wählen Sie eine der folgenden Datenbanken aus: - Oracle - IBM DB2 - Microsoft SQL Server - Sybase ASE
Datenbankbenutzer-ID	Benutzerkonto für die Repository-Datenbank.
Benutzerpasswort	Das Passwort für das Datenbankbenutzerkonto.

Geben Sie bei Auswahl von IBM DB2 den Tablespace für die Repository-Tabellen an:

Eigenschaft	Beschreibung
Tablespace	Der Name des Tablespace, in dem die Tabellen erstellt werden sollen. Geben Sie einen Tablespace an, der die Anforderungen an die Seitengröße (pageSize) von 32768 Byte erfüllt. Wenn Sie in einer Datenbank mit einer einzigen Partition diese Option nicht auswählen, werden die Tabellen vom Installer im Standard-Tablespace erstellt. Wählen Sie in einer Datenbank mit mehreren Partitionen diese Option aus und geben Sie den Namen des Tablespace ein, der sich in der Katalogpartition der Datenbank befindet.

Geben Sie bei Auswahl von Microsoft SQL Server das Schema für die Repository-Tabellen und die Datenbankverbindung an:

Eigenschaft	Beschreibung
Schemaname	Name des Schemas, das die Repository-Tabellen enthält. Ist diese Option nicht aktiviert, werden die Tabellen vom Installationsprogramm im Standardschema erstellt.
Vertrauenswürdige Verbindung	Zeigt an, ob eine vertrauenswürdige Verbindung zu Microsoft SQL Server hergestellt werden soll. Die vertrauenswürdige Authentifizierung verwendet die Sicherheitsanmeldedaten des aktuellen Benutzers zur Herstellung der Verbindung zu Microsoft SQL Server. Ist diese Option nicht aktiviert, wird die Microsoft SQL Server-Authentifizierung verwendet.

Wenn Sie sichere Kommunikation für die Domäne aktiviert haben, können Sie das Domänen-Konfigurations-Repository in einer mit dem SSL-Protokoll gesicherten Datenbank erstellen. Zum Erstellen eines sicheren Domänenkonfigurations-Repositorys wählen Sie **Sichere Datenbank** aus und fahren Sie mit Schritt 26 fort.

Hinweis: Sie können keine sichere Verbindung zu einer Sybase-Datenbank konfigurieren.

25. Geben Sie die Verbindungsinformationen für die Datenbank ein.

Wenn Sie kein sicheres Domänenkonfigurations-Repository erstellen, können Sie die Verbindungseigenschaften für die JDBC-URL angeben oder die JDBC-Verbindungszeichenfolge bereitstellen.

- Um die Verbindungsdaten über die JDBC-URL einzugeben, wählen Sie **JDBC URL** aus, und geben Sie die Eigenschaften der Datenbankverbindung ein.
  In der folgenden Tabelle werden die JDBC-URL-Eigenschaften beschrieben, die Sie festlegen:

Eigenschaft	Beschreibung
Datenbankadresse	Der Hostname und die Portnummer für die Datenbank im Format `host_name:port`.
Datenbankdienstname	Dienst- oder Datenbankname: - Oracle: Geben Sie den Dienstnamen ein. - Microsoft SQL Server: Geben Sie den Datenbanknamen ein. - IBM DB2: Geben Sie den Dienstnamen ein. - Sybase ASE: Geben Sie den Datenbanknamen ein.
JDBC-Parameter	Optionale Parameter, die in der Datenbank-Verbindungszeichenfolge aufgenommen werden können. Mit den Parametern können die Datenbankvorgänge für die Datenbank optimiert werden. Überprüfen Sie die Gültigkeit der Parameterzeichenfolge. Das Installationsprogramm führt vor dem Hinzufügen der Parameterzeichenfolge zur JDBC-URL keine Überprüfung der Zeichenfolge durch. Ist diese Option nicht aktiviert, erstellt das Installationsprogramm die JDBC-URL ohne zusätzliche Parameter.

- Um die Verbindungsdaten mithilfe einer benutzerdefinierten JDBC-Verbindungszeichenfolge einzugeben, wählen Sie **Benutzerdefinierte JDBC-Verbindungszeichenfolge** aus und geben Sie die Verbindungszeichenfolge ein.

26. Wenn Sie die Option **Sichere Datenbank** zum Erstellen eines sicheren Domänenkonfigurations-Repositorys ausgewählt haben, geben Sie die Verbindungsinformationen unter Verwendung einer benutzerdefinierten JDBC-Verbindungszeichenfolge ein.

    Wenn Sie das Repository in einer sicheren Datenbank erstellen, müssen Sie die Truststore-Informationen für die Datenbank angeben. Außerdem müssen Sie eine JDBC-Verbindungszeichenfolge angeben, die die Sicherheitsparameter für die Datenbank enthält.

    In der folgenden Tabelle werden die Eigenschaften beschrieben, die für eine sichere Datenbank eingerichtet werden müssen:

Eigenschaft	Beschreibung
Datenbank-Truststore-Datei	Pfad und Dateiname der Truststore-Datei für die sichere Datenbank.
Datenbank-Truststore-Passwort	Passwort für die TrustStore-Datei.
Benutzerdefinierte JDBC-Verbindungszeichenfolge	JDBC-Verbindungszeichenfolge zum Herstellen einer Verbindung mit der sicheren Datenbank, einschließlich des Hostnamens, der Portnummer und der Sicherheitsparameter für die Datenbank.

    Informationen zu den Sicherheitsparametern, die in die JDBC-Verbindung für eine sichere Datenbank aufgenommen werden müssen, finden Sie unter "Verbindungszeichenfolge für eine sichere Datenbank" auf Seite 71.

27. Klicken Sie auf **Verbindung testen**, um zu überprüfen, ob Sie eine Verbindung zur Datenbank herstellen können, und anschließend auf **OK**, um fortzufahren.
28. Klicken Sie auf **Weiter**.

    Die Seite **Domänensicherheit – Verschlüsselungsschlüssel** wird geöffnet.
29. Geben Sie das Schlüsselwort und das Verzeichnis für den Verschlüsselungsschlüssel der Informatica-Domäne ein.

    In der folgenden Tabelle werden die Verschlüsselungsschlüsselparameter beschrieben, die Sie angeben müssen:

Eigenschaft	Beschreibung
Schlüsselwort	Schlüsselwort zum Erstellen eines benutzerdefinierten Verschlüsselungsschlüssels für die Sicherung vertraulicher Daten in der Domäne. Das Schlüsselwort muss die folgenden Kriterien erfüllen: - Hat eine Länge von 8 bis 20 Zeichen - Enthält mindestens einen Großbuchstaben - Enthält mindestens einen Kleinbuchstaben - Enthält mindestens eine Zahl - Enthält keine Leerzeichen Der Verschlüsselungsschlüssel wird basierend auf dem Schlüsselwort erstellt, das Sie beim Erstellen der Informatica-Domäne angeben.
Verzeichnis des Verschlüsselungsschlüssels	Verzeichnis, in dem der Verschlüsselungsschlüssel für die Domäne gespeichert werden soll. Standardmäßig wird der Verschlüsselungsschlüssel in folgendem Verzeichnis erstellt: `<Informatica-Installationsverzeichnis>/isp/config/keys`.

30. Klicken Sie auf **Weiter**.

    Die Seite **Domäne und Knotenkonfiguration** wird angezeigt.
31. Geben Sie die Informationen für die Domäne und den Knoten ein, die Sie erstellen möchten.

    In der folgenden Tabelle werden die Eigenschaften beschrieben, die Sie für den Domänen- und Gateway-Knoten festlegen:

Eigenschaft	Beschreibung
Domänenname	Name der zu erstellenden Informatica-Domäne. Der Standardname der Domäne lautet Domain_<MachineName>. Der Name darf maximal 128 Zeichen umfassen und muss im 7-Bit-ASCII-Format vorliegen. Der Name darf weder Leerzeichen noch folgende Zeichen enthalten: ` % * + ; " ? , < > \ /
Knotenname	Name des zu erstellenden Knotens.

Eigenschaft	Beschreibung
Knoten-Hostname	Hostname oder IP-Adresse des Computers, auf dem der Knoten erstellt werden soll. Wenn der Computer nur einen Netzwerknamen aufweist, verwenden Sie den Standardhostnamen. Wenn der Computer mehrere Netzwerknamen aufweist, können Sie den Standardhostnamen ändern und einen alternativen Netzwerknamen verwenden. **Hinweis:** Der Hostname des Knotens darf keine Unterstriche (_) enthalten. Verwenden Sie nicht localhost. Der Hostname muss den Computer eindeutig kennzeichnen.
Knoten-Portnummer	Die Portnummer für den Knoten. Die Standard-Portnummer für den Knoten lautet 6005. Wenn die Portnummer auf dem Rechner nicht verfügbar ist, wird die nächste verfügbare Portnummer angezeigt.
Domänenbenutzername	Benutzername für den Domänenadministrator. Sie können diesen Benutzernamen für die Erstanmeldung bei Informatica Administrator verwenden. Beachten Sie folgende Richtlinien: - Beim Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden und er darf nicht mehr als 128 Zeichen umfassen. - Der Name darf weder Tabulatoren und Zeilenendzeichen noch die folgenden Sonderzeichen enthalten: % * + / ? ; < > - Der Name kann ein ASCII-Leerzeichen enthalten, jedoch nicht als erstes oder letztes Zeichen. Alle anderen Leerzeichen sind nicht zulässig.
Domänenpasswort	Das Passwort für den Domänenadministrator. Das Passwort muss mindestens zwei Zeichen und darf bis zu 16 Zeichen enthalten. Nicht verfügbar, wenn Sie die Informatica-Domäne zur Ausführung in einem Netzwerk mit Kerberos-Authentifizierung konfigurieren.
Passwort bestätigen	Geben Sie das Passwort zur Bestätigung erneut ein. Nicht verfügbar, wenn Sie die Informatica-Domäne zur Ausführung in einem Netzwerk mit Kerberos-Authentifizierung konfigurieren.

32. Zur Konfiguration der Unterstützung von Single Sign-On (SSO) auf der Basis der Security Assertion Markup Language (SAML) für webbasierte Informatica-Anwendungen in einer Informatica-Domäne aktivieren Sie die **SAML-Authentifizierung**.

    Hinweis: Wenn Sie die Kerberos-Netzwerkauthentifizierung aktiviert haben, können Sie die SAML-Authentifizierung nicht konfigurieren.

33. Geben Sie die URL des Identitäts-Providers für die Domäne ein.

34. Wählen Sie zur Anzeige der vom Installationsprogramm zugewiesenen Standardports für die Domänen- und Knotenkomponenten die Option **Anzeigen der Seite „Erweiterte Port-Konfiguration“** aus.

    Wenn Sie die Seite für die Portkonfiguration öffnen, werden vom Installationsprogramm die der Domäne und dem Knoten zugewiesenen Standardportnummern angezeigt. Sie können die Portnummern ändern und einen anderen Portnummernbereich für die Anwendungsdienstprozesse angeben. Wenn Sie die Seite für die Portkonfiguration nicht öffnen, zeigt das Installationsprogramm die Standardportnummern nicht an und die zugewiesenen Portnummern können nicht geändert werden.

35. Wählen Sie zum Erstellen eines Modellrepository- und Datenintegrationsdiensts während der Installation die Option **Modellrepository-Dienst und Datenintegrationsdienst konfigurieren** aus.

    Wenn Sie die Dienste konfigurieren, erstellt das Installationsprogramm einen Modellrepository- und einen Datenintegrationsdienst in der neuen Domäne. Sie müssen die Datenbank für das Modellrepository

angeben und die Verbindung zum Datenintegrationsdienst konfigurieren. Standardmäßig startet das Installationsprogramm die Dienste nach Abschluss der Installation.

Wenn Sie die Dienste nicht konfigurieren, erstellt das Installationsprogramm weder einen Modellrepository- noch einen Datenintegrationsdienst in der neuen Domäne. Sie können die Dienste im Administrator Tool nach der Installation erstellen.

36. Klicken Sie auf **Weiter**.

    Wenn Sie angegeben haben, dass die Seite für die Portkonfiguration angezeigt werden soll, zeigt das Installationsprogramm die Seite **Portkonfiguration** an.

    Wenn Sie nicht angegeben haben, dass die Seite für die Portkonfiguration angezeigt werden soll, zeigt das Installationsprogramm die Seite **Windows-Dienstkonfiguration** an. Fahren Sie mit Schritt 39 fort.

37. Geben Sie auf der Seite **Portkonfiguration** die Portnummern für den Dienstmanager der Domäne und die Dienstprozesse ein, die auf dem Knoten ausgeführt werden.

    Stellen Sie sicher, dass die eingegebenen Portnummern nicht bereits von anderen Anwendungen verwendet werden.
    In der folgenden Tabelle werden die Ports beschrieben, die von Ihnen festgelegt werden können:

Port	Beschreibung
Dienstmanager-Port	Portnummer, die vom Dienstmanager auf dem Knoten verwendet wird. Der Dienstmanager überwacht eingehende Verbindungsanfragen auf diesem Port. Clientanwendungen verwenden diesen Port zur Kommunikation mit den Diensten in dieser Domäne. Die Informatica-Befehlszeilenprogramme verwenden diesen Port für die Kommunikation mit der Domäne. Dies ist auch der Port für den JDBC-/ODBC-Treiber des SQL-Datendiensts. Standardwert ist 6006.
Schließungsport des Dienstmanagers	Portnummer, die das Herunterfahren des Servers für den Dienstmanager der Domäne steuert. An diesem Port wartet der Dienstmanager auf Ausschaltbefehle. Standardwert ist 6007.
Informatica Administrator-Port	Portnummer von Informatica Administrator. Standardwert ist 6008.
Informatica Administrator-Schließungsport	Portnummer, die das Herunterfahren des Servers für Informatica Administrator steuert. Informatica Administrator überwacht Befehle zum Herunterfahren auf diesem Port. Standardwert ist 6009.
Niedrigste Portnummer	Niedrigste Portnummer des dynamischen Portnummernbereichs, die den Anwendungsdienstprozessen, die auf diesem Knoten laufen, zugewiesen werden kann. Standardwert ist 6014.
Höchste Portnummer	Höchste Portnummer des dynamischen Portnummernbereichs, die den Anwendungsdienstprozessen, die auf diesem Knoten laufen, zugewiesen werden kann. Standardwert ist 6114.

38. Klicken Sie auf **Weiter**.

    Im Installationsprogramm wird die Seite **Windows-Dienstkonfiguration** angezeigt.

39. Geben Sie auf der Seite **Windows-Dienstkonfiguration** an, ob der Windows-Dienst unter einem anderen Benutzerkonto ausgeführt werden soll.

    Das Installationsprogramm erstellt einen Dienst zum Starten von Informatica. Der Dienst wird standardmäßig unter demselben Benutzerkonto ausgeführt wie dem, das für die Installation verwendet wurde. Sie können den Windows-Dienst unter einem anderen Benutzerkonto ausführen.

In der folgenden Tabelle werden die Eigenschaften beschrieben, die zum Ausführen von Informatica unter einem anderen Benutzerkonto eingerichtet werden:

Eigenschaft	Beschreibung
Informatica unter einem anderen Benutzerkonto ausführen	Gibt an, ob der Windows-Dienst unter einem anderen Benutzerkonto ausgeführt werden soll.
Benutzername	Das Benutzerkonto, unter dem der Informatica-Windows-Dienst ausgeführt werden soll. Verwenden Sie das folgende Format: `<Domänenname>\<Benutzerkonto>` Dieses Benutzerkonto muss „Aktion“ als Betriebssystemberechtigung aufweisen.
Passwort	Das Passwort zum Benutzerkonto, unter dem der Informatica-Windows-Dienst ausgeführt werden soll.

40. Klicken Sie auf **Weiter**.

    Wenn Sie entschieden haben, die Informatica-Anwendungsdienste zu konfigurieren, wird im Installationsprogramm die Seite **Datenbank des Modellrepository-Diensts** angezeigt.

    Wenn Sie die Dienste nicht erstellt haben, wird im Installationsprogramm die Seite **Installationsabschlussbericht** angezeigt. Auf der Seite **Installationsabschlussbericht** wird angezeigt, ob die Installation erfolgreich abgeschlossen wurde. Fahren Sie mit Schritt 49 fort.

41. Geben Sie auf der Seite **Datenbank des Modellrepository-Diensts** die Datenbank- und Benutzerkontoinformationen für das Modellrepository ein.

    In der folgenden Tabelle sind die Eigenschaften beschrieben, die Sie für die Datenbank und das Benutzerkonto festlegen:

Eigenschaft	Beschreibung
Datenbanktyp	Datenbank für das Repository. Wählen Sie eine der folgenden Datenbanken aus: - Oracle - IBM DB2 - Microsoft SQL Server - Sybase ASE
Datenbankbenutzer-ID	Benutzerkonto für die Repository-Datenbank.
Benutzerpasswort	Das Passwort für das Datenbankbenutzerkonto.

Geben Sie bei Auswahl von IBM DB2 den Tablespace für die Repository-Tabellen an:

Eigenschaft	Beschreibung
Tablespace	Der Name des Tablespace, in dem die Tabellen erstellt werden sollen. Geben Sie einen Tablespace an, der die Anforderungen an die Seitengröße (pageSize) von 32768 Byte erfüllt. Wenn Sie in einer Datenbank mit einer einzigen Partition diese Option nicht auswählen, werden die Tabellen vom Installer im Standard-Tablespace erstellt. Wählen Sie in einer Datenbank mit mehreren Partitionen diese Option aus und geben Sie den Namen des Tablespace ein, der sich in der Katalogpartition der Datenbank befindet.

Geben Sie bei Auswahl von Microsoft SQL Server das Schema für die Repository-Tabellen und die Datenbankverbindung an:

Eigenschaft	Beschreibung
Schemaname	Name des Schemas, das die Repository-Tabellen enthält. Ist diese Option nicht aktiviert, werden die Tabellen vom Installationsprogramm im Standardschema erstellt.
Vertrauenswürdige Verbindung	Zeigt an, ob eine vertrauenswürdige Verbindung zu Microsoft SQL Server hergestellt werden soll. Die vertrauenswürdige Authentifizierung verwendet die Sicherheitsanmeldedaten des aktuellen Benutzers zur Herstellung der Verbindung zu Microsoft SQL Server. Ist diese Option nicht aktiviert, wird die Microsoft SQL Server-Authentifizierung verwendet.

Wenn Sie sichere Kommunikation für die Domäne aktiviert haben, können Sie das Modellrepository in einer mit dem SSL-Protokoll gesicherten Datenbank erstellen. Zum Erstellen eines sicheren Modellrepositorys fahren Sie mit Schritt 43 fort.

42. Geben Sie die Verbindungsinformationen für die Datenbank ein.

    Wenn Sie kein sicheres Modellrepository erstellen, können Sie die Verbindungseigenschaften für die JDBC-URL angeben oder die JDBC-Verbindungszeichenfolge bereitstellen.

    - Um die Verbindungsdaten mithilfe der JDBC-URL einzugeben, wählen Sie **JDBC-URL** aus und geben Sie die Eigenschaften der Datenbankverbindung ein.

In der folgenden Tabelle werden die JDBC-URL-Eigenschaften beschrieben, die Sie festlegen:

Eigenschaft	Beschreibung
Datenbankadresse	Der Hostname und die Portnummer für die Datenbank im Format `host_name:port`.
Datenbankdienstname	Dienst- oder Datenbankname: - Oracle: Geben Sie den Dienstnamen ein. - Microsoft SQL Server: Geben Sie den Datenbanknamen ein. - IBM DB2: Geben Sie den Dienstnamen ein. - Sybase ASE: Geben Sie den Datenbanknamen ein.
JDBC-Parameter	Optionale Parameter, die in der Datenbank-Verbindungszeichenfolge aufgenommen werden können. Mit den Parametern können die Datenbankvorgänge für die Datenbank optimiert werden. Überprüfen Sie die Gültigkeit der Parameterzeichenfolge. Das Installationsprogramm führt vor dem Hinzufügen der Parameterzeichenfolge zur JDBC-URL keine Überprüfung der Zeichenfolge durch. Ist diese Option nicht aktiviert, erstellt das Installationsprogramm die JDBC-URL ohne zusätzliche Parameter.

- Um die Verbindungsdaten mithilfe einer benutzerdefinierten JDBC-Verbindungszeichenfolge einzugeben, wählen Sie **Benutzerdefinierte JDBC-Verbindungszeichenfolge** aus und geben Sie die Verbindungszeichenfolge ein.

  IBM DB2

  ```
  jdbc:Informatica:db2://host_name:port_no;DatabaseName=
  ```

  Oracle

  ```
  jdbc:Informatica:oracle://host_name:port_no;ServiceName=
  ```

  Microsoft SQL Server

  ```
  jdbc:Informatica:sqlserver://host_name:port_no;SelectMethod=cursor;DatabaseName=
  ```

  Stellen Sie sicher, dass die Verbindungszeichenfolge alle vom Datenbanksystem benötigten Verbindungsparameter enthält.

43. Wählen Sie zum Erstellen eines sicheren Modellrepositorys die Option **Sichere Datenbank** aus.

    Wenn Sie das Repository in einer sicheren Datenbank erstellen, müssen Sie die Truststore-Informationen für die Datenbank angeben. Außerdem müssen Sie eine JDBC-Verbindungszeichenfolge angeben, die die Sicherheitsparameter für die Datenbank enthält.

In der folgenden Tabelle werden die Eigenschaften beschrieben, die für eine sichere Datenbank eingerichtet werden müssen:

Eigenschaft	Beschreibung
Datenbank-Truststore-Datei	Pfad und Dateiname der Truststore-Datei für die sichere Datenbank.
Datenbank-Truststore-Passwort	Passwort für die TrustStore-Datei.
Benutzerdefinierte JDBC-Verbindungszeichenfolge	JDBC-Verbindungszeichenfolge zum Herstellen einer Verbindung mit der sicheren Datenbank, einschließlich des Hostnamens, der Portnummer und der Sicherheitsparameter für die Datenbank.

Informationen zu den Sicherheitsparametern, die in die JDBC-Verbindung für eine sichere Datenbank aufgenommen werden müssen, finden Sie unter "Verbindungszeichenfolge für eine sichere Datenbank" auf Seite 71.

44. Klicken Sie auf **Verbindung testen**, um zu überprüfen, ob Sie eine Verbindung zur Datenbank herstellen können, und anschließend auf **OK**, um fortzufahren.
45. Klicken Sie auf **Weiter**.
46. Geben Sie auf der Seite **Dienstparameter** den Namen des Modellrepository-Diensts ein und konfigurieren Sie die Eigenschaften des Datenintegrationsdiensts.

    In der folgenden Tabelle werden die einzurichtenden Dienstparameter beschrieben:

Port	Beschreibung
Name des Modellrepository-Diensts	Name des Modellrepository-Diensts, der in der Informatica-Domäne erstellt wird.
Name des Datenintegrationsdiensts	Name des Modellrepository-Diensts, der in der Informatica-Domäne erstellt wird.
HTTP-Protokolltyp	Typ der Verbindung zum Datenintegrationsdienst. Wählen Sie eine der folgenden Optionen aus: - HTTP. Erfordert, dass der Dienst eine HTTP-Verbindung benutzt. - HTTPS. Erfordert, dass der Dienst eine sichere HTTP-Verbindung benutzt. - HTTP&HTTPS. In Anfragen an den Dienst kann entweder eine HTTP- oder eine HTTPS-Verbindung verwendet werden.
HTTP-Port	Portnummer für den Datenintegrationsdienst. Standardwert ist 6030.

47. Geben Sie bei Auswahl einer HTTPS-Verbindung an, ob die SSL-Standardzertifikate von Informatica oder Ihre SSL-Zertifikate verwendet werden sollen, um eine sichere Verbindung zum Datenintegrationsdienst herzustellen.

In der folgenden Tabelle werden die SSL-Zertifikatsoptionen zum Sichern des Datenintegrationsdiensts beschrieben:

Option	Beschreibung
SSL-Standardzertifikatsdateien von Informatica verwenden	Verwenden Sie die von Informatica bereitgestellten SSL-Standardzertifikate. **Hinweis:** Wenn Sie kein SSL-Zertifikat bereitstellen, verwendet Informatica denselben privaten Standardschlüssel für alle Informatica-Installationen. Wenn Sie die von Informatica bereitgestellten standardmäßigen Schlüsselspeicher- und Truststore-Dateien verwenden, wird die Sicherheit Ihrer Domäne unter Umständen gefährdet. Um ein hohes Maß an Sicherheit für die Domäne zu gewährleisten, wählen Sie die Option zum Angeben des Speicherorts der SSL-Zertifikatsdateien aus.
Speicherort der SSL-Zertifikatsdateien eingeben	Verwenden Sie von Ihnen bereitgestellte SSL-Zertifikate. Sie müssen den Speicherort der Schlüsselspeicher- und Truststore-Dateien angeben.

Wenn Sie das Zertifikat bereitstellen, geben Sie den Speicherort und die Passwörter der Schlüsselspeicher- und der Truststore-Dateien an.

In der folgenden Tabelle werden die Parameter beschrieben, die für die SSL-Zertifikatsdateien eingegeben werden müssen:

Eigenschaft	Beschreibung
Schlüsselspeicherdatei	Erforderlich. Pfad und Dateiname der Schlüsselspeicherdatei, die die privaten Schlüssel und SSL-Zertifikate für die Datenbank enthält.
Schlüsselspeicherpasswort	Erforderlich. Passwort der Schlüsselspeicherdatei für die sichere Datenbank.
Truststore-Datei	Erforderlich. Pfad und Dateiname der Truststore-Datei, die den öffentlichen Schlüssel für die Datenbank enthält.
Truststore-Passwort	Erforderlich. Passwort der Truststore-Datei für die sichere Datenbank.

48. Klicken Sie auf **Weiter**.

    Das Installationsprogramm erstellt den Modellrepository-Dienst sowie den Datenintegrationsdienst und startet die Dienste.

    Auf der Seite **Installationsabschlussbericht** wird angezeigt, ob die Installation erfolgreich abgeschlossen wurde. Der Bericht zeigt außerdem den Status der installierten Komponenten und deren Konfiguration an.

49. Klicken Sie zum Beenden des Installationsprogramms auf **Fertig**.

In den Dateien finden Sie weitere Informationen über die vom Installationsprogramm ausgeführten Aufgaben und die Konfigurationseigenschaften der installierten Komponenten.

Beitreten zu einer Domäne

Sie können eine Verknüpfung zu einer Domäne herstellen, wenn Sie eine Installation auf mehreren Computern vornehmen und eine Domäne auf einem anderen Computer erstellt haben.

1. Melden Sie sich mit einem Systembenutzerkonto am Computer an.
2. Schließen Sie alle anderen Anwendungen.

3. Wechseln Sie in das Stammverzeichnis für die Installationsdateien und führen Sie die Datei „install.bat“ als Administrator aus.

   Klicken Sie zum Ausführen der Datei als Administrator mit der rechten Maustaste auf die Datei „install.bat“ und wählen Sie **Als Administrator ausführen** aus.

   Hinweis: Wenn Sie das Installationsprogramm nicht als Administrator ausführen, meldet der Windows-Systemadministrator möglicherweise Probleme, wenn Sie auf die Dateien im Informatica-Installationsverzeichnis zugreifen.

   Die Seite **Informatica 10.1.1 HotFix 1** wird angezeigt.

4. Wählen Sie **Informatica 10.1.1 HotFix 1 installieren** aus.

   Informatica stellt Dienstprogramme bereit, um die Installation der Informatica-Dienste zu vereinfachen. Führen Sie die folgenden Dienstprogramme vor der Installation von Informatica-Diensten aus:

   - Vorinstallations-Systemprüfungstool (i10Pi) Stellt sicher, dass der Computer, auf dem die Informatica-Dienste installiert werden, die Systemanforderungen für die Installation erfüllt.

     Weitere Informationen zum Ausführen des Vorinstallations-Systemprüfungstools (i10Pi) finden Sie unter “Ausführen des Vorinstallations-Systemprüfungstools (i10Pi)” auf Seite 91.

   - Kerberos SPN-Formatgenerator von Informatica. Erstellt eine Liste der Kerberos-Dienstprinzipalnamen und Keytab-Dateinamen, die zum Ausführen von Informatica-Diensten in einem Netzwerk mit Kerberos-Authentifizierung benötigt werden.

     Wenn Sie einer Domäne beitreten möchten, die Kerberos-Authentifizierung verwendet, müssen Sie die Dienstprinzipalnamen und Keytab-Dateien für den von Ihnen erstellten Knoten und den Dienst erzeugen, der auf dem Knoten ausgeführt wird. Weitere Informationen zum Ausführen des Kerberos SPN-Formatgenerators von Informatica finden Sie unter “Ausführen des Kerberos SPN-Formatgenerators von Informatica unter Windows” auf Seite 77.

   Sie können das Installationsprogramm zum Ausführen der Dienstprogramme verwenden, bevor Sie die Informatica-Dienste installieren. Starten Sie nach dem Beenden eines Dienstprogramms das Installationsprogramm erneut, um das nächste Dienstprogramm auszuführen oder die Informatica-Dienste zu installieren.

5. Klicken Sie auf **Start**.

6. Wählen Sie **Informatica 10.1.1 HotFix 1 installieren** aus.

7. Lesen Sie die Bedingungen für die Informatica-Installation und das Toolkit zur Produktverwendung und wählen Sie **Ich stimme den Bedingungen zu** aus.

   Informatica DiscoveryIQ ist ein Produktnutzungstool, das Routineberichte über Datennutzung und Systemstatistiken an Informatica sendet. Nach der Installation und Konfiguration der Informatica-Domäne lädt Informatica DiscoveryIQ alle 15 Minuten Daten an Informatica hoch. Danach sendet die Domäne die Daten alle 30 Tage. Sie können die Verwendung von Statistiken im Administrator-Tool deaktivieren.

8. Klicken Sie auf **Weiter**.

   Die Seite **Installationsvoraussetzungen** zeigt die Installationsanforderungen an. Stellen Sie sicher, dass alle Voraussetzungen erfüllt sind, bevor Sie die Installation fortsetzen.

9. Klicken Sie auf **Weiter**.

   Die Seite **Lizenz- und Installationsverzeichnis** wird angezeigt.

10. Geben Sie den Informatica-Lizenzschlüssel und das Installationsverzeichnis ein.

In der folgenden Tabelle werden der Lizenzschlüssel und das Verzeichnis beschrieben, die für die Installation der Informatica-Dienste angegeben werden:

Eigenschaft	Beschreibung
Lizenzschlüsseldatei	Pfad und Dateinamen des Informatica-Lizenzschlüssels.
Installationsverzeichnis	Absoluter Pfad für das Installationsverzeichnis. Das Installationsverzeichnis muss sich auf dem Computer befinden, auf dem Informatica installiert wird. Die Verzeichnisnamen im Pfad dürfen weder Leerzeichen noch die folgenden Sonderzeichen enthalten: `@ | * $ # ! % ( ) { } [ ]` **Hinweis:** Informatica empfiehlt die Verwendung alphanumerischer Zeichen im Installationsverzeichnispfad. Wenn Sie ein Sonderzeichen wie zum Beispiel á oder € verwenden, können unerwartete Ergebnisse während der Laufzeit auftreten.

11. Um einer in einem Netzwerk mit Kerberos-Authentifizierung ausgeführten Informatica-Domäne beizutreten, wählen Sie **Kerberos-Netzwerkauthentifizierung** aus.
12. Klicken Sie auf **Weiter**.

    Wenn Sie die Kerberos-Netzwerkauthentifizierung aktiviert haben, wird die Seite **Netzwerksicherheit – Dienstprinzipalebene** angezeigt.
    Wenn Kerberos-Netzwerkauthentifizierung nicht aktiviert wurde, wird die Seite **Vorinstallationsübersicht** angezeigt. Fahren Sie mit Schritt 16 fort
13. Wählen Sie auf der Seite **Netzwerksicherheit – Dienstprinzipalebene** die Dienstprinzipalebene der Domäne aus, der Sie beitreten möchten.

    Hinweis: Alle Knoten in der Domäne müssen die gleiche Dienstprinzipalebene verwenden. Wenn Sie einen Knoten zu einer Domäne hinzufügen, wählen Sie die gleiche Dienstprinzipalebene aus, die vom Gateway-Knoten in der Domäne verwendet wird.

    In der folgenden Tabelle werden die Dienstprinzipalebenen beschrieben, die Sie auswählen können:

Ebene	Beschreibung
Prozessebene	Konfiguriert die Domäne für die Verwendung eines eindeutigen SPN und einer Keytab-Datei für jeden Knoten und jeden Anwendungsdienst auf einem Knoten. Die Anzahl der pro Knoten erforderlichen SPNs und Keytab-Dateien hängt von der Anzahl der Anwendungsdienstprozesse ab, die auf dem Knoten ausgeführt werden. Verwenden Sie die Prozessebenenoption für Datendomänen, die einen hohen Grad an Sicherheit erfordern, wie z. B. Produktionsdomänen.
Knotenebene	Konfiguriert die Domäne zur gemeinsamen Nutzung von SPNs und Keytab-Dateien auf einem Knoten. Diese Option erfordert jeweils einen SPN und eine Keytab-Datei für den Knoten und alle Anwendungsdienste, die auf dem Knoten ausgeführt werden. Sie erfordert außerdem einen separaten SPN und eine separate Keytab-Datei für alle HTTP-Prozesse auf dem Knoten. Verwenden Sie die Knotenebenenoption für Domänen, die keinen hohen Grad an Sicherheit erfordern, wie z. B. Test- und Entwicklungsdomänen.

14. Klicken Sie auf **Weiter**.

    Die Seite **Netzwerksicherheit – Kerberos-Authentifizierung** wird angezeigt.

15. Geben Sie die Domäne und die Keytab-Informationen ein, die für die Kerberos-Authentifizierung notwendig sind.

    In der folgenden Tabelle werden die Informationen beschrieben, die Sie über die Domäne, der Sie beitreten möchten, und über den während der Installation zu erstellenden Knoten bereitstellen müssen:

Eigenschaft	Beschreibung
Domänenname	Der Name der zu verknüpfenden Domäne. Der Name darf maximal 128 Zeichen umfassen und muss im 7-Bit-ASCII-Format vorliegen. Der Name darf weder Leerzeichen noch folgende Zeichen enthalten: ` % * + ; " ? , < > \ /
Knotenname	Name des zu erstellenden Knotens.
Knoten-Hostname	Vollständig qualifizierter Hostname oder die IP-Adresse des Computers, auf dem der Knoten erstellt werden soll. **Hinweis:** Der Hostname des Knotens darf keine Unterstriche (_) enthalten. Verwenden Sie nicht localhost. Der Hostname muss den Computer eindeutig kennzeichnen.

    In der folgenden Tabelle werden der Kerberos-Bereich und die Keytab-Informationen beschrieben, die bereitgestellt werden müssen:

Eigenschaft	Beschreibung
Dienstbereichsname	Name des Kerberos-Bereichs, zu dem die Informatica-Domänendienste gehören. Der Bereichsname muss aus Großbuchstaben bestehen. Die Namen des Dienst- und Benutzerbereichs müssen übereinstimmen.
Benutzerbereichsname	Name des Kerberos-Bereichs, zu dem die Informatica-Domänenbenutzer gehören. Der Bereichsname muss aus Großbuchstaben bestehen. Die Namen des Dienst- und Benutzerbereichs müssen übereinstimmen.
Keytab-Verzeichnis	Verzeichnis, in dem alle Keytab-Dateien für die Informatica-Domäne gespeichert werden. Der Name einer Keytab-Datei in der Informatica-Domäne muss einem von Informatica festgelegten Format entsprechen.
Kerberos-Konfigurationsdatei	Pfad und Dateiname der Kerberos-Konfigurationsdatei. Informatica benötigt folgenden Namen für die Kerberos-Konfigurationsdatei: *krb5.conf*

16. Klicken Sie auf **Weiter**.

    Die Seite **Vorinstallationsübersicht** wird angezeigt.

17. Überprüfen Sie die Installationsinformationen und klicken Sie auf **Installieren**, um fortzufahren.

    Der Installer kopiert die Informatica-Dateien in das Installationsverzeichnis. Nach dem Kopieren der Dateien durch das Installationsprogramm wird die Seite **Domänenauswahl** angezeigt.

18. Wählen Sie **Eine Domäne anfügen** aus.

19. Geben Sie an, ob für die anzufügende Domäne sichere Kommunikation aktiviert wurde.

    Zum Anfügen einer Domäne mit aktivierter sicherer Kommunikation wählen Sie **Sichere Domäne anfügen** aus. Zum Anfügen einer Domäne ohne aktivierte sichere Kommunikation löschen Sie die Option.

20. Wählen Sie den Knotentyp aus, den Sie erstellen möchten.

Wählen Sie **Diesen Knoten als Gateway konfigurieren** aus, um einen Gateway-Knoten zu erstellen. Deaktivieren Sie diese Option, wenn Sie einen Worker-Knoten erstellen möchten.

Wenn Sie den Knoten als Gateway konfigurieren, können Sie eine sichere Verbindung zu Informatica Administrator aktivieren.

21. Wählen Sie zum Sichern der Verbindung zu Informatica Administrator **HTTPS für Informatica Administrator aktivieren** aus.

    In der folgenden Tabelle werden die Eigenschaften beschrieben, die Sie für eine sichere Verbindung zum Administrator Tool einrichten:

Eigenschaft	Beschreibung
HTTPS für Informatica Administrator aktivieren	Wählen Sie diese Option zum Sichern der Verbindung zu Informatica Administrator. Deaktivieren Sie diese Option, um eine ungesicherte HTTP-Verbindung zu verwenden. Wenn sichere Kommunikation für die Domäne aktiviert ist, wird diese Option vom Installationsprogramm aktiviert. Sie können diese Option auch verwenden, wenn für die Domäne keine sichere Kommunikation aktiviert wurde.
Port	Der für die Kommunikation zwischen Informatica Administrator und dem Dienstmanager zu verwendende Port.
Vom Installer generierte Schlüsselspeicherdatei verwenden	Verwendung einer vom Installationsprogramm generierten selbstsignierten Schlüsselspeicherdatei. Das Installationsprogramm erstellt eine Schlüsselspeicherdatei mit dem Namen „Default.keystore“ am folgenden Speicherort: `<Informatica-Installationsverzeichnis>\tomcat\conf\`
Schlüsselspeicherdatei und Passwort eingeben	Verwendung einer von Ihnen erstellten Schlüsselspeicherdatei. Sie können eine Schlüsselspeicherdatei mit einem selbstsignierten Zertifikat oder einem von einer Zertifizierungsbehörde signierten Zertifikat verwenden.
Schlüsselspeicherpasswort	Ein Klartext-Passwort für die Schlüsselspeicherdatei. Bei Verwendung einer von Ihnen erstellten Schlüsselspeicherdatei erforderlich.
Schlüsselspeicherdatei	Pfad und Dateiname der Schlüsselspeicherdatei. Bei Verwendung einer von Ihnen erstellten Schlüsselspeicherdatei erforderlich.

22. Klicken Sie auf **Weiter**.

    Wenn die anzufügende Domäne sicher ist, wird die Seite **Domänensicherheit – Sichere Kommunikation** angezeigt.
    Wenn die anzufügende Domäne nicht sicher ist, wird die Seite **Domänenkonfiguration** angezeigt. Fahren Sie mit Schritt 24 fort.

23. Geben Sie auf der Seite **Domänensicherheit – Sichere Kommunikation** an, ob die standardmäßigen SSL-Zertifikate von Informatica oder eigene SSL-Zertifikate zum Aktivieren sicherer Kommunikation in der Domäne verwendet werden sollen.

    Um die von Informatica bereitgestellten SSL-Standardzertifikate zu verwenden, wählen Sie die Option **Standardmäßige SSL-Zertifikatsdateien von Informatica verwenden** aus.

    Um das eigene SSL-Zertifikat zu verwenden, wählen Sie die Option **Speicherort der SSL-Zertifikatsdateien angeben** aus, und geben Sie die Verzeichnisse an, in denen die SSL-Zertifikatsdateien abgelegt sind.

Hinweis: Alle Knoten in der Domäne müssen über das gleiche SSL-Zertifikat verfügen. Wenn Sie einen Knoten zu einer Domäne hinzufügen, geben Sie die gleichen SSL-Zertifikate an, die auch vom Gateway-Knoten in der Domäne verwendet werden.

In der folgenden Tabelle werden die Parameter beschrieben, die für die SSL-Zertifikatsdateien eingegeben werden müssen:

Eigenschaft	Beschreibung
Schlüsselspeicherdatei-Verzeichnis	Verzeichnis, das die Schlüsselspeicherdateien enthält. Das Verzeichnis muss Dateien mit der Bezeichnung "infa_keystore.jks" und "infa_keystore.pem" enthalten.
Schlüsselspeicherpasswort	Passwort für den Schlüsselspeicher „infa_keystore.jks“.
Verzeichnis der Truststore-Datei	Verzeichnis, das die Truststore-Dateien enthält. Das Verzeichnis muss Dateien mit der Bezeichnung "infa_truststore.jks" und "infa_truststore.pem" enthalten.
Truststore-Passwort	Passwort für die Datei infa_truststore.jks.

Klicken Sie auf **Weiter**.

24. Geben Sie die Informationen für die Domäne ein, die Sie anfügen möchten.

    In der folgenden Tabelle werden die Eigenschaften beschrieben, die Sie für die Domäne festlegen:

Eigenschaft	Beschreibung
Domänenname	Der Name der zu verknüpfenden Domäne.
Host des Gateway-Knotens	Der Hostname des Computers, der den Gateway-Knoten für die Domäne hostet.
Port des Gateway-Knotens	Die Portnummer des Gateway-Knotens.
Domänenbenutzername	Der Benutzername des Administrators der Domäne, zu der Sie eine Verknüpfung herstellen möchten.
Domänenpasswort	Das Passwort für den Domänenadministrator.

25. Klicken Sie auf **Weiter**.

    Die Seite **Domänensicherheit – Verschlüsselungsschlüssel** wird geöffnet.

26. Geben Sie die Daten des Verschlüsselungsschlüssels für die anzufügende Informatica-Domäne ein.

In der folgenden Tabelle werden die Verschlüsselungsschlüsselparameter beschrieben, die beim Hinzufügen einer Domäne angegeben werden müssen:

Eigenschaft	Beschreibung
Auswählen des Verschlüsselungsschlüssels	Pfad und Dateiname des Verschlüsselungsschlüssels für die Informatica-Domäne, der Sie beitreten möchten. Alle Knoten in der Informatica-Domäne verwenden den gleichen Verschlüsselungsschlüssel. Sie müssen die Verschlüsselungsschlüsseldatei festlegen, die auf dem Gateway-Knoten für die Domäne erstellt wurde, der Sie beitreten möchten. Wenn Sie die Verschlüsselungsschlüsseldatei in ein temporäres Verzeichnis kopiert haben, damit sie für die Knoten in der Domäne zugänglich ist, geben Sie den Pfad und den Dateinamen der Verschlüsselungsschlüsseldatei im temporären Verzeichnis an.
Verzeichnis des Verschlüsselungsschlüssels	Verzeichnis zum Speichern des Verschlüsselungsschlüssels auf dem während dieser Installation erstellten Knoten. Das Installationsprogramm kopiert die Verschlüsselungsschlüsseldatei für die Domäne in das Verzeichnis des Verschlüsselungsschlüssels auf dem neuen Knoten. Standardmäßig wird der Verschlüsselungsschlüssel in folgendem Verzeichnis erstellt: `<Informatica-Installationsverzeichnis>/isp/config/keys`.

27. Klicken Sie auf **Weiter**.

    Die Seite **Join-Domänenknotenkonfiguration** wird angezeigt.

28. Geben Sie die Informationen für den Knoten ein, den Sie erstellen möchten.

    In der folgenden Tabelle werden die Eigenschaften beschrieben, die Sie für den Knoten festlegen:

Eigenschaft	Beschreibung
Knoten-Hostname	Hostname für den Knoten. Der Hostname des Knotens darf keine Unterstriche (_) enthalten. **Hinweis:** Verwenden Sie nicht localhost. Der Hostname muss den Computer eindeutig kennzeichnen.
Knotenname	Der Name des auf diesem Computer zu erstellenden Informatica-Knotens. Der Knotenname ist nicht mit dem Hostnamen des Computers identisch.
Knoten-Portnummer	Die Portnummer für den Knoten.
Datenbank-Truststore-Datei	Pfad und Dateiname der Truststore-Datei für die sichere Datenbank. Wählen Sie dieselbe Datenbank-Truststore-Datei aus, die vom Master-Gateway-Knoten in der Domäne verwendet wird. Erforderlich, wenn Sie einen Gateway-Knoten mit einer Domäne verbinden, die ein sicheres Domänenkonfigurations-Repository verwendet.
Truststore-Passwort	Passwort für die Datenbank-Truststore-Datei für die sichere Datenbank. Erforderlich, wenn Sie einen Gateway-Knoten mit einer Domäne verbinden, die ein sicheres Domänenkonfigurations-Repository verwendet.

29. Um die vom Installer zugewiesenen Standardports für die Domänen- und Knotenkomponenten anzuzeigen, wählen Sie **Anzeigen der Seite "Erweiterte Port-Konfiguration"** aus.

    Wenn Sie die Seite für die Portkonfiguration öffnen, werden vom Installationsprogramm die der Domäne und dem Knoten zugewiesenen Standardportnummern angezeigt. Sie können die Portnummern ändern

und einen anderen Portnummernbereich für die Anwendungsdienstprozesse angeben. Wenn Sie die Seite für die Portkonfiguration nicht öffnen, zeigt das Installationsprogramm die Standardportnummern nicht an und die zugewiesenen Portnummern können nicht geändert werden.

30. Klicken Sie auf **Weiter**.

    Wenn Sie angegeben haben, dass die Seite für die Portkonfiguration angezeigt werden soll, zeigt das Installationsprogramm die Seite **Portkonfiguration** an.

    Wenn Sie nicht angegeben haben, dass die Seite für die Portkonfiguration angezeigt werden soll, zeigt das Installationsprogramm die Seite **Windows-Dienstkonfiguration** an. Fahren Sie mit Schritt 33 fort.

31. Geben Sie auf der Seite **Portkonfiguration** die Portnummern für den Dienstmanager der Domäne und die Dienstprozesse ein, die auf dem Knoten ausgeführt werden.

    Stellen Sie sicher, dass die eingegebenen Portnummern nicht bereits von anderen Anwendungen verwendet werden.
    In der folgenden Tabelle werden die Ports beschrieben, die von Ihnen festgelegt werden können:

Port	Beschreibung
Dienstmanager-Port	Portnummer, die vom Dienstmanager auf dem Knoten verwendet wird. Der Dienstmanager überwacht eingehende Verbindungsanfragen auf diesem Port. Clientanwendungen verwenden diesen Port zur Kommunikation mit den Diensten in dieser Domäne. Die Informatica-Befehlszeilenprogramme verwenden diesen Port für die Kommunikation mit der Domäne. Dies ist auch der Port für den JDBC-/ODBC-Treiber des SQL-Datendiensts. Standardwert ist 6006.
Schließungsport des Dienstmanagers	Portnummer, die das Herunterfahren des Servers für den Dienstmanager der Domäne steuert. An diesem Port wartet der Dienstmanager auf Ausschaltbefehle. Standardwert ist 6007.
Niedrigste Portnummer	Niedrigste Portnummer des dynamischen Portnummernbereichs, die den Anwendungsdienstprozessen, die auf diesem Knoten laufen, zugewiesen werden kann. Standardwert ist 6014.
Höchste Portnummer	Höchste Portnummer des dynamischen Portnummernbereichs, die den Anwendungsdienstprozessen, die auf diesem Knoten laufen, zugewiesen werden kann. Standardwert ist 6114.

32. Klicken Sie auf **Weiter**.

33. Geben Sie auf der Seite **Windows-Dienstkonfiguration** an, ob der Windows-Dienst unter einem anderen Benutzerkonto ausgeführt werden soll.

    Das Installationsprogramm erstellt einen Dienst zum Starten von Informatica. Der Dienst wird standardmäßig unter demselben Benutzerkonto ausgeführt wie dem, das für die Installation verwendet wurde. Sie können den Windows-Dienst unter einem anderen Benutzerkonto ausführen.

In der folgenden Tabelle werden die Eigenschaften beschrieben, die zum Ausführen von Informatica unter einem anderen Benutzerkonto eingerichtet werden:

Eigenschaft	Beschreibung
Informatica unter einem anderen Benutzerkonto ausführen	Gibt an, ob der Windows-Dienst unter einem anderen Benutzerkonto ausgeführt werden soll.
Benutzername	Das Benutzerkonto, unter dem der Informatica-Windows-Dienst ausgeführt werden soll. Verwenden Sie das folgende Format: `<Domänenname>\<Benutzerkonto>` Dieses Benutzerkonto muss „Aktion“ als Betriebssystemberechtigung aufweisen.
Passwort	Das Passwort zum Benutzerkonto, unter dem der Informatica-Windows-Dienst ausgeführt werden soll.

34. Klicken Sie auf **Weiter**.

    Auf der Seite **Installationsabschlussbericht** wird angezeigt, ob die Installation erfolgreich abgeschlossen wurde. Der Bericht zeigt außerdem den Status der installierten Komponenten und deren Konfiguration an.

35. Klicken Sie zum Beenden des Installationsprogramms auf **Fertig**.

In den Dateien finden Sie weitere Informationen über die vom Installationsprogramm ausgeführten Aufgaben und die Konfigurationseigenschaften der installierten Komponenten.

Installieren der Informatica-Dienste im Konsolenmodus

Sie können die Informatica-Dienste unter UNIX im Konsolenmodus installieren.

Beim Ausführen des Installationsprogramms im Konsolenmodus stellen die Wörter "Beenden" und "Zurück" reservierte Wörter dar. Verwenden Sie sie daher nicht als Eingabetext.

Wenn Sie das Vorinstallations-Systemprüfungstool (i10Pi) vor der Installation ausführen, legt das Installationsprogramm die Werte für bestimmte Felder (beispielsweise die Datenbankverbindung und die Domänenportnummern) basierend auf den während der Systemüberprüfung eingegebenen Daten fest.

Erstellen einer Domäne

Erstellen Sie eine Domäne, wenn Sie zum ersten Mal installieren oder Knoten in separaten Domänen verwalten möchten.

1. Melden Sie sich mit einem Systembenutzerkonto am Computer an.
2. Schließen Sie alle anderen Anwendungen.
3. Führen Sie über eine Shell-Befehlszeile die Datei `install.sh` im Root-Verzeichnis aus.

   Der Installer zeigt die Nachricht an, um sicherzustellen, dass die Gebietsschema-Umgebungsvariablen gesetzt sind.

4. Wurden die Umgebungsvariablen nicht eingestellt, drücken Sie **n**, um den Installer zu beenden. Stellen Sie sie anschließend entsprechend den Anforderungen ein.

   Wenn die Umgebungsvariablen eingestellt sind, drücken Sie **y**, um fortzufahren.

5. Drücken Sie **1**, um Informatica zu installieren.

   Informatica stellt Dienstprogramme bereit, um die Installation der Informatica-Dienste zu vereinfachen. Führen Sie die folgenden Dienstprogramme vor der Installation von Informatica-Diensten aus:

   - Vorinstallations-Systemprüfungstool (i10Pi) Stellt sicher, dass der Computer, auf dem die Informatica-Dienste installiert werden, die Systemanforderungen für die Installation erfüllt.

     Weitere Informationen zum Ausführen des Vorinstallations-Systemprüfungstools (i10Pi) finden Sie unter "Ausführen des Vorinstallations-Systemprüfungstools (i10Pi)" auf Seite 91.

   - Kerberos SPN-Formatgenerator von Informatica. Erstellt eine Liste der Kerberos-Dienstprinzipalnamen und Keytab-Dateinamen, die zum Ausführen von Informatica-Diensten in einem Netzwerk mit Kerberos-Authentifizierung benötigt werden.

     Weitere Informationen zum Ausführen des Kerberos SPN-Formatgenerators von Informatica finden Sie unter "Ausführen des Kerberos SPN-Formatgenerators von Informatica unter Windows" auf Seite 77.

   Wenn Sie das i10Pi-Systemüberprüfungstool ausführen, können Sie den Informatica Kerberos SPN-Formatgenerator oder die Installation der Informatica-Dienste ausführen.

   Nach der Ausführung des Informatica Kerberos SPN-Formatgenerators können Sie die Installation der Informatica-Dienste fortsetzen. Sie können das i10Pi-Systemüberprüfungstool nach der Ausführung des Informatica Kerberos SPN-Formatgenerators ausführen.

6. Drücken Sie **3**, um die Installation der Informatica-Dienste auszuführen.

   Im Installationsprogramm werden basierend auf der Installationsplattform verschiedene Optionen angezeigt.

7. Führen Sie bei einer Installation unter Linux die folgenden Schritte durch:

   a. Lesen Sie die Bedingungen für die Informatica-Installation und das Toolkit zur Produktverwendung und wählen Sie **Ich stimme den Bedingungen zu** aus.

      Informatica DiscoveryIQ ist ein Produktnutzungstool, das Routineberichte über Datennutzung und Systemstatistiken an Informatica sendet. Nach der Installation und Konfiguration der Informatica-Domäne lädt Informatica DiscoveryIQ alle 15 Minuten Daten an Informatica hoch. Danach sendet die Domäne die Daten alle 30 Tage. Sie können die Verwendung von Statistiken im Administrator-Tool deaktivieren.

   b. Drücken Sie **1**, um die Informatica-Dienste zu installieren.

   c. Drücken Sie **1**, um die Informatica-Domäne zur Ausführung in einem Netzwerk zu konfigurieren, das keine Kerberos-Authentifizierung verwendet.

      Drücken Sie **2**, um die Informatica-Domäne zur Ausführung in einem Netzwerk mit Kerberos-Authentifizierung zu konfigurieren.

      Im Abschnitt **Installationsvoraussetzungen** werden die Installationsanforderungen angezeigt. Stellen Sie sicher, dass alle Voraussetzungen erfüllt sind, bevor Sie die Installation fortsetzen.

   d. Drücken Sie die **Eingabetaste**, um fortzufahren.

   e. Geben Sie den Pfad und Dateinamen des Informatica-Lizenzschlüssels ein, und drücken Sie die **Eingabetaste**.

Führen Sie bei einer Installation unter AIX und Solaris die folgenden Schritte durch:

a. Lesen Sie die Bedingungen für die Informatica-Installation und das Toolkit zur Produktverwendung und wählen Sie **Ich stimme den Bedingungen zu** aus.

   Informatica DiscoveryIQ ist ein Produktnutzungstool, das Routineberichte über Datennutzung und Systemstatistiken an Informatica sendet. Nach der Installation und Konfiguration der Informatica-Domäne lädt Informatica DiscoveryIQ alle 15 Minuten Daten an Informatica hoch. Danach sendet die Domäne die Daten alle 30 Tage. Sie können die Verwendung von Statistiken im Administrator-Tool deaktivieren.

b. Im Abschnitt **Installationsvoraussetzungen** werden die Installationsanforderungen angezeigt. Stellen Sie sicher, dass alle Voraussetzungen erfüllt sind, bevor Sie die Installation fortsetzen.

c. Drücken Sie die **Eingabetaste**, um fortzufahren.

d. Geben Sie den Pfad und Dateinamen des Informatica-Lizenzschlüssels ein, und drücken Sie die **Eingabetaste**.

e. Geben Sie den absoluten Pfad für das Installationsverzeichnis an.

   Die Verzeichnisnamen in dem Pfad dürfen weder Leerzeichen noch die folgenden Sonderzeichen enthalten: @|* $ # ! % ( ) { } [ ] , ; ' Standardwert ist /home/toolinst.

   Hinweis: Informatica empfiehlt die Verwendung alphanumerischer Zeichen im Installationsverzeichnispfad. Wenn Sie ein Sonderzeichen wie zum Beispiel á oder € verwenden, können unerwartete Ergebnisse während der Laufzeit auftreten.

f. Drücken Sie **1**, um die Informatica-Domäne zur Ausführung in einem Netzwerk zu konfigurieren, das keine Kerberos-Authentifizierung verwendet.

   Drücken Sie **2**, um die Informatica-Domäne zur Ausführung in einem Netzwerk mit Kerberos-Authentifizierung zu konfigurieren.

8. Drücken Sie die **Eingabetaste**.

   Wenn Sie die Kerberos-Netzwerkauthentifizierung aktiviert haben, wird der Abschnitt **Dienstprinzipalebene** angezeigt.
   Wenn Kerberos-Netzwerkauthentifizierung nicht aktiviert wurde, wird der Abschnitt **Vorinstallationsübersicht** angezeigt. Fahren Sie mit Schritt 11 fort.

9. Wählen Sie im Abschnitt **Dienstprinzipalebene** die Ebene aus, auf die Sie die Kerberos-Dienstprinzipale für die Domäne festlegen möchten.

   Hinweis: Alle Knoten in der Domäne müssen die gleiche Dienstprinzipalebene verwenden. Wenn Sie einen Knoten zu einer Domäne hinzufügen, wählen Sie die gleiche Dienstprinzipalebene aus, die vom Gateway-Knoten in der Domäne verwendet wird.

In der folgenden Tabelle werden die Ebenen beschrieben, die Sie auswählen können:

Ebene	Beschreibung
Prozessebene	Konfiguriert die Domäne für die Verwendung eines eindeutigen SPN und einer Keytab-Datei für jeden Knoten und jeden Anwendungsdienst auf einem Knoten. Die Anzahl der pro Knoten erforderlichen SPNs und Keytab-Dateien hängt von der Anzahl der Anwendungsdienstprozesse ab, die auf dem Knoten ausgeführt werden. Verwenden Sie die Prozessebenenoption für Datendomänen, die einen hohen Grad an Sicherheit erfordern, wie z. B. Produktionsdomänen.
Knotenebene	Konfiguriert die Domäne zur gemeinsamen Nutzung von SPNs und Keytab-Dateien auf einem Knoten. Diese Option erfordert jeweils einen SPN und eine Keytab-Datei für den Knoten und alle Anwendungsdienste, die auf dem Knoten ausgeführt werden. Sie erfordert außerdem einen separaten SPN und eine separate Keytab-Datei für alle HTTP-Prozesse auf dem Knoten. Verwenden Sie die Knotenebenenoption für Domänen, die keinen hohen Grad an Sicherheit erfordern, wie z. B. Test- und Entwicklungsdomänen.

10. Geben Sie im Abschnitt **Netzwerksicherheit – Kerberos-Authentifizierung** die Parameter ein, die für die Kerberos-Authentifizierung benötigt werden.

    In der folgenden Tabelle werden die Kerberos-Authentifizierungsparameter beschrieben, die eingerichtet werden müssen:

Eigenschaft	Beschreibung
Domänenname	Name der Domäne. Der Name darf maximal 128 Zeichen umfassen und muss im 7-Bit-ASCII-Format vorliegen. Der Name darf weder Leerzeichen noch folgende Zeichen enthalten: ` % * + ; " ? , < > \ /
Knotenname	Name des Informatica-Knotens
Knoten-Hostname	Vollständig qualifizierter Hostname oder die IP-Adresse des Computers, auf dem der Knoten erstellt werden soll. Der Hostname des Knotens darf keine Unterstriche (_) enthalten. **Hinweis:** Verwenden Sie nicht *localhost*. Der Hostname muss den Computer eindeutig kennzeichnen.
Dienstbereichsname	Name des Kerberos-Bereichs, zu dem die Informatica-Domänendienste gehören. Der Bereichsname muss aus Großbuchstaben bestehen. Die Namen des Dienst- und Benutzerbereichs müssen übereinstimmen.
Benutzerbereichsname	Name des Kerberos-Bereichs, zu dem die Informatica-Domänenbenutzer gehören. Der Bereichsname muss aus Großbuchstaben bestehen. Die Namen des Dienst- und Benutzerbereichs müssen übereinstimmen.

Eigenschaft	Beschreibung
Keytab-Verzeichnis	Verzeichnis, in dem alle Keytab-Dateien für die Informatica-Domäne gespeichert werden. Der Name einer Keytab-Datei in der Informatica-Domäne muss einem von Informatica festgelegten Format entsprechen.
Kerberos-Konfigurationsdatei	Pfad und Dateiname der Kerberos-Konfigurationsdatei. Informatica benötigt folgenden Namen für die Kerberos-Konfigurationsdatei: *krb5.conf*

Wichtig: Wenn Sie die Domäne zur Ausführung mit Kerberos-Authentifizierung konfigurieren, müssen der Domänen- und Knotenname sowie der Knoten-Hostname mit den Namen übereinstimmen, die beim Ausführen des Kerberos SPN-Formatgenerators von Informatica zum Erzeugen der SPNs und Keytab-Dateinamen angegeben wurden. Wenn Sie einen anderen Domänen-, Knoten- oder Hostnamen verwenden, erzeugen Sie den SPN und die Keytab-Dateinamen erneut und bitten Sie den Kerberos-Administrator, den neuen SPN zur Kerberos-Prinzipaldatenbank hinzuzufügen und die Keytab-Dateien zu erstellen.

11. Überprüfen Sie die Installationsinformationen und drücken Sie die **Eingabetaste**, um fortzufahren.

    Der Installer kopiert die Informatica-Dateien in das Installationsverzeichnis.

12. Drücken Sie **1**, um eine Domäne zu erstellen.

    Beim Erstellen einer Domäne übernimmt der zugehörige Knoten die Funktion eines Gateway-Knotens in der Domäne. Der Gateway-Knoten enthält einen Dienstmanager, der alle Domänenvorgänge verwaltet.

13. Drücken Sie **2**, um sichere Kommunikation für Dienste in der Domäne zu aktivieren. Drücken Sie **1**, um sichere Kommunikation für die Domäne zu deaktivieren.

    Wenn Sie sichere Kommunikation für die Domäne aktivieren, richtet das Installationsprogramm standardmäßig eine HTTPS-Verbindung für Informatica Administrator ein. Sie können auch ein Domänen-Konfigurations-Repository in einer sicheren Datenbank erstellen.

14. Geben Sie die Verbindungsdetails für Informatica Administrator ein.

    a. Wenn Sie sichere Kommunikation für die Domäne nicht aktivieren, können Sie angeben, ob eine sichere HTTPS-Verbindung für Informatica Administrator eingerichtet werden soll.

       In der folgenden Tabelle werden die zum Aktivieren oder Deaktivieren einer sicheren Verbindung mit Informatica Administrator verfügbaren Optionen beschrieben:

Option	Beschreibung
HTTPS für Informatica Administrator aktivieren	Richten Sie eine sichere Verbindung zu Informatica Administrator ein.
HTTPS deaktivieren	Richten Sie keine sichere Verbindung zu Informatica Administrator ein.

    b. Wenn Sie die sichere Kommunikation für die Domäne oder eine HTTPS-Verbindung für Informatica Administrator aktivieren, geben Sie die Schlüsselspeicherdatei und Portnummer für die HTTPS-Verbindung ein.

In der folgenden Tabelle werden die Verbindungsinformationen beschrieben, die Sie bei Aktivierung von HTTPS eingeben müssen:

Option	Beschreibung
Port	Die Portnummer für die HTTPS-Verbindung.
Schlüsselspeicherdatei	Wählen Sie, ob eine vom Installationsprogramm generierte oder eine von Ihnen erstellte Schlüsselspeicherdatei verwendet werden soll. Sie können eine Schlüsselspeicherdatei mit einem selbstsignierten Zertifikat oder einem von einer Zertifizierungsbehörde signierten Zertifikat verwenden. 1 – Von Installationsprogramm generierten Schlüsselspeicher verwenden 2 – Schlüsselspeicherdatei und Passwort eingeben Wenn Sie eine vom Installationsprogramm generierte Schlüsselspeicherdatei verwenden möchten, wird eine selbstsignierte Schlüsselspeicherdatei mit dem Namen „Default.keystore“ in folgendem Speicherort erstellt: `<Informatica-Installationsverzeichnis>/tomcat/conf/`

c. Wenn Sie den Schlüsselspeicher festlegen, geben Sie das Passwort und den Speicherort der Schlüsselspeicherdatei ein.

Wenn Sie die sichere Kommunikation für die Domäne aktiviert haben, wird der Abschnitt **Domänensicherheit – Sichere Kommunikation** angezeigt. Wenn sichere Kommunikation für die Domäne nicht aktiviert wurde, wird der Abschnitt **Domänen-Konfigurations-Repository**angezeigt. Fahren Sie mit Schritt 16 fort.

15. Geben Sie im Abschnitt „Domänensicherheit – Sichere Kommunikation“ an, ob die standardmäßigen SSL-Zertifikate von Informatica oder eigene SSL-Zertifikate zum Sichern der Domänenkommunikation verwendet werden sollen.

    a. Wählen Sie den Typ der zu verwendenden SSL-Zertifikate aus.

In der folgenden Tabelle werden die Optionen für die SSL-Zertifikate beschrieben, die Sie zum Sichern der Informatica-Domäne verwenden können:

Option	Beschreibung
SSL-Standardzertifikatsdateien von Informatica verwenden	Verwenden Sie die von Informatica bereitgestellten SSL-Standardzertifikate. **Hinweis:** Wenn Sie kein SSL-Zertifikat bereitstellen, verwendet Informatica denselben privaten Standardschlüssel für alle Informatica-Installationen. Wenn Sie die von Informatica bereitgestellten standardmäßigen Schlüsselspeicher- und Truststore-Dateien verwenden, wird die Sicherheit Ihrer Domäne unter Umständen gefährdet. Um ein hohes Maß an Sicherheit für die Domäne zu gewährleisten, wählen Sie die Option zum Angeben des Speicherorts der SSL-Zertifikatsdateien aus.
Speicherort der SSL-Zertifikatsdateien angeben	Verwenden Sie von Ihnen bereitgestellte SSL-Zertifikate. Sie müssen den Speicherort der Schlüsselspeicher- und Truststore-Dateien angeben. Sie können ein selbstsigniertes Zertifikat oder ein von einer Zertifizierungsstelle ausgegebenes Zertifikat verwenden. Sie müssen SSL-Zertifikate im PEM-Format und in Java-Schlüsselspeicherdateien (JKS) bereitstellen. Informatica benötigt bestimmte Namen für die SSL-Zertifikatsdateien in der Informatica-Domäne. Sie müssen für alle Knoten in der Domäne dieselben SSL-Zertifikate verwenden. Speichern Sie die Truststore- und Schlüsselspeicherdateien in einem Verzeichnis, auf das alle Knoten in der Domäne zugreifen können, und geben Sie für alle Knoten in derselben Domäne dasselbe Schlüsselspeicherdatei- und Truststore-Datei-Verzeichnis an.

b. Wenn Sie das SSL-Zertifikat bereitstellen, geben Sie den Speicherort und die Passwörter der Schlüsselspeicher- und der Truststore-Dateien an.

   In der folgenden Tabelle werden die Parameter beschrieben, die für die SSL-Zertifikatsdateien eingegeben werden müssen:

Eigenschaft	Beschreibung
Schlüsselspeicherdatei-Verzeichnis	Verzeichnis, das die Schlüsselspeicherdateien enthält. Das Verzeichnis muss Dateien mit der Bezeichnung "infa_keystore.jks" und "infa_keystore.pem" enthalten.
Schlüsselspeicherpasswort	Passwort für den Schlüsselspeicher „infa_keystore.jks“.
Verzeichnis der Truststore-Datei	Verzeichnis, das die Truststore-Dateien enthält. Das Verzeichnis muss Dateien mit der Bezeichnung "infa_truststore.jks" und "infa_truststore.pem" enthalten.
Truststore-Passwort	Passwort für die Datei infa_truststore.jks.

Der Abschnitt **Domänen-Konfigurations-Repository** wird angezeigt.

16. Wählen Sie die Datenbank aus, die für das Domänen-Konfigurations-Repository verwendet werden soll.

In der folgenden Tabelle werden die Datenbanken aufgelistet, die Sie für das Domänen-Konfigurations-Repository verwenden können:

Eingabeaufforderung	Beschreibung
Datenbanktyp	Der Datenbanktyp für das Domänen-Konfigurations-Repository. Wählen Sie eine der folgenden Optionen aus: 1 – Oracle 2 – Microsoft SQL Server 3 – IBM DB2 4 – Sybase ASE

Im Domänenkonfigurations-Repository von Informatica werden Metadaten für Domänenvorgänge und die Benutzerauthentifizierung gespeichert. Das Domänen-Konfigurations-Repository muss allen Gateway-Knoten in der Domäne zugänglich sein.

17. Geben Sie die Eigenschaften für die Datenbank und das Benutzerkonto ein.

    In der folgenden Tabelle werden die Eigenschaften für das Datenbankbenutzerkonto aufgelistet:

Eigenschaft	Beschreibung
Datenbankbenutzer-ID	Der Name des Benutzerkontos der Domänen-Konfigurationsdatenbank.
Benutzerpasswort	Das Passwort für die Domänen-Konfigurationsdatenbank.

18. Geben Sie an, ob ein sicheres Domänen-Konfigurations-Repository erstellt werden soll.

    In einer mit dem SSL-Protokoll gesicherten Datenbank können Sie ein Domänen-Konfigurations-Repository erstellen. Zum Erstellen eines Domänen-Konfigurations-Repository in einer sicheren Datenbank drücken Sie „1“ und fahren mit 20 fort.

    Zum Erstellen eines Domänen-Konfigurations-Repositorys in einer ungesicherten Datenbank drücken Sie 2.

19. Wenn Sie kein sicheres Domänen-Konfigurations-Repository erstellen, geben Sie die Parameter für die Datenbank ein.

    a. Geben Sie bei Auswahl von IBM DB2 an, ob ein Tablespace konfiguriert werden soll. Geben Sie dann den Namen des Tablespace ein.

In der folgenden Tabelle werden die Eigenschaften beschrieben, die Sie für die IBM DB2-Datenbank konfigurieren müssen:

Eigenschaft	Beschreibung
Tablespace konfigurieren	Wählen Sie aus, ob ein Tablespace festgelegt werden soll. 1 – Nein 2 – Ja Wenn Sie in einer Datenbank mit einer einzigen Partition „Nein“ auswählen, erstellt das Installationsprogramm die Tabellen im Standard-Tablespace. In einer Datenbank mit mehreren Partitionen müssen Sie „Ja“ wählen.
Tablespace	Der Name des Tablespace, in dem die Tabellen erstellt werden sollen. Geben Sie einen Tablespace an, der die Anforderungen an die Seitengröße (pageSize) von 32768 Byte erfüllt. Wenn Sie in einer Datenbank mit einer einzigen Partition die Option „Ja“ für die Konfiguration des Tablespace konfigurieren, geben Sie den Namen des Tablespace ein, in dem die Tabellen konfiguriert werden sollen. Geben Sie in einer Datenbank mit mehreren Partitionen den Namen des Tablespace ein, der sich in der Katalogpartition der Datenbank befindet.

b. Geben Sie bei Auswahl von Microsoft SQL Server den Schemanamen für die Datenbank ein.

   In der folgenden Tabelle werden die Eigenschaften beschrieben, die Sie für die Microsoft SQL Server-Datenbank konfigurieren müssen:

Eigenschaft	Beschreibung
Schemaname	Der Name des Schemas, das Domänenkonfigurationstabellen enthalten soll. Ist dieser Parameter leer, werden die Tabellen im Standardschema erstellt.

c. Um die JDBC-Verbindungsdaten mithilfe der JDBC-URL-Daten einzugeben, drücken Sie **1**. Um die JDBC-Verbindungsdaten mithilfe einer benutzerdefinierten JDBC-Verbindungszeichenfolge einzugeben, drücken Sie **2**.

d. Geben Sie die JDBC-Verbindungsdaten ein.

   - Um die Verbindungsdaten mithilfe der JDBC-URL-Daten einzugeben, legen Sie die JDBC-URL-Eigenschaften fest.
     In der folgenden Tabelle werden die Datenbankverbindungsinformationen beschrieben:

Eingabeaufforderung	Beschreibung
Datenbank-Hostname	Der Hostname für die Datenbank.
Datenbank-Portnummer	Portnummer der Datenbank.

Eingabeaufforderung	Beschreibung
Datenbankdienstname	Dienst- oder Datenbankname: - Oracle: Geben Sie den Dienstnamen ein. - Microsoft SQL Server: Geben Sie den Datenbanknamen ein. - IBM DB2: Geben Sie den Dienstnamen ein. - Sybase ASE: Geben Sie den Datenbanknamen ein.
JDBC-Parameter konfigurieren	Geben Sie an, ob der Verbindungszeichenfolge weitere JDBC-Parameter hinzugefügt werden sollen: 1 – Ja 2 – Nein Geben Sie bei Auswahl von „Ja“ die Parameter ein oder drücken Sie die Eingabetaste, um die Standardparameter zu übernehmen. Bei Auswahl von „Nein“ wird die JDBC-Verbindungszeichenfolge ohne Parameter erstellt.

- Um die Verbindungsdaten mithilfe einer benutzerdefinierten JDBC-Verbindungszeichenfolge einzugeben, geben Sie die Verbindungszeichenfolge ein.
  Verwenden Sie die folgende Syntax in der JDBC-Verbindungszeichenfolge:
  IBM DB2

  ```
  jdbc:Informatica:db2://host_name:port_no;DatabaseName=
  ```

  Oracle

  ```
  jdbc:Informatica:oracle://host_name:port_no;ServiceName=
  ```

  Microsoft SQL Server

  ```
  jdbc:Informatica:sqlserver://
  host_name:port_no;SelectMethod=cursor;DatabaseName=
  ```

  Sybase

  ```
  jdbc:Informatica:sybase://host_name:port_no;DatabaseName=
  ```

  Stellen Sie sicher, dass die Verbindungszeichenfolge alle vom Datenbanksystem benötigten Verbindungsparameter enthält.

20. Wenn Sie ein sicheres Domänen-Konfigurations-Repository erstellen, geben Sie die Parameter für die sichere Datenbank ein.

    Wenn Sie das Domänen-Konfigurations-Repository in einer sicheren Datenbank erstellen, müssen Sie die Truststore-Informationen für die Datenbank angeben. Außerdem müssen Sie eine JDBC-Verbindungszeichenfolge angeben, die die Sicherheitsparameter für die Datenbank enthält.

In der folgenden Tabelle werden die zum Erstellen einer sicheren Domänenkonfigurations-Repository-Datenbank verfügbaren Optionen beschrieben:

Eigenschaft	Beschreibung
Datenbank-Truststore-Datei	Pfad und Dateiname der Truststore-Datei für die sichere Datenbank.
Datenbank-Truststore-Passwort	Passwort für die TrustStore-Datei.
Benutzerdefinierte JDBC-Verbindungszeichenfolge	JDBC-Verbindungszeichenfolge zum Herstellen einer Verbindung mit der sicheren Datenbank, einschließlich des Hostnamens, der Portnummer und der Sicherheitsparameter für die Datenbank.

Zusätzlich zum Hostnamen und der Portnummer für den Datenbankserver müssen Sie die folgenden sicheren Datenbankparameter angeben. Sie können die folgende Syntax für die Verbindungszeichenfolgen verwenden:

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 der Datenbankserver sendet.

Wenn dieser Parameter auf TRUE gesetzt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat. Wenn Sie den HostNameInCertificate-Parameter angeben, validiert Informatica ebenfalls den Hostnamen im Zertifikat.

Wenn dieser Parameter auf FALSE gesetzt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat nicht. Informatica ignoriert alle Truststore-Informationen, die Sie angeben

Standardwert ist „True“.

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.

cryptoProtocolVersion

Erforderlich. Gibt das Kryptografieprotokoll an, das für die Verbindung mit einer sicheren Datenbank verwendet werden soll. Sie können je nach dem vom Datenbankserver verwendeten Kryptografieprotokoll den Parameter auf `cryptoProtocolVersion=TLSv1.1` oder `cryptoProtocolVersion=TLSv1.2` festlegen.

- Oracle: `jdbc:Informatica:oracle:// host_name:port_no;ServiceName=service_name;EncryptionMethod=SSL;HostNameInCertificate= DB_host_name;ValidateServerCertificate=true_or_false`
- IBM DB2: `jdbc:Informatica:db2:// host_name:port_no;DatabaseName=database_name;EncryptionMethod=SSL;HostNameInCertificat e=DB_host_name;ValidateServerCertificate=true_or_false`
- Microsoft SQL Server: `jdbc:Informatica:sqlserver:// host_name:port_no;SelectMethod=cursor;DatabaseName=database_name;EncryptionMethod=SSL; HostNameInCertificate=DB_host_name;ValidateServerCertificate=true_or_false`

Hinweis: Die Verbindungszeichenfolge wird vom Installationsprogramm nicht überprüft. Stellen Sie sicher, dass die Verbindungszeichenfolge alle von der Datenbank benötigten Verbindungs- und Sicherheitsparameter enthält.

21. Wenn die Datenbank ein Domänen-Konfigurations-Repository für eine frühere Domäne enthält, überschreiben Sie die Daten oder richten Sie eine weitere Datenbank ein.

    In der folgenden Tabelle werden die Optionen zum Überschreiben der Daten oder zum Einrichten einer weiteren Datenbank beim Erstellen eines Domänen-Konfigurations-Repositorys für eine frühere Domäne beschrieben:

Option	Beschreibung
1 – OK	Geben Sie die Verbindungsdaten für eine neue Datenbank ein.
2 – Fortfahren	Die Daten in der Datenbank werden mit der neuen Domänenkonfiguration überschrieben.

22. Geben Sie im Abschnitt **Domänensicherheit – Verschlüsselungsschlüssel** das Schlüsselwort und das Verzeichnis für den Verschlüsselungsschlüssel in der Informatica-Domäne ein.

    In der folgenden Tabelle werden die Verschlüsselungsschlüsselparameter beschrieben, die Sie angeben müssen:

Eigenschaft	Beschreibung
Schlüsselwort	Schlüsselwort zum Erstellen eines benutzerdefinierten Verschlüsselungsschlüssels für die Sicherung vertraulicher Daten in der Domäne. Das Schlüsselwort muss die folgenden Kriterien erfüllen: - Hat eine Länge von 8 bis 20 Zeichen - Enthält mindestens einen Großbuchstaben - Enthält mindestens einen Kleinbuchstaben - Enthält mindestens eine Zahl - Enthält keine Leerzeichen Der Verschlüsselungsschlüssel wird basierend auf dem Schlüsselwort erstellt, das Sie beim Erstellen der Informatica-Domäne angeben.
Verzeichnis des Verschlüsselungsschlüssels	Verzeichnis, in dem der Verschlüsselungsschlüssel für die Domäne gespeichert werden soll. Standardmäßig wird der Verschlüsselungsschlüssel in folgendem Verzeichnis erstellt: `<Informatica-Installationsverzeichnis>/isp/config/keys`.

    Das Installationsprogramm legt verschiedene Berechtigungen für das Verzeichnis und die Dateien im Verzeichnis fest. Weitere Informationen über die Berechtigungen für die Verschlüsselungsschlüsseldatei und das Verzeichnis finden Sie unter "Sichere Dateien und Verzeichnisse" auf Seite 107.

23. Drücken Sie die **Eingabetaste**, um OK auszuwählen.

    Der Abschnitt **Domänen- und Knotenkonfiguration** wird angezeigt.

24. Geben Sie die Informationen für die Domäne und den Knoten ein, die Sie erstellen möchten.

In der folgenden Tabelle sind die Eigenschaften beschrieben, die Sie für den Domänen- und den Gateway-Knoten festlegen:

Eigenschaft	Beschreibung
Domänenname	Name der zu erstellenden Informatica-Domäne. Der Standardname der Domäne lautet Domain_<MachineName>. Der Name darf maximal 128 Zeichen umfassen und muss im 7-Bit-ASCII-Format vorliegen. Der Name darf weder Leerzeichen noch folgende Zeichen enthalten: ` % * + ; " ? , < > \ /
Knotenname	Name des zu erstellenden Knotens.
Knoten-Hostname	Hostname oder IP-Adresse des Computers, auf dem der Knoten erstellt werden soll. Wenn der Computer nur einen Netzwerknamen aufweist, verwenden Sie den Standardhostnamen. Wenn der Computer mehrere Netzwerknamen aufweist, können Sie den Standardhostnamen ändern und einen alternativen Netzwerknamen verwenden. **Hinweis:** Der Hostname des Knotens darf keine Unterstriche (_) enthalten. Verwenden Sie nicht localhost. Der Hostname muss den Computer eindeutig kennzeichnen.
Knoten-Portnummer	Die Portnummer für den Knoten. Die Standard-Portnummer für den Knoten lautet 6005. Wenn die Portnummer auf dem Rechner nicht verfügbar ist, wird die nächste verfügbare Portnummer angezeigt.
Domänenbenutzername	Benutzername für den Domänenadministrator. Sie können diesen Benutzernamen für die Erstanmeldung bei Informatica Administrator verwenden. Beachten Sie folgende Richtlinien: - Beim Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden und er darf nicht mehr als 128 Zeichen umfassen. - Der Name darf weder Tabulatoren und Zeilenendzeichen noch die folgenden Sonderzeichen enthalten: % * + / ? ; < > - Der Name kann ein ASCII-Leerzeichen enthalten, jedoch nicht als erstes oder letztes Zeichen. Alle anderen Leerzeichen sind nicht zulässig.
Domänenpasswort	Das Passwort für den Domänenadministrator. Das Passwort muss mindestens zwei Zeichen und darf bis zu 16 Zeichen enthalten. Nicht verfügbar, wenn Sie die Informatica-Domäne zur Ausführung in einem Netzwerk mit Kerberos-Authentifizierung konfigurieren.
Passwort bestätigen	Geben Sie das Passwort zur Bestätigung erneut ein. Nicht verfügbar, wenn Sie die Informatica-Domäne zur Ausführung in einem Netzwerk mit Kerberos-Authentifizierung konfigurieren.

25. Wählen Sie, ob Sie SAML-basiertes Single Sign-On aktivieren möchten, um auf Security Assertion Markup Language (SAML) basierte Unterstützung für Single Sign-On (SSO) für webbasierte Informatica-Anwendungen in einer Informatica-Domäne zu konfigurieren.

Die folgende Tabelle beschreibt die Informationen, die Sie eingeben müssen, um SAML-basiertes Single Sign-On zu aktivieren:

Eingabeaufforderung	Beschreibung
SAML-basiertes Single Sign-On aktivieren	Wählen Sie, ob Sie SAML-basiertes Single Sign-On aktivieren möchten: 1 – Nein 2 – Ja Wenn Sie „Ja“ auswählen, müssen Sie die Identitäts-Provider-URL für die Domäne eingeben.

26. Legen Sie fest, ob die vom Installer zugewiesenen Standardports für die Domänen- und Knotenkomponenten angezeigt werden sollen.

    In der folgenden Tabelle wird die Seite „Erweiterte Port-Konfiguration“ beschrieben:

Eingabeaufforderung	Beschreibung
Anzeigen der Seite „Erweiterte Port-Konfiguration“	Legen Sie fest, ob die vom Installationsprogramm zugewiesenen Portnummern für die Domänen- und Knotenkomponenten angezeigt werden sollen: 1 – Nein 2 – Ja Wenn Sie „Ja“ auswählen, zeigt das Installationsprogramm die Standard-Portnummern an, die den Domänenkomponenten zugewiesen sind. Sie können die für die Domänen- und Knotenkomponenten zu verwendenden Portnummern festlegen. Sie können für den Dienstprozess, der auf dem Knoten laufen wird, auch einen Bereich für Portnummern festlegen. Sie können die Standard-Portnummern verwenden oder neue Portnummern festlegen. Stellen Sie sicher, dass die eingegebenen Portnummern nicht bereits von anderen Anwendungen verwendet werden.

27. Geben Sie auf der Seite „Port-Konfiguration“ neue Portnummern ein, wenn Sie dazu aufgefordert werden, oder drücken Sie die Eingabetaste, um die Standard-Portnummern zu verwenden.

    In der folgenden Tabelle werden die Ports beschrieben, die von Ihnen festgelegt werden können:

Port	Beschreibung
Dienstmanager-Port	Portnummer, die vom Dienstmanager auf dem Knoten verwendet wird. Der Dienstmanager überwacht eingehende Verbindungsanfragen auf diesem Port. Clientanwendungen verwenden diesen Port zur Kommunikation mit den Diensten in dieser Domäne. Die Informatica-Befehlszeilenprogramme verwenden diesen Port für die Kommunikation mit der Domäne. Dies ist auch der Port für den JDBC-/ODBC-Treiber des SQL-Datendiensts. Standardwert ist 6006.
Schließungsport des Dienstmanagers	Portnummer, die das Herunterfahren des Servers für den Dienstmanager der Domäne steuert. An diesem Port wartet der Dienstmanager auf Ausschaltbefehle. Standardwert ist 6007.
Informatica Administrator-Port	Portnummer von Informatica Administrator. Standardwert ist 6008.

Port	Beschreibung
Informatica Administrator-Schließungsport	Portnummer, die das Herunterfahren des Servers für Informatica Administrator steuert. Informatica Administrator überwacht Befehle zum Herunterfahren auf diesem Port. Standardwert ist 6009.
Niedrigste Portnummer	Niedrigste Portnummer des dynamischen Portnummernbereichs, die den Anwendungsdienstprozessen, die auf diesem Knoten laufen, zugewiesen werden kann. Standardwert ist 6014.
Höchste Portnummer	Höchste Portnummer des dynamischen Portnummernbereichs, die den Anwendungsdienstprozessen, die auf diesem Knoten laufen, zugewiesen werden kann. Standardwert ist 6114.

28. Wenn Sie die Option **Modellrepository-Dienst und Datenintegrationsdienst konfigurieren** gewählt haben, konfigurieren Sie die Anwendungsdienste.
    a. Konfigurieren Sie die Modellrepository-Datenbank-Eigenschaften.
    b. Geben Sie den Modellrepository-Dienstnamen ein.

       Wenn die Informatica-Domäne Kerberos-Authentifizierung verwendet und sich der Dienstprinzipal auf Prozessebene befindet, geben Sie die Keytab-Datei für den Modellrepository-Dienst ein.
    c. Der Datenintegrationsdienst-Name.

       Wenn die Informatica-Domäne Kerberos-Authentifizierung verwendet und sich der Dienstprinzipal auf Prozessebene befindet, geben Sie die Keytab-Datei für den Datenintegrationsdienst ein.
    d. Wählen Sie das Verbindungsprotokoll für den Datenintegrationsdienst aus.

       Geben Sie einen der folgenden Werte ein:
       - HTTP. Erfordert, dass der Dienst eine HTTP-Verbindung benutzt.
       - HTTPS. Erfordert, dass der Dienst eine sichere HTTP-Verbindung benutzt.
       - HTTP&HTTPS. In Anfragen an den Dienst kann entweder eine HTTP- oder eine HTTPS-Verbindung verwendet werden.

       Wenn Sie HTTPS oder HTTP&HTTPS auswählen, aktivieren Sie TLS (Transport Layer Security) für den Dienst.

       Sie können TLS auch für jeden Webdienst aktivieren, der für eine Anwendung bereitgestellt wurde. Wenn Sie HTTPS für den Datenintegrationsdienst und TLS für den Webdienst aktivieren, verwendet der Webdienst eine HTTPS-URL. Wenn Sie HTTPS für den Datenintegrationsdienst und nicht für den Webdienst aktivieren, kann der Webdienst eine HTTP-URL oder eine HTTPS-URL nutzen. Wenn Sie TLS für einen Webdienst aktivieren, aber HTTPS nicht für den Datenintegrationsdienst aktivieren, startet der Webdienst nicht.

       Standardwert ist „HTTP“.
    e. Geben Sie die Portnummer für HTTP oder HTTPS oder beides ein, je nach dem von Ihnen ausgewählten Verbindungsprotokoll.

       Wenn Sie HTTPS oder HTTP&HTTPS ausgewählt haben, können Sie die standardmäßigen Informatica SSL-Zertifikatsdateien oder benutzerdefinierten SSL-Zertifikatsdateien für den Datenintegrationsdienst verwenden.
    f. Wählen Sie, ob die standardmäßigen Informatica SSL-Zertifikatsdateien verwendet werden sollen, oder geben Sie den Speicherort der SSL-Zertifikatsdateien ein, die für den Datenintegrationsdienst spezifisch sind.

g. Wenn Sie wählen, den Speicherort für SSL-Zertifikatsdateien einzugeben, geben Sie den Speicherort der KeyStore- und Truststore-Dateien und ihre Passwörter ein.

   Die KeyStore-Datei und die Truststore-Datei müssen im JKS-Format vorhanden sein.

Das Installationsprogramm erstellt den Modellrepository-Dienst sowie den Datenintegrationsdienst und startet die Dienste.

Im Abschnitt **Nach der Installation – Zusammenfassung** wird angezeigt, ob die Installation erfolgreich abgeschlossen wurde. Der Bericht zeigt außerdem den Status der installierten Komponenten und deren Konfiguration an.

In den Protokolldateien der Installation finden Sie weitere Informationen über die vom Installationsprogramm ausgeführten Aufgaben und die Konfigurationseigenschaften der installierten Komponenten.

Standardmäßig sind die Systemdienste nach Abschluss der Installation deaktiviert. Sie müssen sie im Administrator Tool aktivieren.

Beitreten zu einer Domäne

Sie können eine Verknüpfung zu einer Domäne herstellen, wenn Sie eine Installation auf mehreren Computern vornehmen und eine Domäne auf einem anderen Computer erstellt haben.

1. Melden Sie sich mit einem Systembenutzerkonto am Computer an.
2. Schließen Sie alle anderen Anwendungen.
3. Führen Sie über eine Shell-Befehlszeile die Datei „install.sh“ im Root-Verzeichnis aus.

   Der Installer zeigt die Nachricht an, um sicherzustellen, dass die Gebietsschema-Umgebungsvariablen gesetzt sind.
4. Wurden die Umgebungsvariablen nicht eingestellt, drücken Sie **n**, um den Installer zu beenden. Stellen Sie sie anschließend entsprechend den Anforderungen ein.

   Wurden die Umgebungsvariablen angegeben, drücken Sie **y**, um fortzufahren.
5. Drücken Sie **1**, um die Installation oder das Upgrade von Informatica durchzuführen.

   Informatica stellt Dienstprogramme bereit, um die Installation der Informatica-Dienste zu vereinfachen. Führen Sie die folgenden Dienstprogramme vor der Installation von Informatica-Diensten aus:

   - Vorinstallations-Systemprüfungstool (i10Pi) Stellt sicher, dass der Computer, auf dem die Informatica-Dienste installiert werden, die Systemanforderungen für die Installation erfüllt.

     Weitere Informationen zum Ausführen des Vorinstallations-Systemprüfungstools (i10Pi) finden Sie unter “Ausführen des Vorinstallations-Systemprüfungstools (i10Pi)” auf Seite 91.
   - Kerberos SPN-Formatgenerator von Informatica. Erstellt eine Liste der Kerberos-Dienstprinzipalnamen und Keytab-Dateinamen, die zum Ausführen von Informatica-Diensten in einem Netzwerk mit Kerberos-Authentifizierung benötigt werden.

     Weitere Informationen zum Ausführen des Kerberos SPN-Formatgenerators von Informatica finden Sie unter “Ausführen des Kerberos SPN-Formatgenerators von Informatica unter Windows” auf Seite 77.

   Wenn Sie das i10Pi-Systemüberprüfungstool ausführen, können Sie den Informatica Kerberos SPN-Formatgenerator oder die Installation der Informatica-Dienste ausführen.

   Nach der Ausführung des Informatica Kerberos SPN-Formatgenerators können Sie die Installation der Informatica-Dienste fortsetzen. Sie können das i10Pi-Systemüberprüfungstool nach der Ausführung des Informatica Kerberos SPN-Formatgenerators ausführen.
6. Drücken Sie **3**, um die Installation der Informatica-Dienste auszuführen.
7. Drücken Sie **1**, um die Informatica-Dienste zu installieren.

Im Installationsprogramm werden basierend auf der Installationsplattform verschiedene Optionen angezeigt.

8. Führen Sie bei einer Installation unter Linux die folgenden Schritte durch:

   a. Lesen Sie die Bedingungen für die Informatica-Installation und das Toolkit zur Produktverwendung und wählen Sie **Ich stimme den Bedingungen zu** aus.

      Informatica DiscoveryIQ ist ein Produktnutzungstool, das Routineberichte über Datennutzung und Systemstatistiken an Informatica sendet. Nach der Installation und Konfiguration der Informatica-Domäne lädt Informatica DiscoveryIQ alle 15 Minuten Daten an Informatica hoch. Danach sendet die Domäne die Daten alle 30 Tage. Sie können die Verwendung von Statistiken im Administrator-Tool deaktivieren.

   b. Drücken Sie **1**, um die Informatica-Dienste zu installieren.

   c. Drücken Sie **1**, um die Informatica-Domäne zur Ausführung in einem Netzwerk zu konfigurieren, das keine Kerberos-Authentifizierung verwendet.

      Drücken Sie **2**, um die Informatica-Domäne zur Ausführung in einem Netzwerk mit Kerberos-Authentifizierung zu konfigurieren.

      Im Abschnitt **Installationsvoraussetzungen** werden die Installationsanforderungen angezeigt. Stellen Sie sicher, dass alle Voraussetzungen erfüllt sind, bevor Sie die Installation fortsetzen.

   Führen Sie bei einer Installation unter AIX die folgenden Schritte durch:

   a. Drücken Sie **1**, um die Informatica-Domäne zur Ausführung in einem Netzwerk zu konfigurieren, das keine Kerberos-Authentifizierung verwendet.

      Drücken Sie **2**, um die Informatica-Domäne zur Ausführung in einem Netzwerk mit Kerberos-Authentifizierung zu konfigurieren.

      Im Abschnitt **Installationsvoraussetzungen** werden die Installationsanforderungen angezeigt. Stellen Sie sicher, dass alle Voraussetzungen erfüllt sind, bevor Sie die Installation fortsetzen.

   b. Lesen Sie die Bedingungen für die Informatica-Installation und das Toolkit zur Produktverwendung und wählen Sie **Ich stimme den Bedingungen zu** aus.

      Informatica DiscoveryIQ ist ein Produktnutzungstool, das Routineberichte über Datennutzung und Systemstatistiken an Informatica sendet. Nach der Installation und Konfiguration der Informatica-Domäne lädt Informatica DiscoveryIQ alle 15 Minuten Daten an Informatica hoch. Danach sendet die Domäne die Daten alle 30 Tage. Sie können die Verwendung von Statistiken im Administrator-Tool deaktivieren.

9. Drücken Sie die **Eingabetaste**, um fortzufahren.

10. Geben Sie den Pfad und Dateinamen des Informatica-Lizenzschlüssels ein und drücken Sie die **Eingabetaste**.

11. Geben Sie den absoluten Pfad für das Installationsverzeichnis ein.

    Die Verzeichnisnamen in dem Pfad dürfen weder Leerzeichen noch die folgenden Sonderzeichen enthalten: @|* $ # ! % ( ) { } [ ] , ; ' Standardwert ist /home/toolinst.

    Hinweis: Informatica empfiehlt die Verwendung alphanumerischer Zeichen im Installationsverzeichnispfad. Wenn Sie ein Sonderzeichen wie zum Beispiel á oder € verwenden, können unerwartete Ergebnisse während der Laufzeit auftreten.

12. Drücken Sie die **Eingabetaste**.

    Wenn Sie die Kerberos-Netzwerkauthentifizierung aktiviert haben, wird der Abschnitt **Dienstprinzipalebene** angezeigt.
    Wenn Kerberos-Netzwerkauthentifizierung nicht aktiviert wurde, wird der Abschnitt **Vorinstallationsübersicht** angezeigt. Fahren Sie mit Schritt 15 fort.

13. Wählen Sie im Abschnitt **Dienstprinzipalebene** die Dienstprinzipalebene für die Domäne aus.

    Hinweis: Alle Knoten in der Domäne müssen die gleiche Dienstprinzipalebene verwenden. Wenn Sie einen Knoten zu einer Domäne hinzufügen, wählen Sie die gleiche Dienstprinzipalebene aus, die vom Gateway-Knoten in der Domäne verwendet wird.

    In der folgenden Tabelle werden die Ebenen beschrieben, die Sie auswählen können:

Ebene	Beschreibung
Prozessebene	Konfiguriert die Domäne für die Verwendung eines eindeutigen SPN und einer Keytab-Datei für jeden Knoten und jeden Anwendungsdienst auf einem Knoten. Die Anzahl der pro Knoten erforderlichen SPNs und Keytab-Dateien hängt von der Anzahl der Anwendungsdienstprozesse ab, die auf dem Knoten ausgeführt werden. Verwenden Sie die Prozessebenenoption für Datendomänen, die einen hohen Grad an Sicherheit erfordern, wie z. B. Produktionsdomänen.
Knotenebene	Konfiguriert die Domäne zur gemeinsamen Nutzung von SPNs und Keytab-Dateien auf einem Knoten. Diese Option erfordert jeweils einen SPN und eine Keytab-Datei für den Knoten und alle Anwendungsdienste, die auf dem Knoten ausgeführt werden. Sie erfordert außerdem einen separaten SPN und eine separate Keytab-Datei für alle HTTP-Prozesse auf dem Knoten. Verwenden Sie die Knotenebenenoption für Domänen, die keinen hohen Grad an Sicherheit erfordern, wie z. B. Test- und Entwicklungsdomänen.

14. Geben Sie im Abschnitt **Netzwerksicherheit – Kerberos-Authentifizierung** die Parameter ein, die für die Kerberos-Authentifizierung benötigt werden.

    In der folgenden Tabelle werden die Kerberos-Authentifizierungsparameter beschrieben, die eingerichtet werden müssen:

Eigenschaft	Beschreibung
Domänenname	Name der Domäne. Der Name darf maximal 128 Zeichen umfassen und muss im 7-Bit-ASCII-Format vorliegen. Der Name darf weder Leerzeichen noch folgende Zeichen enthalten: ` % * + ; " ? , < > \ /
Knotenname	Name des Informatica-Knotens
Knoten-Hostname	Vollständig qualifizierter Hostname oder die IP-Adresse des Computers, auf dem der Knoten erstellt werden soll. Der Hostname des Knotens darf keine Unterstriche (_) enthalten. **Hinweis:** Verwenden Sie nicht *localhost*. Der Hostname muss den Computer eindeutig kennzeichnen.
Dienstbereichsname	Name des Kerberos-Bereichs, zu dem die Informatica-Domänendienste gehören. Der Bereichsname muss aus Großbuchstaben bestehen. Die Namen des Dienst- und Benutzerbereichs müssen übereinstimmen.
Benutzerbereichsname	Name des Kerberos-Bereichs, zu dem die Informatica-Domänenbenutzer gehören. Der Bereichsname muss aus Großbuchstaben bestehen. Die Namen des Dienst- und Benutzerbereichs müssen übereinstimmen.

Eigenschaft	Beschreibung
Keytab-Verzeichnis	Verzeichnis, in dem alle Keytab-Dateien für die Informatica-Domäne gespeichert werden. Der Name einer Keytab-Datei in der Informatica-Domäne muss einem von Informatica festgelegten Format entsprechen.
Kerberos-Konfigurationsdatei	Pfad und Dateiname der Kerberos-Konfigurationsdatei. Informatica benötigt folgenden Namen für die Kerberos-Konfigurationsdatei: *krb5.conf*

15. Überprüfen Sie die Installationsinformationen und drücken Sie die **Eingabetaste**, um fortzufahren.

    Der Installer kopiert die Informatica-Dateien in das Installationsverzeichnis.

16. Drücken Sie **2**, um eine Domäne anzufügen.

    Das Installationsprogramm erstellt einen Knoten auf dem Computer, auf dem die Installation erfolgt. Sie können den zu erstellenden Knotentyp und die Domäne, zu der eine Verknüpfung hergestellt werden soll, festlegen.

17. Geben Sie an, ob für die anzufügende Domäne die Option zur sicheren Kommunikation aktiviert wurde.

    Drücken Sie 1, um eine ungesicherte Domäne anzufügen, oder 2, um eine sichere Domäne anzufügen.

18. Wählen Sie den Knotentyp aus, den Sie erstellen möchten.

    In der folgenden Tabelle werden die Knotentypen beschrieben, die Sie erstellen können:

Eigenschaft	Beschreibung
Diesen Knoten als Gateway konfigurieren	Legen Sie fest, ob Sie diesen Knoten als Gateway- oder Worker-Knoten konfigurieren möchten. 1 – Ja 2 – Nein Wählen Sie „1“ zum Konfigurieren eines Gateway-Knotens oder „2“ zum Konfigurieren eines Worker-Knotens.

    Wenn Sie den Knoten als Gateway konfigurieren, können Sie eine sichere HTTPS-Verbindung zu Informatica Administrator aktivieren.

19. Geben Sie die Verbindungsdetails zu Informatica Administrator ein.

    a. Geben Sie an, ob eine sichere HTTPS-Verbindung zu Informatica Administrator eingerichtet werden soll.

Option	Beschreibung
1 – HTTPS für Informatica Administrator aktivieren	Richten Sie eine sichere Verbindung zu Informatica Administrator ein.
2 – HTTPS deaktivieren	Richten Sie keine sichere Verbindung zu Informatica Administrator ein.

b. Wenn Sie eine HTTPS-Verbindung für Informatica Administrator aktivieren, geben Sie die zum Sichern der Verbindung zu verwendende Schlüsselspeicherdatei und Portnummer ein.

Option	Beschreibung
Port	Die Portnummer für die HTTPS-Verbindung.
Schlüsselspeicherdatei	Wählen Sie, ob eine vom Installationsprogramm generierte oder eine von Ihnen erstellte Schlüsselspeicherdatei verwendet werden soll. Sie können eine Schlüsselspeicherdatei mit einem selbstsignierten Zertifikat oder einem von einer Zertifizierungsbehörde signierten Zertifikat verwenden. 1 – Von Installationsprogramm generierten Schlüsselspeicher verwenden 2 – Schlüsselspeicherdatei und Passwort eingeben Wenn Sie eine vom Installationsprogramm generierte Schlüsselspeicherdatei verwenden möchten, wird eine selbstsignierte Schlüsselspeicherdatei mit dem Namen „Default.keystore“ in folgendem Speicherort erstellt: `<Informatica-Installationsverzeichnis>/tomcat/conf/`

c. Wenn Sie den Schlüsselspeicher festlegen, geben Sie das Passwort und den Speicherort der Schlüsselspeicherdatei ein.

Wenn Sie die sichere Kommunikation für die Domäne aktiviert haben, wird der Abschnitt **Domänensicherheit – Sichere Kommunikation** angezeigt. Wenn sichere Kommunikation für die Domäne nicht aktiviert wurde, wird der Abschnitt **Domänenkonfiguration** angezeigt. Fahren Sie mit Schritt 21 fort.

20. Geben Sie im Abschnitt „Domänensicherheit – Sichere Kommunikation“ an, ob die standardmäßigen SSL-Zertifikate von Informatica oder eigene SSL-Zertifikate zum Sichern der Domänenkommunikation verwendet werden sollen.

    a. Wählen Sie den Typ der zu verwendenden SSL-Zertifikate aus.

In der folgenden Tabelle werden die SSL-Zertifikatsoptionen zum Sichern der Informatica-Domäne beschrieben:

Option	Beschreibung
SSL-Standardzertifikatsdateien von Informatica verwenden	Verwenden Sie die von Informatica bereitgestellten SSL-Standardzertifikate. **Hinweis:** Wenn Sie kein SSL-Zertifikat bereitstellen, verwendet Informatica denselben privaten Standardschlüssel für alle Informatica-Installationen. Wenn Sie die von Informatica bereitgestellten standardmäßigen Schlüsselspeicher- und Truststore-Dateien verwenden, wird die Sicherheit Ihrer Domäne unter Umständen gefährdet. Um ein hohes Maß an Sicherheit für die Domäne zu gewährleisten, wählen Sie die Option zum Angeben des Speicherorts der SSL-Zertifikatsdateien aus.
Speicherort der SSL-Zertifikatsdateien angeben	Verwenden Sie von Ihnen bereitgestellte SSL-Zertifikate. Sie müssen den Speicherort der Schlüsselspeicher- und Truststore-Dateien angeben. Sie können ein selbstsigniertes Zertifikat oder ein von einer Zertifizierungsstelle ausgegebenes Zertifikat verwenden. Sie müssen SSL-Zertifikate im PEM-Format und in Java-Schlüsselspeicherdateien (JKS) bereitstellen. Informatica benötigt bestimmte Namen für die SSL-Zertifikatsdateien in der Informatica-Domäne. Sie müssen für alle Knoten in der Domäne dieselben SSL-Zertifikate verwenden. Speichern Sie die Truststore- und Schlüsselspeicherdateien in einem Verzeichnis, auf das alle Knoten in der Domäne zugreifen können, und geben Sie für alle Knoten in derselben Domäne dasselbe Schlüsselspeicherdatei- und Truststore-Datei-Verzeichnis an.

b. Wenn Sie das SSL-Zertifikat bereitstellen, geben Sie den Speicherort und die Passwörter der Schlüsselspeicher- und der Truststore-Dateien an.

   In der folgenden Tabelle werden die Parameter beschrieben, die für die SSL-Zertifikatsdateien eingegeben werden müssen:

Eigenschaft	Beschreibung
Schlüsselspeicherdatei-Verzeichnis	Verzeichnis, das die Schlüsselspeicherdateien enthält. Das Verzeichnis muss Dateien mit der Bezeichnung "infa_keystore.jks" und "infa_keystore.pem" enthalten.
Schlüsselspeicherpasswort	Passwort für den Schlüsselspeicher „infa_keystore.jks“.
Verzeichnis der Truststore-Datei	Verzeichnis, das die Truststore-Dateien enthält. Das Verzeichnis muss Dateien mit der Bezeichnung "infa_truststore.jks" und "infa_truststore.pem" enthalten.
Truststore-Passwort	Passwort für die Datei infa_truststore.jks.

Der Abschnitt „Domänen-Konfigurations-Repository“ wird angezeigt.

21. Geben Sie an der Eingabeaufforderung die Informationen für die Domäne ein, zu der Sie eine Verknüpfung herstellen möchten.

In der folgenden Tabelle werden die Eigenschaften beschrieben, die Sie für die Domäne festlegen:

Eigenschaft	Beschreibung
Domänenname	Der Name der zu verknüpfenden Domäne.
Host des Gateway-Knotens	Der Hostname des Computers, der den Gateway-Knoten für die Domäne hostet.
Port des Gateway-Knotens	Die Portnummer des Gateway-Knotens.
Domänenbenutzername	Der Benutzername des Administrators der Domäne, zu der Sie eine Verknüpfung herstellen möchten.
Domänenpasswort	Das Passwort für den Domänenadministrator.

Der Abschnitt „Domänensicherheit – Verschlüsselungsschlüssel“ wird angezeigt.

22. Geben Sie die Daten des Verschlüsselungsschlüssels für die anzufügende Informatica-Domäne ein.

    Wenn der aktuelle Knoten nicht auf den Speicherort des Verschlüsselungsschlüssels im Gateway-Knoten zugreifen kann, kopieren Sie die Verschlüsselungsschlüsseldatei in ein zugängliches Verzeichnis. Möglicherweise müssen Sie eine Leseberechtigung zum Verzeichnis hinzufügen, das die Verschlüsselungsschlüsseldatei auf dem Gateway-Knoten enthält, bevor Sie die Datei kopieren können. Weitere Informationen über die Berechtigungen für die Verschlüsselungsschlüsseldatei und das Verzeichnis finden Sie unter “Sichere Dateien und Verzeichnisse” auf Seite 107.

    In der folgenden Tabelle werden die Verschlüsselungsschlüsselparameter beschrieben, die beim Hinzufügen einer Domäne angegeben werden müssen:

Eigenschaft	Beschreibung
Auswählen des Verschlüsselungsschlüssels	Pfad und Dateiname des Verschlüsselungsschlüssels für die Informatica-Domäne, der Sie beitreten möchten. Alle Knoten in der Informatica-Domäne verwenden den gleichen Verschlüsselungsschlüssel. Sie müssen die Verschlüsselungsschlüsseldatei festlegen, die auf dem Gateway-Knoten für die Domäne erstellt wurde, der Sie beitreten möchten. Wenn Sie die Verschlüsselungsschlüsseldatei in ein temporäres Verzeichnis kopiert haben, damit sie für die Knoten in der Domäne zugänglich ist, geben Sie den Pfad und den Dateinamen der Verschlüsselungsschlüsseldatei im temporären Verzeichnis an.
Verzeichnis des Verschlüsselungsschlüssels	Verzeichnis zum Speichern des Verschlüsselungsschlüssels auf dem während dieser Installation erstellten Knoten. Das Installationsprogramm kopiert die Verschlüsselungsschlüsseldatei für die Domäne in das Verzeichnis des Verschlüsselungsschlüssels auf dem neuen Knoten. Standardmäßig wird der Verschlüsselungsschlüssel in folgendem Verzeichnis erstellt: `<Informatica-Installationsverzeichnis>/isp/config/keys`.

23. Geben Sie im Abschnitt „Mit Domäne verknüpfen – Knotenkonfiguration“ die Informationen für den zu erstellenden Knoten ein.

In der folgenden Tabelle werden die Eigenschaften beschrieben, die Sie für den Knoten festlegen:

Eigenschaft	Beschreibung
Knoten-Hostname	Hostname für den Knoten. Der Hostname des Knotens darf keine Unterstriche (_) enthalten. **Hinweis:** Verwenden Sie nicht localhost. Der Hostname muss den Computer eindeutig kennzeichnen.
Knotenname	Der Name des auf diesem Computer zu erstellenden Informatica-Knotens. Der Knotenname ist nicht mit dem Hostnamen des Computers identisch.
Knoten-Portnummer	Die Portnummer für den Knoten.
Datenbank-Truststore-Datei	Pfad und Dateiname der Truststore-Datei für die sichere Datenbank. Wählen Sie dieselbe Datenbank-Truststore-Datei aus, die vom Master-Gateway-Knoten in der Domäne verwendet wird. Erforderlich, wenn Sie einen Gateway-Knoten mit einer Domäne verbinden, die ein sicheres Domänenkonfigurations-Repository verwendet.
Truststore-Passwort	Passwort für die Datenbank-Truststore-Datei für die sichere Datenbank. Erforderlich, wenn Sie einen Gateway-Knoten mit einer Domäne verbinden, die ein sicheres Domänenkonfigurations-Repository verwendet.

24. Legen Sie fest, ob die vom Installer zugewiesenen Standardports für die Domänen- und Knotenkomponenten angezeigt werden sollen.

    In der folgenden Tabelle wird die Seite „Erweiterte Port-Konfiguration“ beschrieben:

Eingabeaufforderung	Beschreibung
Anzeigen der Seite „Erweiterte Port-Konfiguration“	Legen Sie fest, ob die vom Installationsprogramm zugewiesenen Portnummern für die Domänen- und Knotenkomponenten angezeigt werden sollen: 1 – Nein 2 – Ja Wenn Sie „Ja“ auswählen, zeigt das Installationsprogramm die Standard-Portnummern an, die den Domänenkomponenten zugewiesen sind. Sie können die für die Domänen- und Knotenkomponenten zu verwendenden Portnummern festlegen. Sie können für den Dienstprozess, der auf dem Knoten laufen wird, auch einen Bereich für Portnummern festlegen. Sie können die Standard-Portnummern verwenden oder neue Portnummern festlegen. Stellen Sie sicher, dass die eingegebenen Portnummern nicht bereits von anderen Anwendungen verwendet werden.

25. Wenn Sie die Seite „Portkonfiguration“ anzeigen, geben Sie an der Eingabeaufforderung die neuen Portnummern ein oder drücken Sie die **Eingabetaste**, um die Standardportnummern zu verwenden.

In der folgenden Tabelle werden die Ports beschrieben, die von Ihnen festgelegt werden können:

Port	Beschreibung
Dienstmanager-Port	Portnummer, die vom Dienstmanager auf dem Knoten verwendet wird. Der Dienstmanager überwacht eingehende Verbindungsanfragen auf diesem Port. Clientanwendungen verwenden diesen Port zur Kommunikation mit den Diensten in dieser Domäne. Die Informatica-Befehlszeilenprogramme verwenden diesen Port für die Kommunikation mit der Domäne. Dies ist auch der Port für den JDBC-/ODBC-Treiber des SQL-Datendiensts. Standardwert ist 6006.
Schließungsport des Dienstmanagers	Portnummer, die das Herunterfahren des Servers für den Dienstmanager der Domäne steuert. An diesem Port wartet der Dienstmanager auf Ausschaltbefehle. Standardwert ist 6007.
Informatica Administrator-Port	Portnummer von Informatica Administrator. Standardwert ist 6008.
Informatica Administrator-Schließungsport	Portnummer, die das Herunterfahren des Servers für Informatica Administrator steuert. Informatica Administrator überwacht Befehle zum Herunterfahren auf diesem Port. Standardwert ist 6009.
Niedrigste Portnummer	Niedrigste Portnummer des dynamischen Portnummernbereichs, die den Anwendungsdienstprozessen, die auf diesem Knoten laufen, zugewiesen werden kann. Standardwert ist 6014.
Höchste Portnummer	Höchste Portnummer des dynamischen Portnummernbereichs, die den Anwendungsdienstprozessen, die auf diesem Knoten laufen, zugewiesen werden kann. Standardwert ist 6114.

Die Installations-Zusammenfassung zeigt an, ob die Installation erfolgreich abgeschlossen wurde. Es zeigt außerdem den Status der installierten Komponenten und deren Konfiguration an. In den Protokolldateien der Installation finden Sie weitere Informationen über die vom Installationsprogramm ausgeführten Aufgaben und die Konfigurationseigenschaften der installierten Komponenten.

Standardmäßig sind die Systemdienste nach Abschluss der Installation deaktiviert. Sie müssen sie im Administrator Tool aktivieren.

Automatisches Installieren der Informatica-Dienst

Beim automatischen Installieren der Informatica-Dienste ist keinerlei Benutzereingriff erforderlich. Geben Sie die Installationsoptionen mithilfe einer Eigenschaftendatei an. Das Installationsprogramm liest die Datei, um die Installationsoptionen zu ermitteln. Mit der automatischen Installation können Sie die Informatica-Dienste auf mehreren Computern im Netzwerk installieren oder die Installation auf den verschiedenen Computern standardisieren.

Kopieren Sie die Informatica-Installationsdateien auf die Festplatte des Computers, auf dem Sie Informatica installieren möchten. Stellen Sie bei der Installation auf einem Remotecomputer sicher, dass Sie darauf zugreifen und Dateien erstellen können.

Gehen Sie zum automatischen Installieren folgendermaßen vor:

1. Konfigurieren Sie die Installationseigenschaftendatei und geben Sie darin die Installationsoptionen an.
2. Führen Sie das Installationsprogramm mit der Installationseigenschaftendatei aus.

3. Sichern Sie die Passwörter in der Installationseigenschaftendatei.

Konfigurieren der Eigenschaftendatei

Informatica stellt eine Beispiel-Eigenschaftendatei mit den vom Installer benötigten Parametern bereit. Sie können die Beispiel-Eigenschaftendatei mit den gewünschten Optionen für Ihre Installation anpassen. Führen Sie anschließend die Installation im Hintergrund aus.

Die Beispieldatei „SilentInput.properties“ befindet sich im Root-Verzeichnis auf der DVD oder im Downloadverzeichnis des Installationsprogramms. Nachdem Sie die Datei angepasst haben, speichern Sie sie unter dem Namen SilentInput.properties.

1. Wechseln Sie zum Root-Verzeichnis, das die Installationsdateien enthält.
2. Suchen Sie die Beispieldatei `SilentInput.properties`.
3. Erstellen Sie eine Sicherungskopie der Datei „SilentInput.properties“.
4. Öffnen Sie die Datei in einem Texteditor und ändern Sie die Werte der Installationsparameter.

   In der folgenden Tabelle werden die Installationsparameter beschrieben, die Sie ändern können:

Eigenschaftsname	Beschreibung
LICENSE_KEY_LOC	Der absolute Pfad und Dateiname der Lizenzschlüsseldatei.
USER_INSTALL_DIR	Das Verzeichnis, in dem Informatica installiert werden soll.
INSTALL_TYPE	Zeigt an, ob Informatica installiert oder upgegradet werden soll. Bei einem Wert von 0 wird Informatica von Grund auf neu installiert. Bei einem Wert von 1 wird ein Upgrade einer Vorgängerversion von Informatica vorgenommen.
ENABLE_KERBEROS	Gibt an, ob die Informatica-Domäne für die Ausführung in einem Netzwerk mit Kerberos-Authentifizierung konfiguriert werden soll. Setzen Sie diesen Parameter auf 1, um die Informatica-Domäne für die Ausführung in einem Netzwerk mit Kerberos-Authentifizierung zu konfigurieren.
SERVICE_REALM_NAME	Name des Kerberos-Bereichs, zu dem die Informatica-Domänendienste gehören. Die Namen des Dienst- und Benutzerbereichs müssen übereinstimmen.
USER_REALM_NAME	Name des Kerberos-Bereichs, zu dem die Informatica-Domänenbenutzer gehören. Die Namen des Dienst- und Benutzerbereichs müssen übereinstimmen.
KEYTAB_LOCATION	Verzeichnis, in dem alle Keytab-Dateien für die Informatica-Domäne gespeichert werden. Der Name einer Keytab-Datei in der Informatica-Domäne muss einem von Informatica festgelegten Format entsprechen.

Eigenschaftsname	Beschreibung
KRB5_FILE_LOCATION	Pfad und Dateiname der Kerberos-Konfigurationsdatei. Informatica benötigt folgenden Namen für die Kerberos-Konfigurationsdatei: krb5.conf
SPN_SHARE_LEVEL	Gibt die Dienst-Prinzipalebene für die Domäne an. Legen Sie eine der folgenden Ebenen für die Eigenschaft fest: - Prozess Die Domäne erfordert einen eindeutigen Dienst-Prinzipalnamen (SPN) und eine Keytab-Datei für jeden Knoten und für jeden Dienst auf einem Knoten. Die Anzahl der pro Knoten erforderlichen SPNs und Keytab-Dateien hängt von der Anzahl der Dienstprozesse ab, die auf dem Knoten ausgeführt werden. Empfohlen für Produktionsdomänen. - Knoten. Die Domäne verwendet einen SPN und eine Keytab-Datei für den Knoten und für alle Dienste, die auf dem Knoten ausgeführt werden. Sie erfordert außerdem einen separaten SPN und eine separate Keytab-Datei für alle HTTP-Prozesse auf dem Knoten. Empfohlen für Test- und Entwicklungsdomänen. Standardwert ist „Prozess“.
HTTPS_ENABLED	Zeigt an, ob die Verbindung zu Informatica Administrator gesichert werden muss. Bei einem Wert von 0 wird eine ungesicherte HTTP-Verbindung zu Informatica Administrator hergestellt. Bei einem Wert von 1 wird eine gesicherte HTTPS-Verbindung zu Informatica Administrator hergestellt.
DEFAULT_HTTPS_ENABLED	Zeigt an, ob eine Schlüsselspeicherdatei erstellt wird. Bei einem Wert von 1 wird vom Installationsprogramm ein Schlüsselspeicher erstellt und für die HTTPS-Verbindung verwendet. Bei einem Wert von 0 wird vom Installationsprogramm eine von Ihnen angegebene Schlüsselspeicherdatei verwendet.
CUSTOM_HTTPS_ENABLED	Zeigt an, ob eine vorhandene Schlüsselspeicherdatei verwendet wird. Bei einem Wert von 1 wird vom Installationsprogramm eine von Ihnen angegebene Schlüsselspeicherdatei verwendet. Falls DEFAULT_HTTPS_ENABLED=1 müssen Sie diesen Parameter auf 0 setzen. Falls DEFAULT_HTTPS_ENABLED=0 müssen Sie diesen Parameter auf 1 setzen.
KSTORE_PSSWD	Klartextpasswort für die Schlüsselspeicherdatei.
KSTORE_FILE_LOCATION	Der absolute Pfad und Dateiname der Schlüsselspeicherdatei.
HTTPS_PORT	Zu verwendende Portnummer für die gesicherte Verbindung zu Informatica Administrator.

Eigenschaftsname	Beschreibung
CREATE_DOMAIN	Zeigt an, ob eine Informatica-Domäne erstellt werden soll. Bei einem Wert von 1 werden vom Installationsprogramm ein Knoten und eine Informatica-Domäne erstellt. Bei einem Wert von 0 wird vom Installationsprogramm ein Knoten erstellt und an eine andere bei einer früheren Installation erstellte Domäne angefügt.
KEY_DEST_LOCATION	Verzeichnis zum Speichern des Verschlüsselungsschlüssels auf dem Knoten, der während der Installation erstellt wurde.
PASS_PHRASE_PASSWD	Schlüsselwort zum Erstellen eines Verschlüsselungsschlüssels für die Sicherung vertraulicher Daten in der Domäne. Das Schlüsselwort muss die folgenden Kriterien erfüllen: - Hat eine Länge von 8 bis 20 Zeichen - Enthält mindestens einen Großbuchstaben - Enthält mindestens einen Kleinbuchstaben - Enthält mindestens eine Zahl - Enthält keine Leerzeichen
JOIN_DOMAIN	Zeigt an, ob der Knoten an eine andere bei einer früheren Installation erstellte Domäne angefügt werden soll. Bei einem Wert von 1 wird vom Installationsprogramm ein Knoten erstellt und an eine Domäne angefügt. Falls CREATE_DOMAIN=1 müssen Sie diesen Parameter auf 0 setzen. Falls CREATE_DOMAIN=0 müssen Sie diesen Parameter auf 1 setzen.
KEY_SRC_LOCATION	Verzeichnis, das den Verschlüsselungsschlüssel auf dem Master-Gateway-Knoten der anzufügenden Informatica-Domäne enthält.
SSL_ENABLED	Aktiviert oder deaktiviert sichere Kommunikation zwischen Diensten in der Informatica-Domäne. Zeigt an, ob eine gesicherte Kommunikation zwischen Diensten in der Domäne eingerichtet werden soll. Bei einem Wert "true" ist die gesicherte Kommunikation zwischen Diensten in der Domäne aktiviert. Bei CREATE_DOMAIN=1 können Sie diese Eigenschaft auf "true" setzen. Bei JOIN_DOMAIN=1 müssen Sie diese Eigenschaft auf "true" setzen.
SECURITY_DOMAIN_NAME	Name der standardmäßigen Sicherheitsdomäne in der Domäne, der Sie den erstellten Knoten anfügen.
TLS_CUSTOM_SELECTION	Gibt an, ob von Ihnen bereitgestellte SSL-Zertifikate zum Aktivieren sicherer Kommunikation in der Informatica-Domäne verwendet werden sollen. Setzen Sie diese Eigenschaft auf TRUE, um die von Ihnen bereitgestellten SSL-Zertifikate zu verwenden.

Eigenschaftsname	Beschreibung
NODE_KEYSTORE_DIR	Erforderlich, wenn TLS_CUSTOM_SELECTION auf TRUE gesetzt ist. Verzeichnis, das die Schlüsselspeicherdateien enthält. Das Verzeichnis muss Dateien mit der Bezeichnung "infa_keystore.jks" und "infa_keystore.pem" enthalten.
NODE_KEYSTORE_PASSWD	Erforderlich, wenn TLS_CUSTOM_SELECTION auf TRUE gesetzt ist. Passwort für den Schlüsselspeicher „infa_keystore.jks“.
NODE_TRUSTSTORE_DIR	Erforderlich, wenn TLS_CUSTOM_SELECTION auf TRUE gesetzt ist. Verzeichnis, das die Truststore-Dateien enthält. Das Verzeichnis muss Dateien mit der Bezeichnung "infa_truststore.jks" und "infa_truststore.pem" enthalten.
NODE_TRUSTSTORE_PASSWD	Erforderlich, wenn TLS_CUSTOM_SELECTION auf TRUE gesetzt ist. Passwort für die Datei infa_truststore.jks.
SERVES_AS_GATEWAY	Zeigt an, ob ein Gateway- oder ein Worker-Knoten erstellt werden soll. Bei einem Wert von 1 wird der Knoten vom Installationsprogramm als Gateway-Knoten konfiguriert. Bei einem Wert von 0 wird der Knoten vom Installationsprogramm als Worker-Knoten konfiguriert.
DB_TYPE	Datenbank des Domänenkonfigurations-Repositorys. Geben Sie einen der folgenden Werte ein: - Oracle - MSSQLServer - DB2 - Sybase
DB_UNAME	Name des Datenbankbenutzerkontos für das Domänenkonfigurations-Repository.
DB_PASSWD	Das Passwort für das Datenbankbenutzerkonto.
DB_SSL_ENABLED	Gibt an, ob die Datenbank für das Domänen-Konfigurations-Repository sicher ist. Setzen Sie diesen Parameter auf TRUE, um das Domänen-Konfigurations-Repository in einer sicheren Datenbank zu erstellen. Wenn dieser Parameter auf TRUE gesetzt ist, müssen Sie die JDBC-Verbindungszeichenfolge mit den Parametern der sicheren Datenbank bereitstellen.
TRUSTSTORE_DB_FILE	Pfad und Dateiname der Truststore-Datei für die sichere Domänen-Konfigurations-Repositorydatenbank. Wenn die Domäne, die Sie erstellen oder der Sie beitreten, ein sicheres Domänen-Konfigurations-Repository verwendet, legen Sie diese Eigenschaft mit der Truststore-Datei der Repository-Datenbank fest.
TRUSTSTORE_DB_PASSWD	Passwort der Truststore-Datei für die sichere Domänen-Konfigurations-Repositorydatenbank.

Eigenschaftsname	Beschreibung
SQLSERVER_SCHEMA_NAME	Für Microsoft SQL Server. Der Name des Schemas, das Domänenkonfigurationstabellen enthalten soll. Ist dieser Parameter leer, werden die Tabellen im Standardschema erstellt.
TRUSTED_CONNECTION	Für Microsoft SQL Server. Zeigt an, ob eine vertrauenswürdige Verbindung zu Microsoft SQL Server hergestellt werden soll. Ist dieser Parameter leer, verwendet das Installationsprogramm Microsoft SQL Server-Authentifizierung. Richten Sie diesen Parameter nur bei einer Installation unter Windows ein.
DB2_TABLESPACE	Für IBM DB2. Der Name des Tablespace, in dem die Tabellen erstellt werden sollen. Geben Sie einen Tablespace an, der die Anforderungen an die Seitengröße (pageSize) von 32768 Byte erfüllt. Wenn DB2_TABLESPACE in einer Datenbank mit einer einzigen Partition leer ist, erstellt das Installationsprogramm die Tabellen im Standard-Tablespace. Definieren Sie in einer Datenbank mit mehreren Partitionen den Tablespace in der Katalogpartition der Datenbank.
DB_CUSTOM_STRING_SELECTION	Legt fest, ob eine JDBC-URL oder eine benutzerdefinierter Verbindungszeichenfolge für die Verbindung zur Domänenkonfigurationsdatenbank verwendet werden soll. Bei einem Wert von 0 erstellt das Installationsprogramm anhand der angegebenen Datenbankeigenschaften eine JDBC-URL. Bei einem Wert von 1 wird die angegebene benutzerdefinierte Verbindungszeichenfolge verwendet. Setzen Sie diesen Parameter auf 1, wenn Sie das Domänen-Konfigurations-Repository in einer sicheren Datenbank erstellen.
DB_SERVICENAME	Erforderlich, wenn DB_CUSTOM_STRING_SELECTION=0. Dienstname für Oracle- und IBM DB2-Datenbanken. Der Datenbankname für Microsoft SQL Server und Sybase ASE.
DB_ADDRESS	Erforderlich, wenn DB_CUSTOM_STRING_SELECTION=0. Hostname und Portnummer für die Datenbankinstanz im Format *HostName*:*Port*.

Eigenschaftsname	Beschreibung
ADVANCE_JDBC_PARAM	Sie können diesen Parameter einstellen, wenn DB_CUSTOM_STRING_SELECTION=0 ist. Optionale Parameter, die in die JDBC-URL-Verbindungszeichenfolge aufgenommen werden können. Überprüfen Sie die Gültigkeit der Parameterzeichenfolge. Das Installationsprogramm führt vor dem Hinzufügen der Parameterzeichenfolge zur JDBC-URL keine Überprüfung der Zeichenfolge durch. Ist dieser Parameter leer, wird die JDBC-URL vom Installationsprogramm ohne zusätzliche Parameter erstellt.
DB_CUSTOM_STRING	Erforderlich, wenn DB_CUSTOM_STRING_SELECTION=1. Der gültige benutzerdefinierte JDBC-Verbindungs-String.
DOMAIN_NAME	Wenn Sie eine Domäne erstellen, der Name der zu erstellenden Domäne. Wenn Sie einer Domäne beitreten, Name der anzufügenden Domäne, die in einer früheren Installation erstellt wurde. Der Standard-Domänenname lautet Domain_<*MachineName*>. Der Name darf maximal 128 Zeichen umfassen und muss im 7-Bit-ASCII-Format vorliegen. Er darf weder Leerzeichen noch die folgenden Zeichen enthalten: ` % * + ; " ? , < > \ /
DOMAIN_HOST_NAME	Bei Erstellung einer Domäne ist dies der Hostname des Rechners, auf dem der Knoten erstellt werden soll. Der Hostname des Knotens darf keine Unterstriche (_) enthalten. Wenn der Computer nur einen Netzwerknamen aufweist, verwenden Sie den Standardhostnamen. Wenn der Computer mehrere Netzwerknamen aufweist, können Sie den Standardhostnamen ändern und einen alternativen Netzwerknamen verwenden. Optional können Sie die IP-Adresse verwenden. Bei Anfügen einer Domäne ist dies der Hostname des Rechners, auf dem sich der Gateway-Knoten der anzufügenden Domäne befindet. Hinweis: Verwenden Sie nicht localhost. Der Hostname muss den Computer eindeutig kennzeichnen.
NODE_NAME	Bei CREATE_DOMAIN=1 erforderlich. Name des auf diesem Computer zu erstellenden Knotens. Der Knotenname ist nicht mit dem Hostnamen des Computers identisch.
DOMAIN_PORT	Bei Erstellung einer Domäne ist dies die Portnummer für den zu erstellenden Knoten. Die Standard-Portnummer für den Knoten lautet 6005. Wenn die Standard-Portnummer auf dem Rechner nicht verfügbar ist, wird die nächste verfügbare Portnummer angezeigt. Bei Anfügen einer Domäne ist dies die Portnummer des Gateway-Knotens der anzufügenden Domäne.

Eigenschaftsname	Beschreibung
DOMAIN_USER	Benutzername für den Domänenadministrator. Bei Erstellung einer Domäne können Sie diesen Benutzernamen für Ihre Erstanmeldung bei Informatica Administrator verwenden. Beachten Sie folgende Richtlinien: - Beim Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden und er darf nicht mehr als 128 Zeichen umfassen. - Der Name darf weder Tabulatoren und Zeilenendzeichen noch die folgenden Sonderzeichen enthalten: % * + \ / ' . ? ; < > - Der Name kann ein ASCII-Leerzeichen enthalten, jedoch nicht als erstes oder letztes Zeichen. Alle anderen Leerzeichen sind nicht zulässig. Bei Anfügen einer Domäne ist dies der Benutzername, mit dem Sie sich bei der anzufügenden Domäne anmelden.
DOMAIN_PSSWD	Das Passwort für den Domänenadministrator. Das Passwort muss mehr als zwei Zeichen und darf bis zu 16 Zeichen enthalten.
DOMAIN_CNFRM_PSSWD	Geben Sie das Passwort zur Bestätigung erneut ein.
SAML_AUTHENTICATION	Erforderlich, wenn ENABLE_KERBEROS=0. Legen Sie diesen Parameter auf „True“ fest, um auf Security Assertion Markup Language (SAML) basierte Unterstützung für Single Sign-On (SSO) für webbasierte Informatica-Anwendungen in einer Informatica-Domäne zu konfigurieren. Wenn dieser Parameter auf „True“ festgelegt ist, müssen Sie die IDP-URL angeben.
IDP_URL	Erforderlich, wenn ENABLE_KERBEROS=0 und SAML_AUTHENTICATION=True. Geben Sie die URL des Identitäts-Providers für die Domäne ein.
JOIN_NODE_NAME	Bei JOIN_DOMAIN=1 erforderlich. Name des Knotens, den Sie der Domäne anfügen. Der Knotenname ist nicht mit dem Hostnamen des Computers identisch.
JOIN_HOST_NAME	Bei JOIN_DOMAIN=1 erforderlich. Hostname des Computers, auf dem der Knoten erstellt wird, den Sie der Domäne anfügen. Der Hostname des Knotens darf keine Unterstriche (_) enthalten. Hinweis: Verwenden Sie nicht localhost. Der Hostname muss den Computer eindeutig kennzeichnen.
JOIN_DOMAIN_PORT	Bei JOIN_DOMAIN=1 erforderlich. Die Portnummer des Gateway-Knotens der anzufügenden Domäne.

Eigenschaftsname	Beschreibung
ADVANCE_PORT_CONFIG	Zeigt an, ob die Liste der Portnummern für die Domänen- und Knotenkomponenten angezeigt werden soll. Bei einem Wert von 0 werden den Domänen- und Knotenkomponenten vom Installationsprogramm Standardportnummern zugewiesen. Bei einem Wert von 1 können Sie die Portnummern für die Domänen- und Knotenkomponenten festlegen.
MIN_PORT	Sie können diesen Parameter einrichten, wenn ADVANCE_PORT_CONFIG=1 ist. Niedrigste Portnummer des dynamischen Portnummernbereichs, die den Anwendungsdienstprozessen, die auf diesem Knoten laufen, zugewiesen werden kann.
MAX_PORT	Sie können diesen Parameter einrichten, wenn ADVANCE_PORT_CONFIG=1 ist. Höchste Portnummer des dynamischen Portnummernbereichs, die den Anwendungsdienstprozessen, die auf diesem Knoten laufen, zugewiesen werden kann.
TOMCAT_PORT	Sie können diesen Parameter einrichten, wenn ADVANCE_PORT_CONFIG=1 ist. Portnummer, die vom Dienstmanager auf dem Knoten verwendet wird. Der Dienstmanager überwacht eingehende Verbindungsanfragen auf diesem Port. Clientanwendungen verwenden diesen Port zur Kommunikation mit den Diensten in dieser Domäne. Der Port, den die Informatica-Befehlszeilenprogramme zur Kommunikation mit der Domäne verwenden. Dies ist auch der Port für den JDBC-/ODBC-Treiber des SQL-Datendiensts. Standardwert ist 6006.
AC_PORT	Sie können diesen Parameter einstellen, wenn CREATE_DOMAIN=1 und ADVANCE_PORT_CONFIG=1 ist. Portnummer von Informatica Administrator. Standardwert ist 6007.
SERVER_PORT	Sie können diesen Parameter einrichten, wenn ADVANCE_PORT_CONFIG=1 ist. Portnummer, die das Herunterfahren des Servers für den Dienstmanager der Domäne steuert. An diesem Port wartet der Dienstmanager auf Ausschaltbefehle. Standardwert ist 6008.

Eigenschaftsname	Beschreibung
AC_SHUTDWN_PORT	Sie können diesen Parameter einstellen, wenn CREATE_DOMAIN=1 und ADVANCE_PORT_CONFIG=1 ist. Portnummer, die das Herunterfahren des Servers für Informatica Administrator steuert. Informatica Administrator überwacht Befehle zum Herunterfahren auf diesem Port. Standardwert ist 6009.
ENABLE_USAGE_COLLECTION	Aktiviert das Produktnutzungstool Informatica DiscoveryIQ, das Routineberichte über die Datennutzung und Systemstatistiken an Informatica sendet. Nach der Installation und Konfiguration der Informatica-Domäne lädt Informatica DiscoveryIQ alle 15 Minuten Daten an Informatica hoch. Danach sendet die Domäne die Daten alle 30 Tage. Sie können angeben, dass keine Nutzungsstatistiken an Informatica gesendet werden. Weitere Informationen darüber, wie Sie das Senden von Statistiken an Informatica deaktivieren können, finden Sie im *Informatica Administrator-Handbuch*. Sie müssen den Wert auf 1 festlegen, um den Hotfix anzuwenden.

5. Sie können optional während der Installation einen Modellrepository-Dienst und einen Datenintegrationsdienst erstellen.

   Die folgende Tabelle enthält eine Beschreibung der Eigenschaften, die Sie festlegen, wenn Sie während der Installation einen Modellrepository-Dienst und einen Datenintegrationsdienst erstellen möchten:

Eigenschaft	Beschreibung
CREATE_SERVICES	Ermöglicht das Erstellen des Modellrepository-Diensts und Datenintegrationsdiensts während der Installation. Legen Sie den Wert mit 1 fest, um die Erstellung der Dienste während der Installation zu ermöglichen. Standardwert ist 0.
KERBEROS_SECURITY_DOMAIN_NAME	Kerberos-Sicherheitsdomänenname. Sie müssen den Kerberos-Sicherheitsdomänennamen eingeben, wenn für die Domäne Kerberos-Authentifizierung aktiviert ist.
KERBEROS_DOMAIN_PSSWD	Kerber-Sicherheitsdomänenpasswort. Sie müssen das Kerberos-Sicherheitsdomänenpasswort eingeben, wenn für die Domäne Kerberos-Authentifizierung aktiviert ist.
MRS_DB_TYPE	Der Typ der Modellrepository-Datenbank Geben Sie einen der folgenden Werte ein: - Oracle - DB2 - MSSQLServer
MRS_DB_UNAME	Der Datenbankbenutzername für die Modellrepository-Datenbank.

Eigenschaft	Beschreibung
MRS_DB_PASSWD	Das Passwort für das Datenbankbenutzerkonto.
MRS_DB_SSL_ENABLED	Gibt an, ob die Datenbank, die als Modellrepository-Datenbank verwendet wird, sicher ist. Setzen Sie diesen Parameter auf TRUE, um die Modellrepository-Datenbank als sichere Datenbank zu erstellen. Wenn dieser Parameter auf TRUE gesetzt ist, müssen Sie die JDBC-Verbindungszeichenfolge mit den Parametern der sicheren Datenbank bereitstellen.
MRS_SSL_DEFAULT_STRING	Sicherheitsparameter für die JDBC-Verbindungszeichenfolge, die zur Verbindung mit der Modellrepository-Datenbank verwendet wird. Beispiel: `EncryptionMethod=SSL;HostNameInCertificate=;ValidateServerCertificate=`
TRUSTSTORE_MRS_DB_FILE	Pfad und Dateiname der Truststore-Datei für die sichere Modellrepository-Datenbank.
TRUSTSTORE_MRS_DB_PASSWD	Passwort der Truststore-Datei für die sichere Modellrepository-Datenbank.
MRS_SQLSERVER_SCHEMA_NAME	Für Microsoft SQL Server. Name des Schemas, das die Modellrepository-Tabellen enthält. Ist dieser Parameter leer, werden die Tabellen im Standardschema erstellt.
MRS_DB2_TABLESPACE	Für IBM DB2. Der Name des Tablespace, in dem die Tabellen für das Modellrepository erstellt werden sollen. Geben Sie einen Tablespace an, der die Anforderungen an die Seitengröße (pageSize) von 32768 Byte erfüllt. Wenn DB2_TABLESPACE in einer Datenbank mit einer einzigen Partition leer ist, erstellt das Installationsprogramm die Tabellen im Standard-Tablespace. Definieren Sie in einer Datenbank mit mehreren Partitionen den Tablespace in der Katalogpartition der Datenbank.
MRS_DB_CUSTOM_STRING_SELECTION	Legt fest, ob eine JDBC-URL oder eine benutzerdefinierte Verbindungszeichenfolge für die Verbindung mit der Modellrepository-Datenbank verwendet werden soll. Bei einem Wert von 0 erstellt das Installationsprogramm anhand der angegebenen Datenbankeigenschaften eine JDBC-URL. Bei einem Wert von 1 wird die angegebene benutzerdefinierte Verbindungszeichenfolge verwendet. Setzen Sie diesen Parameter auf 1, wenn Sie die Modellrepository-Datenbank als sichere Datenbank erstellen.

Eigenschaft	Beschreibung
MRS_DB_SERVICENAME	Dienst oder Datenbankname für die Modellrepository-Datenbank. Bei MRS_DB_CUSTOM_STRING_SELECTION=0 erforderlich. Wenn das Modellrepository auf einer Oracle- IBM DB2-Datenbank eingerichtet ist, legen Sie die Eigenschaft mit dem Dienstnamen fest. Wenn das Modellrepository auf einer Microsoft SQL Server- oder Sybase ASE-Datenbank eingerichtet ist, legen Sie die Eigenschaft mit dem Datenbanknamen fest.
MRS_DB_ADDRESS	Bei MRS_DB_CUSTOM_STRING_SELECTION=0 erforderlich. Hostname und Portnummer für die Datenbankinstanz im Format *HostName*:*Port*.
MRS_ADVANCE_JDBC_PARAM	Sie können diesen Parameter einrichten, wenn MRS_DB_CUSTOM_STRING_SELECTION=0 ist. Optionale Parameter, die in die JDBC-URL-Verbindungszeichenfolge aufgenommen werden können. Überprüfen Sie die Gültigkeit der Parameterzeichenfolge. Das Installationsprogramm führt vor dem Hinzufügen der Parameterzeichenfolge zur JDBC-URL keine Überprüfung der Zeichenfolge durch. Ist dieser Parameter leer, wird die JDBC-URL vom Installationsprogramm ohne zusätzliche Parameter erstellt.
MRS_DB_CUSTOM_STRING	Bei MRS_DB_CUSTOM_STRING_SELECTION=1 erforderlich. Der gültige benutzerdefinierte JDBC-Verbindungs-String.
MRS_SERVICE_NAME	Name des Modellrepository-Diensts.
MRS_KEYTAB_FILELOC	Erforderlich, wenn ENABLE_KERBEROS=1 und SPN_SHARE_LEVEL=PROCESS Verzeichnis, in dem die Keytab-Datei für den Modellrepository-Dienst gespeichert ist. Der Name einer Keytab-Datei in der Informatica-Domäne muss einem von Informatica festgelegten Format entsprechen.
DIS_SERVICE_NAME	Name des Datenintegrationsdiensts.
DIS_KEYTAB_FILELOC	Erforderlich, wenn ENABLE_KERBEROS=1 und SPN_SHARE_LEVEL=PROCESS Das Verzeichnis, in dem die Keytab-Datei für den Datenintegrationsdienst gespeichert ist. Der Name einer Keytab-Datei in der Informatica-Domäne muss einem von Informatica festgelegten Format entsprechen.
DIS_PROTOCOL_TYPE	HTTP-Protokolltyp des Datenintegrationsdiensts. Verwenden Sie einen der folgenden Werte: - http - https - Beide

Eigenschaft	Beschreibung
DIS_HTTP_PORT	Erforderlich, wenn DIS_PROTOCOL_TYPE http oder beides ist. HTTP-Port des Datenintegrationsdiensts.
DIS_HTTPS_PORT	Erforderlich, wenn DIS_PROTOCOL_TYPE https oder beides ist. HTTP-Port des Datenintegrationsdiensts.
DIS_CUSTOM_SELECTION	Optionaler Parameter, wenn Sie den Wert von DIS_PROTOCOL_TYPE mit https oder beiden festlegen. Wenn Sie den Wert auf „true“ setzen, übergeben Sie die SSL-Zertifikate, um den Datenintegrationsdienst zu schützen. Sie müssen die zu benutzenden KeyStore- und Truststore-Dateien bereitstellen, um den Datenintegrationsdienst zu schützen.
DIS_KEYSTORE_DIR	Erforderlich, wenn DIS_CUSTOM_SELECTION auf TRUE gesetzt ist. Der Speicherort der KeyStore-Datei für den Datenintegrationsdienst.
DIS_KEYSTORE_PASSWD	Erforderlich, wenn DIS_CUSTOM_SELECTION auf TRUE gesetzt ist. Das Passwort der KeyStore-Datei für den Datenintegrationsdienst.
DIS_TRUSTSTORE_DIR	Erforderlich, wenn DIS_CUSTOM_SELECTION auf TRUE gesetzt ist. Der Speicherort der Truststore-Datei für den Datenintegrationsdienst.
DIS_TRUSTSTORE_PASSWD	Erforderlich, wenn DIS_CUSTOM_SELECTION auf TRUE gesetzt ist. Das Passwort der Truststore-Datei für den Datenintegrationsdienst.

6. Geben Sie unter Windows an, ob der Informatica-Dienst unter demselben Benutzerkonto ausgeführt werden soll wie unter dem Konto, das für die Installation verwendet wurde.

In der folgenden Tabelle werden die Eigenschaften beschrieben, die Sie festlegen, wenn Sie den Informatica-Dienst unter einem anderen Benutzerkonto ausführen möchten:

Eigenschaft	Beschreibung
USE_LOGIN_DETAILS	Gibt an, ob der Windows-Dienst unter einem anderen Benutzerkonto ausgeführt werden soll. Bei einem Wert von 0 konfiguriert das Installationsprogramm den Dienst so, dass er unter dem aktuellen Benutzerkonto ausgeführt wird. Bei einem Wert von 1 konfiguriert das Installationsprogramm den Dienst so, dass er unter einem anderen Benutzerkonto ausgeführt wird.
WIN_USER_ID	Das Benutzerkonto, unter dem der Informatica-Windows-Dienst ausgeführt werden soll. Verwenden Sie das folgende Format: `<domain name>\<user account>` Dieses Benutzerkonto muss „Aktion“ als Betriebssystemberechtigung aufweisen.
WIN_USER_PSSWD	Das Passwort zum Benutzerkonto, unter dem der Informatica-Windows-Dienst ausgeführt werden soll.

7. Speichern Sie die Eigenschaftendatei unter dem Namen „SilentInput.properties“.

Ausführen des automatischen Installationsprogramms

Öffnen Sie nach dem Konfigurieren der Eigenschaftendatei eine Eingabeaufforderung, um die automatische Installation zu starten.

1. Öffnen Sie die Eingabeaufforderung.

   Öffnen Sie unter Windows die Eingabeaufforderung als Administrator. Wenn Sie die Eingabeaufforderung nicht als Administrator öffnen, meldet der Windows-Systemadministrator möglicherweise Probleme, wenn Sie auf die Dateien im Informatica-Installationsverzeichnis zugreifen.
2. Wechseln Sie zum Root-Verzeichnis, das die Installationsdateien enthält.
3. Stellen Sie sicher, dass das Verzeichnis die Datei SilentInput.properties enthält, die Sie bearbeitet und erneut gespeichert haben.
4. Führen Sie die automatische Installation aus. Führen Sie unter Windows silentInstall.bat aus. Führen Sie unter UNIX silentInstall.sh. aus.

Die automatische Installation wird im Hintergrund ausgeführt. Der Vorgang kann eine Weile dauern. Die automatische Installation ist abgeschlossen, wenn die Datei Informatica_<Version>_Services_InstallLog<Zeitstempel>.log im Installationsverzeichnis erstellt ist.

Die automatische Installation schlägt fehl, wenn die Eigenschaftendatei nicht ordnungsgemäß konfiguriert oder der Zugriff auf das Installationsverzeichnis nicht möglich ist. Zeigen Sie die Installationsprotokolldateien an und korrigieren Sie die Fehler. Führen Sie die automatische Installation anschließend noch einmal aus.

Sichern der Passwörter in der Eigenschaftendatei

Stellen Sie nach dem Ausführen des automatischen Installationsprogramms sicher, dass die Passwörter in der Eigenschaftendatei gesichert sind.

Beim Konfigurieren der Eigenschaftendatei für eine automatische Installation geben Sie die Passwörter in Klartext ein. Nachdem Sie das automatische Installationsprogramm ausgeführt haben, verwenden Sie eine der folgenden Methoden zum Sichern der Passwörter:

- Entfernen Sie die Passwörter aus der Eigenschaftendatei.
- Löschen Sie die Eigenschaftendatei.
- Speichern Sie die Eigenschaftendatei an einem sicheren Speicherort.

KAPITEL 8

Fehlerbehebung

Dieses Kapitel umfasst die folgenden Themen:

- Behebung von Problemen bei der Installation - Übersicht, 169
- Fehlerbehebung bei Installationsprotokolldateien, 169
- Fehlerbehebung von Domänen und Knoten, 171

Behebung von Problemen bei der Installation - Übersicht

Das Thema in diesem Abschnitt enthält Informationen zur Fehlerbehebung bei möglichen Problemen, die während der Installation von Informatica unter Umständen auftreten können. Die Beispiele in diesem Thema beschreiben allgemeine Strategien zur Fehlerbehebung und stellen keine vollständige Liste der möglichen Ursachen von Installationsproblemen dar.

Fehlerbehebung bei Installationsprotokolldateien

Folgende Protokolldateien können zur Fehlerbehebung einer Informatica-Installation verwendet werden:

Installations-Protokolldateien

Protokolldateien werden während und nach einer Installation erstellt. Sie bieten Ihnen Aufschluss über die vom Installationsprogramm durchgeführten Aufgaben und während der Installation aufgetretene Fehler. Die Installations-Protokolldateien enthalten die folgenden Protokolle:

- Debug-Protokolle
- Datei-Installationsprotokolle

Dienstmanager-Protokolldateien

Protokolldateien werden generiert, wenn der Dienstmanager auf einem Knoten startet.

Debug-Protokolldateien

Das Installationsprogramm schreibt Aktionen und Fehler in die Debug-Protokolldatei. Der Name der Protokolldatei hängt von der installierten Informatica-Komponente ab.

In der nachstehenden Tabelle sind die Eigenschaften der Debug-Protokolldatei beschrieben:

Eigenschaft	Beschreibung
Name der Log-Datei	- Informatica_<Version>_Services.log - Informatica_<Version>_Client.log - Informatica_<Version>_Services_Upgrade.log - Informatica_<Version>_Services_Upgrade.log
Speicherort	Installationsverzeichnis
Verwendung	Erhalt von weiteren Informationen zu den vom Installationsprogramm durchgeführten Aktionen und zu Installationsfehlern. Während der Installation werden Informationen in diese Datei geschrieben. Wenn das Installationsprogramm einen Fehler generiert, können Sie dieses Protokoll zur Fehlerbehebung hinzuziehen.
Inhalt	Eine ausführliche Zusammenfassung aller vom Installationsprogramm durchgeführten Aktionen, die in das Installationsprogramm eingegebenen Informationen, alle vom Installationsprogramm verwendeten Befehlszeilenbefehle und den vom Befehl zurückgegebenen Fehlercode.

Das Debug-Protokoll enthält die Ausgabe von den Befehlen infacmd und infasetup, mit denen die Domäne, der Knoten und die Anwendungsdienste erstellt wurden. Des Weiteren enthält es Informationen zum Starten der Anwendungsdienste.

Dateiinstallations-Protokolldatei

Die Dateiinstallations-Protokolldatei enthält Informationen zu den installierten Dateien.

In der nachstehenden Tabelle sind die Eigenschaften der Installationsprotokolldatei beschrieben:

Eigenschaft	Beschreibung
Name der Log-Datei	- Informatica_<Version>_Services_InstallLog.log - Informatica_<Version>_Client_InstallLog.log
Speicherort	Installationsverzeichnis
Verwendung	Erhalt von Informationen zu den installierten Dateien und den erstellten Registry-Einträgen.
Inhalt	Die erstellten Verzeichnisse, Namen der installierten Dateien und ausgeführten Befehle und der Status zu jeder installierten Datei.

Service Manager-Protokolldateien

Das Installationsprogramm startet den Informatica-Dienst. Der Informatica-Dienst startet den Service Manager für den Knoten. Der Service Manager generiert Protokolldateien, die Aufschluss über den Startstatus eines Knotens bieten. Mithilfe dieser Dateien können Sie Probleme lösen, wenn der Informatica-Dienst nicht gestartet wird und Sie sich nicht bei Informatica Administrator anmelden können. Die Service Manager-Protokolldateien werden auf jedem Knoten erstellt.

In der nachstehenden Tabelle sind die vom Service Manager generierten Dateien beschrieben:

Eigenschaft	Beschreibung
catalina.out	Zeichnet Ereignisse von der Java Virtual Machine (JVM) auf, die den Dienstmanager ausführt. Beispiel: Ein Port ist während der Installation verfügbar, jedoch beim Start des Dienstmanager in Gebrauch. In diesem Protokoll finden Sie weitere Informationen dazu, welcher Port während des Starts des Dienstmanager nicht verfügbar war. Die catalina.out-Datei befindet sich im folgenden Verzeichnis: `<Informatica-Installationsverzeichnis>/logs/< Knotenname>/catalina.out`
node.log	Zeichnet Ereignisse auf, die während des Starts des Dienstmanager auf einem Knoten generiert wurden. In diesem Protokoll finden Sie weitere Informationen dazu, warum der Dienstmanager zu einem Knoten nicht gestartet wurde. Beispiel: Wenn der Dienstmanager nach 30 Sekunden keine Verbindung zur Domänen-Konfigurations-Datenbank herstellen kann, schlägt das Starten des Dienstmanager fehl. Die Datei node.log befindet sich im Verzeichnis /tomcat/logs.

Hinweis: Der Service Manager verwendet node.log außerdem zum Aufzeichnen von Ereignissen, bei denen der Log Manager nicht verfügbar ist. Beispiel: Wenn der Rechner, auf dem der Service Manager ausgeführt wird, nicht über genügend Speicherplatz zum Schreiben von Protokollereignisdateien verfügt, ist der Log Manager nicht verfügbar.

Fehlerbehebung von Domänen und Knoten

Das Installationsprogramm kann beim Erstellen und Konfigurieren von Domänen und Knoten während der Installation von Informatica Fehler generieren.

Fehler können bei den folgenden Tasks des Installationsprogramms auftreten:

- Hinzufügen des Domänen-Konfigurations-Repository
- Erstellen oder Beitreten einer Domäne
- Starten von Informatica
- Pingen der Domäne
- Hinzufügen einer Lizenz

Erstellen des Domänen-Konfigurations-Repository

Bei Erstellung einer Domäne wird ein Domänen-Konfigurations-Repository erstellt, in dem Metadaten gespeichert werden. Das Installationsprogramm fügt dem Domänen-Konfigurations-Repository entsprechend den von Ihnen während der Installation eingegebenen Optionen Konfigurations-Metadaten hinzu. Das Installationsprogramm kommuniziert mittels JDBC mit der Datenbank. Sie brauchen ODBC oder die native Konnektivität auf dem Rechner, auf dem Sie die Informatica-Dienste installieren, nicht zu konfigurieren.

Zur Überprüfung der Verbindungsinformation erstellt und löscht das Installationsprogramm eine Tabelle im Domänen-Konfigurations-Repository. Das Benutzerkonto für die Datenbank muss über Erstellungsberechtigung in der Datenbankverfügen. Jede Domäne muss über ein separates Domänen-Konfigurations-Repository verfügen.

Erstellen oder Anfügen einer Domäne

Das Installationsprogramm führt je nachdem, ob Sie eine Domäne erstellen oder einer Domäne beitreten, unterschiedliche Tasks durch.

- **Erstellen einer Domäne** Das Installationsprogramm führt den Befehl infasetup DefineDomain zum Erstellen der Domäne und des Gateway-Knotens für die Domäne auf dem aktuellen Rechner basierend auf den im Fenster "Domäne konfigurieren" eingegebenen Daten aus.
- **Beitreten einer Domäne** Das Installationsprogramm führt den Befehl infasetup DefineWorkerNode zum Erstellen eines Knotens auf dem aktuellen Rechner und den Befehl infacmd AddDomainNode zum Hinzufügen des Knotens zur Domäne aus. Die im Fenster "Domäne erstellen" eingegebenen Daten werden zum Ausführen der Befehle verwendet.

Wenn der Gateway-Knoten nicht verfügbar ist, schlagen die Befehle infasetup und infacmd fehl. Ist der Gateway-Knoten nicht verfügbar, können Sie sich nicht bei Informatica Administrator anmelden.

Beispiel: Der Befehl DefineDomain schlägt fehl, wenn Sie auf "Verbindung testen" klicken und der Verbindungstest erfolgreich ist, die Datenbank jedoch vor dem Klicken auf "Weiter" nicht mehr verfügbar ist. Der Befehl DefineDomain kann auch fehlschlagen, wenn der Hostname oder die IP-Adresse nicht zum aktuellen Rechner gehören. Stellen Sie sicher, dass die Datenbank für die Domänenkonfiguration verfügbar und der Hostname richtig ist und wiederholen Sie den Vorgang.

Wenn der Befehl AddDomainNode fehlschlägt, überprüfen Sie, ob der Informatica-Dienst auf dem Knoten ausgeführt wird und wiederholen Sie den Vorgang.

Starten von Informatica

Das Installationsprogramm führt infaservice aus, um die Informatica-Dienste zu starten. Wenn Informatica nicht startet, verwenden Sie die Informationen im Informatica-Debug-Log, um Fehler zu beheben und die Dienst-Manager-Protokolldateien node.log und catalina.out, um die Ursache des Fehlers zu identifizieren.

Wenn Sie eine Domäne erstellen, melden Sie sich bei Informatica Administrator an, nachdem der Informatica-Dienst die Verfügbarkeit der Domäne überprüft hat. Wenn Sie eine Verknüpfung zu einer Domäne herstellen, melden Sie sich bei Informatica Administrator an, nachdem der Informatica-Dienst das erfolgreiche Erstellen und Starten des Knotens überprüft hat.

Wenn Informatica nicht startet, kann das die folgenden Ursachen haben:

- **Der Dienst-Manager hat nicht genügend Systemspeicher.** Die Java-Laufzeitumgebung (Java Runtime Environment, JRE), die Informatica startet und den Dienst-Manager ausführt, hat eventuell nicht genügend Systemspeicher, um zu starten. Setzen Sie die Umgebungsvariable INFA_JAVA_OPTS, um die Größe des von Informatica verwendeten Systemspeichers zu konfigurieren. Unter UNIX können Sie die Speicherkonfiguration beim Start von Informatica festlegen.
- **Die Domänen-Konfigurationsdatenbank ist nicht verfügbar.** Informatica kann auf einem Knoten nicht starten, wenn der Dienst-Manager auf einem Gateway-Knoten nicht innerhalb von 30 Sekunden eine Verbindung zu der Domänen-Konfigurationsdatenbank herstellen kann. Vergewissern Sie sich, dass das Domänenkonfigurations-Repository verfügbar ist.
- **Sie haben das Benutzerkonto des Informatica-Dienstes nicht korrekt konfiguriert.** Informatica kann nicht starten, wenn Sie beim Konfigurieren des Benutzerkontos zum Start des Informatica-Dienstes unter Windows die Windows-Domäne, den Benutzernamen oder das Passwort nicht korrekt konfiguriert haben. Außerdem muss das Benutzerkonto über die Berechtigung „Als Betriebssystem fungieren“ verfügen.
- **Der Inhalt der Umgebungsvariablen PATH überschreitet die maximal zulässige Länge.** Informatica kann unter Windows nicht starten, wenn die von Informatica benötigten Dateien und Bibliotheken sich nicht im Systempfad befinden und daher nicht auf sie zugegriffen werden kann. Dieses Problem kann auftreten,

wenn die gesamte Anzahl der Zeichen in der Umgebungsvariable PATH das zugelassene Limit überschreitet.

- **Einige Ordner im Informatica-Installationsverzeichnis verfügen nicht über die entsprechenden Ausführungsberechtigungen.** Gewähren Sie die Ausführungsberechtigung für das Informatica-Installationsverzeichnis.

Pingen der Domäne

Das Installationsprogramm führt den Ping-Befehl *infacmd* aus, um vor dem Fortsetzen der Installation zu überprüfen, ob die Domäne verfügbar ist. Die Domäne muss verfügbar sein, damit ihr Lizenzobjekte hinzugefügt werden können. Wenn der Ping-Befehl fehlschlägt, starten Sie Informatica auf dem Gateway-Knoten.

Hinzufügen einer Lizenz

Das Installationsprogramm führt den Befehl *infacmd* AddLicense aus, mit dem die Informatica-Lizenzschlüsseldatei gelesen und ein Lizenzobjekt in der Domäne erstellt wird. Zum Ausführen der Anwendungsdienste in Informatica Administrator muss in der Domäne ein gültiges Lizenzobjekt vorliegen.

Wenn Sie eine inkrementelle Lizenz verwenden und eine Domäne anfügen, muss die Seriennummer der inkrementellen Lizenz mit der Seriennummer eines vorhandenen Lizenzobjekts in der Domäne übereinstimmen. Stimmen die Seriennummern nicht überein, schlägt der Befehl AddLicense fehl.

Weitere Informationen zum Inhalt der für die Installation verwendeten Lizenzschlüsseldatei einschließlich Seriennummer, Version, Ablaufdatum, Betriebssystemen und Konnektivitätsoptionen finden Sie im Installations-Debug-Log. Es sind weitere Informationen zu vorhandenen Lizenzen für die Domäne in Informatica Administrator verfügbar.

Teil IV: Nach dem Installieren der Dienste

Dieser Teil enthält die folgenden Kapitel:

- Durchführen der Domänenkonfiguration, 175
- Vorbereiten zum Erstellen der Anwendungsdienste, 182
- Erstellen der Anwendungsdienste, 191

KAPITEL 9

Durchführen der Domänenkonfiguration

Dieses Kapitel umfasst die folgenden Themen:

- Durchführen der Domänenkonfiguration - Übersicht, 175
- Überprüfen der Gebietsschemaeinstellungen und der Codepage-Kompatibilität, 175
- Konfigurieren der Umgebungsvariablen, 177
- Konfigurieren der Windows-Firewall, 180

Durchführen der Domänenkonfiguration - Übersicht

Nach der Installation der Informatica-Dienste und vor dem Erstellen der Anwendungsdienste führen Sie die Konfiguration für die Domänen-Dienste durch.

Zu den Aufgaben der Domänenkonfiguration gehören das Überprüfen der Codepages, das Konfigurieren der Umgebungsvariablen für die Domäne und das Konfigurieren der Firewall.

Überprüfen der Gebietsschemaeinstellungen und der Codepage-Kompatibilität

Die Codepages für Anwendungsdienste müssen mit den Codepages in der Domäne kompatibel sein.

Überprüfen und konfigurieren Sie die Gebietsschemaeinstellungen und Codepages:

Stellen Sie sicher, dass die Domänen-Konfigurationsdatenbank mit den Codeseiten der Anwendungsdienste, die Sie in der Domäne erstellen, kompatibel ist.

Der Dienstmanager 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 Codepage des Anwendungsdiensts nicht erkennt, werden diese Zeichen nicht ordnungsgemäß umgewandelt, was zu Inkonsistenzen führt.

Stellen Sie sicher, dass die Gebietsschemaeinstellungen auf Computern mit Zugriff auf das Administrator-Tool und die Informatica-Client-Tools mit den Codepages der Repositorys in der Domäne kompatibel sind.

Ist die Gebietsschemaeinstellung nicht mit der Codepage für das Repository kompatibel, kann kein Anwendungsdienst erstellt werden.

Überprüfen Sie die Gebietsschemaeinstellungen unter Windows in der Systemsteuerung unter „Region und Sprache“. Weitere Informationen erhalten Sie in der Windows-Dokumentation.

Konfigurieren der lokalen Umgebungsvariablen unter UNIX

Stellen Sie sicher, dass die Gebietsschemaeinstellung mit der Codepage für das Repository kompatibel ist. Ist die Gebietsschemaeinstellung nicht mit der Codepage für das Repository kompatibel, kann kein Anwendungsdienst erstellt werden.

Verwenden Sie LANG, LC_CTYPE oder LC_ALL zum Einrichten der UNIX-Codepage.

Für unterschiedliche UNIX-Betriebssysteme sind unterschiedliche Werte für ein und dasselbe Gebietsschema erforderlich. Beim Wert für die Gebietsschemavariable muss auf Groß- und Kleinschreibung geachtet werden.

Überprüfen Sie mithilfe des folgenden Befehls, ob der Wert der Gebietsschema-Umgebungsvariable mit den Spracheinstellungen des Rechners und des Codeseitentyps kompatibel ist, den Sie für das Repository verwenden möchten:

```
locale -a
```

Der Befehl gibt die auf UNIX-Betriebssystemen installierten Sprachen und die vorhandenen Gebietsschemaeinstellungen zurück.

Richten Sie die folgenden lokalen Umgebungsvariablen ein:

Gebietsschema unter Linux

Zu allen UNIX-Betriebssystemen mit Ausnahme von Linux gibt es zu jedem Gebietsschema einen einmaligen Wert. Unter Linux können unterschiedliche Werte dasselbe Gebietsschema darstellen. So stellen beispielsweise “utf8,” “UTF-8,” “UTF8” und “utf-8” auf einem Linux-Rechner ein und dasselbe Gebietsschema dar. Für Informatica müssen Sie einen speziellen Wert für jedes Gebietsschema auf einem Linux-Rechner verwenden Achten Sie darauf, die Umgebungsvariable LANG entsprechend auf allen Linux-Rechnern einzustellen.

Gebietsschema für Oracle-Datenbank-Clients

Stellen Sie NLS_LANG bei Oracle-Datenbank-Clients auf das Gebietsschema ein, das der Datenbank-Client und -Server bei der Anmeldung verwenden soll. Eine Gebietsschemaeinstellung besteht aus der Sprache, der Region und dem Zeichensatz. Der Wert von NLS_LANG hängt von der Konfiguration ab.

Wenn der Wert beispielsweise american_america.UTF8 lautet, legen Sie die Variable mit dem folgenden Befehl in einer C-Shell fest:

```
setenv NLS_LANG american_america.UTF8
```

Um Multibyte-Zeichen in der Datenbank zu lesen, legen Sie die Variable mit dem folgenden Befehl fest:

```
setenv NLS_LANG=american_america.AL32UTF8
```

Sie müssen die richtige Variable auf dem Rechner des Datenintegrationsdiensts festlegen, damit der Datenintegrationsdienst die Oracle-Daten korrekt lesen kann.

Konfigurieren der Umgebungsvariablen

Informatica verwendet Umgebungsvariablen zum Speichern von Konfigurationsinformationen, wenn es die Anwendungsdienste ausführt und eine Verbindung zu den Clients herstellt. Konfigurieren Sie die Umgebungsvariablen so, dass sie den Anforderungen von Informatica entsprechen.

Falsch konfigurierte Umgebungsvariablen können das Starten der Informatica-Domäne oder der Knoten verhindern oder zu Problemen zwischen den Informatica-Clients und der Domäne führen.

Zum Konfigurieren von Umgebungsvariablen unter UNIX melden Sie sich mit dem Systembenutzerkonto an, mit dem Sie Informatica installiert haben.

Konfigurieren der Informatica-Umgebungsvariablen

Sie können Informatica-Umgebungsvariablen zum Speichern von Speicher-, Domänen- und Speicherorteinstellungen konfigurieren.

Richten Sie die folgenden Umgebungsvariablen ein:

INFA_JAVA_OPTS

Standardmäßig verwendet Informatica maximal 512 MB Systemspeicher.

Die folgende Tabelle listet die Minimalanforderungen für die maximalen Heap-Größeneinstellungen auf, basierend auf der Anzahl der Benutzer und Dienste in der Domäne:

Anzahl der Domänenbenutzernamen	Maximale Heap-Größe (1-5 Dienste)	Maximale Heap-Größe (6-10 Dienste)
Bis zu 1.000	512 MB (Standard)	1024 MB
5,000	2048 MB	3072 MB
10,000	3072 MB	5120 MB
20,000	5120 MB	6144 MB
30,000	5120 MB	6144 MB

Hinweis: Die Einstellungen für die maximale Heap-Größe in der Tabelle basieren auf der Anzahl der Anwendungsdienste in der Domäne.

Wenn die Domäne mehr als 1.000 Benutzer hat, aktualisieren Sie die maximale Heap-Größe basierend auf der Anzahl der Benutzer in der Domäne.

Sie können die Umgebungsvariable INFA_JAVA_OPTS verwenden, um die Größe des von Informatica verwendeten Systemspeichers zu konfigurieren. Um zum Beispiel 1 GB Systemspeicher für den Informatica-Daemon unter UNIX in einer C-Shell zu konfigurieren, verwenden Sie den folgenden Befehl:

```
setenv INFA_JAVA_OPTS "-Xmx1024m"
```

Konfigurieren Sie INFA_JAVA_OPTS unter Windows als Systemvariable.

Starten Sie den Knoten neu, damit die Änderungen wirksam werden.

INFA_DOMAINS_FILE

Das Installationsprogramm erstellt im Informatica-Installationsverzeichnis eine domains.infa-Datei. Die domains.infa-Datei enthält die Konnektivitätsinformationen der Gateway-Knoten in einer Domäne, einschließlich der Domänennamen, Domänenhostnamen und Domänenhostportnummern.

Stellen Sie den Wert der Variable INFA_DOMAINS_FILE auf den Pfad und Dateinamen der Datei domains.infa ein.

Konfigurieren Sie die Variable INFA_DOMAINS_FILE auf dem Computer, auf dem Sie die Informatica-Dienste installieren. Konfigurieren Sie INFA_DOMAINS_FILE unter Windows als Systemvariable.

INFA_HOME

Verwenden Sie INFA_HOME, um das Informatica-Installationsverzeichnis zu bestimmen. Wenn Sie die Informatica-Verzeichnisstruktur verändern, dann müssen Sie die Umgebungsvariable so setzen, dass sie auf den Speicherort des Informatica-Installationsverzeichnisses verweist oder auf das Verzeichnis, in dem sich die installierten Informatica-Dateien befinden.

So verwenden Sie unter UNIX zum Beispiel einen Softlink für alle Informatica-Verzeichnisse. Um INFA_HOME so zu konfigurieren, dass alle Informatica-Anwendungen und -Dienste die auszuführenden anderen Informatica-Komponenten finden, müssen Sie INFA_HOME so setzen, dass es auf das Informatica-Installationsverzeichnis verweist.

INFA_TRUSTSTORE

Wenn Sie sichere Kommunikation für die Domäne aktivieren, legen Sie die Variable INFA_TRUSTSTORE mit dem Verzeichnis fest, das die Truststore-Dateien für die SSL-Zertifikate enthält. Das Verzeichnis muss Truststore-Dateien mit der Bezeichnung „infa_truststore.jks“ und „infa_truststore.pem“ enthalten.

Sie müssen die Variable INFA_TRUSTSTORE einrichten, wenn Sie das von Informatica bereitgestellte SSL-Standardzertifikat oder ein eigenes Zertifikat verwenden.

INFA_TRUSTSTORE_PASSWORD

Wenn Sie sichere Kommunikation für die Domäne aktivieren und das zu verwendende SSL-Zertifikat festlegen, richten Sie die Variable INFA_TRUSTSTORE_PASSWORD mit dem Passwort für die Datei „infa_truststore.jks“ ein, die das SSL-Zertifikat enthält. Das Passwort muss verschlüsselt werden. Verwenden Sie das Befehlszeilenprogramm „pmpasswd“ zum Verschlüsseln des Passworts.

Konfigurieren der Bibliothekspfad-Umgebungsvariablen unter UNIX

Konfigurieren Sie die Bibliothekspfad-Umgebungsvariablen auf den Computern, auf denen die Datenintegrationsdienst-, PowerCenter-Integrationsdienst- und PowerCenter-Repository-Dienst-Prozesse ausgeführt werden. Der Name der Variable und die Anforderungen hängen von der Plattform und der Datenbank ab.

Linux

Konfigurieren Sie die Umgebungsvariable LD_LIBRARY_PATH.

In der nachstehenden Tabelle sind die Werte beschrieben, die Sie für die Umgebungsvariable LD_LIBRARY_PATH für die verschiedenen Datenbanken festlegen:

Datenbank	Wert
Oracle	<*DatabasePath*>/lib
IBM DB2	<*DatabasePath*>/lib
Sybase ASE	"${SYBASE_OCS}/lib:${SYBASE_ASE}/lib:${LD_LIBRARY_PATH}"
Informix	<*DatabasePath*>/lib
Teradata	<*DatabasePath*>/lib
ODBC	<CLOSEDODBCHOME>/lib

AIX

Konfigurieren Sie die Umgebungsvariable LIBPATH für die folgenden Java-basierten Komponenten und Datenbanken:

Java-Komponenten-Variablen

Der PowerCenter-Integrationsdienst erfordert die Java-Laufzeitumgebung-Bibliotheken zum Verarbeiten der folgenden Java-basierten Komponenten:

- Benutzerdefinierte Umwandlungen, die Java verwenden
- Java-Umwandlungen
- PowerExchange®-Adapter, die Java verwenden: PowerExchange for JMS, PowerExchange for Web Services und PowerExchange for webMethods.

Konfigurieren Sie die Bibliothekspfad-Umgebungsvariable so, dass sie auf das installierte Java-Verzeichnis auf Computern verweist, auf denen der PowerCenter-Integrationsdienst-Prozess ausgeführt wird. Konfigurieren Sie die Umgebungsvariable LIBPATH mit den folgenden Werten:

- *INFA_JRE_HOME*/bin
- *JAVA_HOME*/java/jre/bin/classic

Datenbanken

In der nachstehenden Tabelle sind die Werte beschrieben, die Sie für die Umgebungsvariable LIBPATH für die verschiedenen Datenbanken festlegen:

Datenbank	Wert
Oracle	<*DatabasePath*>/lib
IBM DB2	<*DatabasePath*>/lib
Sybase ASE	"${SYBASE_OCS}/lib:${SYBASE_ASE}/lib:${LIBPATH}"
Informix	<*DatabasePath*>/lib

Datenbank	Wert
Teradata	*<DatabasePath>*/lib
ODBC	<CLOSEDODBCHOME>/lib

Konfigurieren der Kerberos-Umgebungsvariablen

Wenn Sie die Informatica-Domäne zur Ausführung in einem Netzwerk mit Kerberos-Authentifizierung konfigurieren, müssen Sie die Umgebungsvariablen für die Kerberos-Konfiguration und den Zugangsdaten-Cache einrichten.

Richten Sie die folgenden Umgebungsvariablen ein:

KRB5_CONFIG

Verwenden Sie die Umgebungsvariable KRB5_CONFIG, um den Pfad und Dateinamen der Kerberos-Konfigurationsdatei zu speichern. Der Name der Kerberos-Konfigurationsdatei lautet *krb5.conf*. Sie müssen die Umgebungsvariable KRB5_CONFIG auf jedem Knoten in der Informatica-Domäne einrichten.

KRB5CCNAME

Richten Sie die Umgebungsvariable KRB5CCNAME mit dem Pfad und Dateinamen des Kerberos-Benutzerzugangsdaten-Cache ein. Kerberos-SSO (Single Sign-On, einmalige Anmeldung) erfordert einen Kerberos-Zugangsdaten-Cache für Benutzerkonten.

Wenn Sie die Benutzerzugangsdaten zwischenspeichern, müssen Sie die Option *Weiterleitbar* verwenden. Wenn Sie beispielsweise mithilfe von *kinit* Benutzerzugangsdaten abrufen und zwischenspeichern, müssen Sie die Option *-f* zum Anfordern weiterleitbarer Tickets verwenden.

Konfigurieren der Windows-Firewall

Beim Starten des Informatica-Windows-Diensts können die Rechner, auf denen Sie die Informatica-Clients installieren, in der Informatica-Domäne nicht auf den Dienstmanager zugreifen. Damit die Clients auf den Dienstmanager zugreifen können, müssen Sie die Firewall so konfigurieren, dass sie den Client-Rechnern Zugriff auf die Domäne ermöglicht.

Fügen Sie die Client-Rechner auf dem Rechner, auf dem Sie die Informatica-Domäne erstellt haben, zur Liste der Firewall-Ausnahmen hinzu.

1. Öffnen Sie in der Windows-Systemsteuerung die **Windows-Firewall**.
2. Klicken Sie im Fenster „Windows Firewall“ auf die Registerkarte **Ausnahmen**.
3. Klicken Sie auf **Programm hinzufügen**.
4. Klicken Sie im Fenster für das Hinzufügen eines Programms auf **Durchsuchen**.

   Die Datei infasvcs.exe führt den Dienstmanager in der Domäne aus.
5. Navigieren Sie zu folgendem Verzeichnis:

   ```
   <Informatica installation directory>\tomcat\bin
   ```
6. Wählen Sie **infasvcs.exe** und klicken Sie auf **Öffnen**.

   Die Datei infasvcs.exe wird in der Liste der Programme angezeigt.

Durch Klicken auf **Bereich ändern** können Sie die Rechner angeben, auf die Informatica zugreifen soll.

7. Überprüfen Sie, ob die Datei infasvcs.exe in der Liste der Programme und Dienste angezeigt wird und aktiviert ist.
8. Klicken Sie auf **OK**.

KAPITEL 10

Vorbereiten zum Erstellen der Anwendungsdienste

Dieses Kapitel umfasst die folgenden Themen:

- Vorbereitung zum Erstellen der Anwendungsdienste - Übersicht, 182
- Überprüfen des Setups für 64-Bit-Windows, 182
- Erstellen von Verzeichnissen für den Analyst-Dienst, 183
- Erstellen der Dienstprinzipalnamen und Keytab-Dateien für Anwendungsdienste, 184
- Erstellen eines Schlüsselspeichers für eine sichere Verbindung zu einem Web-Anwendungsdienst, 184
- Anmelden beim Informatica Administrator, 185
- Erstellen von Verbindungen, 186

Vorbereitung zum Erstellen der Anwendungsdienste - Übersicht

Bevor Sie einen Anwendungsdienst erstellen, überprüfen Sie die Installation und Konfiguration auf dem Knoten.

Melden Sie sich am Administrator-Tool an und erstellen Sie Verbindungen zu den Datenbanken, auf die die Anwendungsdienste über die native Konnektivität zugreifen.

Überprüfen des Setups für 64-Bit-Windows

Unter Windows müssen Sie die Informatica-Dienste und das Developer Tool auf der 64-Bit-Plattform ausführen. Sie können den PowerCenter Client auf einer 32-Bit- oder 64-Bit-Plattform ausführen.

Eine 64-Bit-Architektur bietet mehr Speicherplatz, der die Zwischenspeicherung und die Datendurchsatzleistung der Integrationsdienste verbessern kann. Die Informatica-64-Bit-Plattform adressiert bis zu 18 Millionen Terabyte (2^64 Byte) des Systemspeichers und hat bis zu 256 Terabyte (2^48 Byte) für eine einzelne Anwendung verfügbar.

Wenn Sie Informatica auf 64-Bit-Plattformen ausführen, konfigurieren Sie die Umgebung, um die richtigen Bibliotheken, Datenbank-Clients und Cachegrößen pro Sitzung zu verwenden.

Halten Sie sich an die folgenden Richtlinien, wenn Sie Informatica-Dienste auf 64-Bit-Windows installieren:

- Verknüpfen Sie 64-Bit-Anwendungen mit 64-Bit-Bibliotheken.
- Verknüpfen Sie 64-Bit-Computer, auf denen der Datenintegrationsdienst, der PowerCenter-Repository-Dienst oder der PowerCenter-Integrationsdienst mit einem 64-Bit-Datenbank-Client ausgeführt wird.

Erstellen von Verzeichnissen für den Analyst-Dienst

Vor dem Erstellen des Analyst-Diensts müssen Sie Verzeichnisse für das Analyst Tool zum Speichern temporärer Dateien erstellen.

Erstellen Sie die folgenden Verzeichnisse auf dem Knoten, auf dem der Analyst-Dienst ausgeführt wird:

Verzeichnis des Einfachdatei-Cache

Erstellen Sie ein Verzeichnis für den Einfachdatei-Cache, in dem das Analyst-Tool hochgeladene Einfachdateien speichert. Der Datenintegrationsdienst muss auch in der Lage sein, auf dieses Verzeichnis zuzugreifen. Wenn der Analyst-Dienst und der Datenintegrationsdienst auf verschiedenen Knoten ausgeführt werden, konfigurieren Sie das Einfachdateiverzeichnis zur Verwendung eines freigegebenen Verzeichnisses. Wenn der Datenintegrationsdienst auf primären und Backup-Knoten oder auf einem Gitter läuft, muss jeder Prozess des Datenintegrationsdiensts auf die Dateien im freigegebenen Verzeichnis zugreifen können.

Beispiel: Sie können ein Verzeichnis mit dem Namen „flatfilecache“ auf dem folgenden gemounteten Laufwerk erstellen, auf das alle Prozesse des Analyst-Diensts und des Datenintegrationsdiensts zugreifen können.

```
F:\shared\<InformaticaInstallationDir>\server
```

Wenn Sie eine Referenztabelle oder eine Einfachdatei-Quelle importieren, verwendet das Analyst-Tool die Dateien aus diesem Verzeichnis, um eine Referenztabelle oder ein Einfachdatei-Datenobjekt zu erstellen.

Temporäres Verzeichnis für Exportdateien

Erstellen Sie ein Verzeichnis zum Speichern der temporären Unternehmensglossardateien, die der Unternehmensglossar-Exportprozess erstellt. Erstellen Sie das Verzeichnis auf dem Knoten, auf dem der Analyst-Dienst ausgeführt wird.

Beispiel: Sie können ein Verzeichnis namens "exportfiledirectory" an dem folgenden Speicherort erstellen: `<Informatica-Installationsverzeichnis>/server`

Verzeichnis für Objektanhänge

Erstellen Sie ein Verzeichnis, um die Dateien zu speichern, die von Content-Managern als Anhänge zu Glossarobjekten hinzugefügt werden können. Erstellen Sie das Verzeichnis auf dem Knoten, auf dem der Analyst-Dienst ausgeführt wird.

Beispiel: Sie können ein Verzeichnis namens "attachmentdirectory" an dem folgenden Speicherort erstellen: `<Informatica-Installationsverzeichnis>/server`.

Erstellen der Dienstprinzipalnamen und Keytab-Dateien für Anwendungsdienste

Wenn die Informatica-Domäne Kerberos-Authentifizierung verwendet und Sie die Dienstprinzipalebene für die Domäne auf die Prozessebene festlegen, erfordert die Domäne eine SPN- und eine Keytab-Datei für jeden Anwendungsdienst, den Sie in der Domäne erstellen. Bevor Sie einen Dienst aktivieren, stellen Sie sicher, dass für den Dienst eine SPN- und eine Keytab-Datei verfügbar ist. Kerberos kann den Anwendungsdienst nicht authentifizieren, wenn der Dienst nicht über eine Keytab-Datei im Informatica-Verzeichnis verfügt.

Die Informatica-Domäne benötigt für die SPN- und Keytab-Dateinamen ein bestimmtes Format. Sie können den Kerberos SPN-Formatgenerator von Informatica verwenden, um das Format der SPN- und Keytab-Dateinamen für den Dienst zu generieren. Um Zeit zu sparen, legen Sie die Namen der zu erstellenden Dienste und die Knoten fest, auf denen die Dienste ausgeführt werden sollen. Führen Sie anschließend das Dienstprogramm aus, um das Format des SPN- und Keytab-Dateinamens für alle Dienste gleichzeitig zu generieren. Bei den SPN- und Keytab-Dateinamen muss die Groß-/Kleinschreibung beachtet werden.

Sie können den Kerberos SPN-Formatgenerator von Informatica über das folgende Verzeichnis ausführen: `<Informatica-Installationsverzeichnis>/Tools/Kerberos`

Weitere Informationen zum Ausführen des Kerberos SPN-Formatgenerators von Informatica finden Sie unter "Generieren des Namensformats für Dienstprinzipale und Keytab-Dateien" auf Seite 75.

Senden Sie eine Anfrage an den Kerberos-Administrator, um die SPNs zur Prinzipaldatenbank hinzuzufügen und die entsprechende Keytab-Datei zu erstellen.

Wenn Sie die Keytab-Dateien von dem Kerberos-Administrator erhalten, kopieren Sie die Dateien in das Verzeichnis für die Keytab-Datei. Standardmäßig werden Keytab-Dateien im folgenden Verzeichnis gespeichert: `<Informatica-Installationsverzeichnis>/isp/config/keys`. Wenn Sie während der Installation ein anderes Verzeichnis für die Keytab-Datei angegeben haben, kopieren Sie die Dateien in dieses Verzeichnis.

Hinweis: Wenn sich der Dienstprinzipal für die Domäne auf Knotenebene befindet, können Sie Anwendungsdienste erstellen und aktivieren, ohne zusätzliche SPNs und Keytab-Dateien zu erstellen.

Erstellen eines Schlüsselspeichers für eine sichere Verbindung zu einem Web-Anwendungsdienst

Sie können eine sichere Verbindung zwischen der Informatica-Domäne und einem Web-Anwendungsdienst wie Analyst-Dienst herstellen. Informatica verwendet das SSL/TLS-Protokoll zum Verschlüsseln von Netzwerkverkehr. Um die Verbindung zu sichern, müssen Sie die erforderlichen Dateien erstellen.

Bevor Sie die Verbindung zu einem Web-Anwendungsdienst sichern, überprüfen Sie, ob die folgenden Anforderungen erfüllt sind:

Sie haben eine Zertifikatssignieranfrage und einen privaten Schlüssel erstellt.

Sie können keytool oder OpenSSL zum Erstellen der Zertifikatssignieranfrage und des privaten Schlüssels verwenden.

Bei Verwendung von RSA-Verschlüsselung müssen Sie mehr als 512 Bit verwenden.

Sie haben ein signiertes SSL-Zertifikat.

Das Zertifikat kann selbstsigniert oder von einer Zertifizierungsstelle signiert sein. Informatica empfiehlt ein von einer Zertifizierungsstelle signiertes Zertifikat.

Sie haben das Zertifikat in einen Schlüsselspeicher im JKS-Format importiert.

Ein Schlüsselspeicher muss nur ein Zertifikat enthalten. Wenn Sie ein eindeutiges Zertifikat für jeden Webanwendungsdienst verwenden, erstellen Sie einen separaten Schlüsselspeicher für jedes Zertifikat. Alternativ können Sie ein gemeinsam genutztes Zertifikat und einen gemeinsam genutzten Schlüsselspeicher verwenden.

Wenn Sie das vom Installationsprogramm erzeugte SSL-Zertifikat für das Administrator-Tool verwenden, müssen Sie das Zertifikat nicht in einen Schlüsselspeicher im JKS-Format importieren.

Der Schlüsselspeicher befindet sich in einem Verzeichnis, auf das zugegriffen werden kann.

Der Schlüsselspeicher muss sich in einem Verzeichnis befinden, auf das das Administrator-Tool zugreifen kann.

Anmelden beim 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>/administrator/
     ```

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

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

   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, wenden Sie sich an den Informatica-Domänenadministrator.

   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.

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 Delegierung für alle Benutzerkonten mit in der Informatica-Domäne verwendeten Dienstprinzipalen aktiviert haben. Zum Aktivieren der Delegierung legen Sie im Microsoft Active Directory Service die Option **Benutzer bei Delegierungen aller Dienste vertrauen (nur Kerberos)** für jedes Benutzerkonto fest, für das Sie einen SPN festgelegt haben.

Erstellen von Verbindungen

Erstellen Sie im Administrator Tool Verbindungen zu den Datenbanken, die die Anwendungsdienste verwenden. Sie müssen die Verbindungsdetails beim Konfigurieren des Anwendungsdiensts angeben.

Wenn Sie die Datenbankverbindung erstellen, geben Sie die Eigenschaften der Datenbankverbindung an, und testen Sie die Verbindung.

In der folgenden Tabelle werden die Datenbankverbindungen beschrieben, die Sie vor dem Erstellen der zugehörigen Anwendungsdienste erstellen müssen:

Datenbankverbindung	Beschreibung
Datenobjekt-Cache-Datenbank	Um auf den Datenobjekt-Cache zuzugreifen, erstellen Sie die Datenobjekt-Cache-Verbindung für den Datenintegrationsdienst.
Arbeitsablauf-Datenbank	Um die Metadaten für Arbeitsabläufe zu speichern, erstellen Sie die Verbindung zur Arbeitsablauf-Datenbank für den Datenintegrationsdienst.
Profiling-Warehouse-Datenbank	Zum Erstellen und Ausführen von Profilen und Scorecards erstellen Sie die Profiling-Warehouse-Datenbankverbindung für den Datenintegrationsdienst. Verwenden Sie diese Instanz des Datenintegrationsdiensts, wenn Sie die Laufzeiteigenschaften des Analyst-Diensts konfigurieren. **Hinweis:** Wenn Sie die Microsoft SQL Server-Datenbank als Profiling Warehouse verwenden möchten, wählen Sie ODBC als Provider-Typ aus und deaktivieren Sie die Option **DSN verwenden** im Dialogfeld **Microsoft SQL Server-Verbindungseigenschaften**, wenn Sie die Microsoft SQL Server-Verbindung konfigurieren.
Referenzdaten-Warehouse	Zum Speichern der Daten von Referenztabellen erstellen Sie die Verbindung des Referenzdaten-Warehouses für den Content-Managementdienst.

Eigenschaften von IBM DB2-Verbindungen

Verwenden Sie eine DB2 für LUW-Verbindung, um auf Tabellen in einer DB2 für LUW-Datenbank zuzugreifen.

In der folgenden Tabelle werden die DB2 für LUW-Verbindungseigenschaften erläutert:

Eigenschaft	Beschreibung
Benutzername	Datenbankbenutzername.
Passwort	Passwort für den Benutzernamen.
Verbindungsstring für den Metadatenzugriff	Verbindungs-String für das Importieren von physischen Datenobjekten. Verwenden Sie den folgenden Verbindungs-String: `jdbc:informatica:db2:<host>:50000;databaseName=<dbname>`
Verbindungsstring für den Datenzugriff	Verbindungs-String für die Datenvorschau und das Ausführen von Mappings. Geben Sie den `dbname` aus dem im DB2-Client konfigurierten Alias ein.
Codepage	Datenbank-Codepage
Umgebungs-SQL	Optional. Geben Sie die SQL-Befehle zum Einrichten der Datenbankumgebung ein, wenn Sie eine Verbindung zur Datenbank herstellen. Der Datenintegrationsdienst führt den Verbindungs-Umgebungs-SQL jedes Mal beim Verbinden mit der Datenbank aus.
Transaktions-SQL	Optional. Geben Sie die SQL-Befehle zum Einrichten der Datenbankumgebung ein, wenn Sie eine Verbindung zur Datenbank herstellen. Der Datenintegrationsdienst führt die SQL-Befehle zur Transaktionsumgebung am Anfang jeder Transaktion aus.
Wiederholungszeitraum	Diese Eigenschaft ist für die zukünftige Verwendung reserviert.
Tablespace	Tablespace-Name der DB2 für LUW-Datenbank.
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.
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.

Eigenschaften von Microsoft SQL Server-Verbindungen

Verwenden Sie eine Microsoft SQL Server-Verbindung, um auf Tabellen in einer Microsoft SQL Server-Datenbank zuzugreifen.

In der folgenden Tabelle werden die Eigenschaften von Microsoft SQL Server-Verbindungen erläutert.

Eigenschaft	Beschreibung
Benutzername	Der Benutzername für die Datenbank.
Passwort	Das Passwort für den Benutzernamen.
Vertrauenswürdige Verbindung verwenden	Optional. Bei Aktivierung verwendet der Datenintegrationsdienst die Windows-Authentifizierung, um auf die Microsoft SQL Server-Datenbank zuzugreifen. Der Benutzername, mit dem der Datenintegrationsdienst gestartet wird, muss ein gültiger Windows-Benutzer mit Zugriff auf die Microsoft SQL Server-Datenbank sein.
Verbindungszeichenfolge für den Metadatenzugriff	Die Verbindungszeichenfolge für das Importieren von physischen Datenobjekten. Verwenden Sie die folgende Verbindungszeichenfolge: `jdbc:informatica:sqlserver:// <host>:<port>;databaseName=<dbname>`
Verbindungszeichenfolge für den Datenzugriff	Die Verbindungszeichenfolge für die Datenvorschau und das Ausführen von Mappings. Geben Sie `<ServerName>@<DBName>` ein
Domänenname	Optional. Der Name der Domäne, in der Microsoft SQL Server ausgeführt wird.
Paketgröße	Erforderlich. Optimieren Sie die ODBC-Verbindung zum Microsoft SQL Server. Erhöhen Sie die Paketgröße, um die Leistung zu erhöhen. Standardwert ist 0.
Codepage	Datenbank-Codepage
Eigentümername	Der Name des Eigentümers des Schemas. Geben Sie ihn für die Verbindungen zur Profiling Warehouse-Datenbank oder zur Datenobjekt-Cache-Datenbank an.
Schemaname	Der Name des Schemas in der Datenbank. Geben Sie ihn für die Verbindungen zum Profiling Warehouse oder zur Datenobjekt-Cache-Datenbank an. Sie müssen den Schemanamen für das Profiling Warehouse angeben, wenn der Schemaname anders lautet als der Benutzername der 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	Optional. Geben Sie die SQL-Befehle zum Einrichten der Datenbankumgebung ein, wenn Sie eine Verbindung zur Datenbank herstellen. Der Datenintegrationsdienst führt die SQL-Befehle zur Verbindungsumgebung jedes Mal aus, wenn er eine Verbindung zur Datenbank herstellt.
Transaktions-SQL	Optional. Geben Sie die SQL-Befehle zum Einrichten der Datenbankumgebung ein, wenn Sie eine Verbindung zur Datenbank herstellen. Der Datenintegrationsdienst führt die SQL-Befehle zur Transaktionsumgebung am Anfang jeder Transaktion aus.

Eigenschaft	Beschreibung
Wiederholungsperiode	Diese Eigenschaft ist für die zukünftige Verwendung reserviert.
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 ID-Eigenschaft für gemischte Groß- und Kleinschreibung.
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.

Hinweis: Wenn Sie eine Microsoft SQL Server-Verbindung verwenden, um auf Tabellen in einer Microsoft SQL Server-Datenbank zuzugreifen, zeigt das Developer-Tool nicht die Synonyme für die Tabellen an.

Eigenschaften für Oracle-Verbindungen

Verwenden Sie eine Oracle-Verbindung, um auf Tabellen in einer Oracle-Datenbank zuzugreifen.

In der folgenden Tabelle werden die Eigenschaften von Oracle-Verbindungen erläutert.

Eigenschaft	Beschreibung
Benutzername	Datenbankbenutzername.
Passwort	Passwort für den Benutzernamen.
Verbindungsstring für den Metadatenzugriff	Verbindungs-String für das Importieren von physischen Datenobjekten. Verwenden Sie den folgenden Verbindungs-String: `jdbc:informatica:oracle://<host>:1521;SID=<sid>`
Verbindungsstring für den Datenzugriff	Verbindungs-String für die Datenvorschau und das Ausführen von Mappings. Geben Sie `dbname.world` aus dem TNSNAMES-Eintrag ein.
Codepage	Datenbank-Codepage
Umgebungs-SQL	Optional. Geben Sie die SQL-Befehle zum Einrichten der Datenbankumgebung ein, wenn Sie eine Verbindung zur Datenbank herstellen. Der Datenintegrationsdienst führt den Verbindungs-Umgebungs-SQL jedes Mal beim Verbinden mit der Datenbank aus.
Transaktions-SQL	Optional. Geben Sie die SQL-Befehle zum Einrichten der Datenbankumgebung ein, wenn Sie eine Verbindung zur Datenbank herstellen. Der Datenintegrationsdienst führt die SQL-Befehle zur Transaktionsumgebung am Anfang jeder Transaktion aus.
Wiederholungszeitraum	Diese Eigenschaft ist für die zukünftige Verwendung reserviert.
Parallelmodus	Optional. Ermöglicht Parallelverarbeitung beim Laden von Daten in eine Tabelle im Bulk-Modus. Standardwert ist „Deaktiviert“.

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.
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.

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 **Verwalten**.
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**.

KAPITEL 11

Erstellen der Anwendungsdienste

Dieses Kapitel umfasst die folgenden Themen:

- Erstellen der Anwendungsdienste – Übersicht, 191
- Überprüfen der Voraussetzungen für Anwendungsdienste, 192
- Anwendungsdienst-Abhängigkeiten, 194
- Erstellen und Konfigurieren des Modellrepository-Dienstes, 195
- Erstellen und Konfigurieren des Datenintegrationsdienstes, 200
- Erstellen und Konfigurieren des Analyst-Dienstes, 204
- Erstellen und Konfigurieren des Content-Management-Dienstes, 206
- Erstellen und Konfigurieren des Suchdienstes, 208
- Erstellen und Konfigurieren des PowerCenter-Repository-Dienstes, 210
- Erstellen und Konfigurieren des PowerCenter-Integrationsdienstes, 214
- Erstellen und Konfigurieren des Metadata Manager-Dienstes, 216
- Erstellen und Konfigurieren des Webdienst-Hub-Dienstes, 222

Erstellen der Anwendungsdienste – Übersicht

Verwenden Sie das Administrator-Tool, um die Anwendungsdienste in der erforderlichen Reihenfolge zu erstellen.

Einige Anwendungsdienste sind von anderen Anwendungsdiensten abhängig. Beim Erstellen dieser abhängigen Anwendungsdienste müssen Sie die Namen anderer ausgeführter Anwendungsdienste angeben. Überprüfen Sie die Anwendungsdienst-Abhängigkeiten, um die Reihenfolge zu ermitteln, in der die Dienste erstellt werden müssen. Sie müssen beispielsweise einen Modellrepository-Dienst und einen Datenintegrationsdienst erstellen, bevor Sie einen Analyst-Dienst erstellen.

Stellen Sie vor dem Erstellen der Anwendungsdienste sicher, dass Sie die erforderlichen Aufgaben für die Installation und Konfiguration abgeschlossen haben.

Überprüfen Sie nach dem Erstellen der einzelnen Anwendungsdienste die nächsten Aufgaben, die Sie durchführen müssen.

Überprüfen der Voraussetzungen für Anwendungsdienste

Stellen Sie vor dem Erstellen eines Anwendungsdienstes sicher, dass Sie die folgenden erforderlichen Aufgaben durchgeführt haben, die zuvor in diesem Handbuch beschrieben wurden:

Einrichten der Datenbank

Richten Sie die folgenden Datenbanken ein:

- Modellrepository für den Modellrepository-Dienst
- Die Datenobjekt-Cache-Datenbank zum Zwischenspeichern logischer Datenobjekte und virtueller Tabellen
- Profiling Warehouse für Data Profiling und Discovery
- Arbeitsablauf-Datenbank zum Speichern der Laufzeit-Metadaten für Arbeitsabläufe.
- Referenzdaten-Warehouse zum Speichern von Tabellendaten für den Content-Managementdienst.
- PowerCenter-Repository für den PowerCenter-Repository-Dienst
- Metadata Manager-Repository für den Metadata Manager-Dienst

Installieren der Datenbank-Clientsoftware auf den Servercomputern

Konfigurieren Sie die native Konnektivität wie folgt:

- Installieren und konfigurieren Sie die native Datenbank-Clientsoftware für die relationalen Datenquellen und die Repository-Datenbanken auf dem Computer, auf dem der Datenintegrationsdienst ausgeführt wird.
- Installieren Sie die Datenbank-Clientsoftware und konfigurieren Sie die Konnektivität auf den Computern, auf denen der PowerCenter-Repository-Dienst und die PowerCenter-Repository-Dienstprozesse ausgeführt werden.
- Installieren Sie die Datenbank-Clientsoftware für die relationalen Datenquellen und die Repository-Datenbanken auf den Computern, auf denen der PowerCenter-Integrationsdienst ausgeführt wird.

Konfigurieren von Datenbank-Client-Umgebungsvariablen unter UNIX

Sie müssen Sie Datenbank-Client-Umgebungsvariablen auf den Computern konfigurieren, auf denen die folgenden Dienste ausgeführt werden:

- Datenintegrationsdienst
- PowerCenter-Repository-Dienst
- PowerCenter-Integrationsdienst

Erstellen einer Keytab-Datei für den Dienst

Wenn die Domäne Kerberos-Authentifizierung verwendet und Sie die Dienstprinzipalebene auf Prozessebene einrichten, erstellen Sie eine eindeutige Keytab-Datei für folgende Dienste:

- Modellrepository-Dienst
- Datenintegrationsdienst
- Analyst-Dienst
- Content-Managementdienst
- Suchdienst
- PowerCenter-Repository-Dienst

- PowerCenter-Integrationsdienst
- Metadata Manager-Dienst

Hinweis: Der Name des Dienstes, den Sie erstellen, muss mit dem Dienstnamen im Keytab-Dateinamen identisch sein.

Einrichten von Schlüsselspeicherdateien

Um eine sichere Verbindung zum Anwendungs-Client einzurichten, erstellen Sie eine Schlüsselspeicherdatei für die folgenden Dienste:

- Analyst-Dienst
- Metadata Manager-Dienst
- Webdienst-Hub-Dienst

Konfigurieren von POSIX Asynchronous I/O

Konfigurieren Sie POSIX Asynchronous I/O bei der Installation von Informatica auf IBM AIX auf allen Knoten, auf denen Sie einen PowerCenter-Integrationsdienst ausführen möchten.

Bestimmen der Codepage für das Repository

Stellen Sie die Codepage-Kompatibilität wie folgt sicher:

- Die Domänen-Konfigurationsdatenbank ist mit den Codepages der Anwendungsdienste kompatibel, die Sie in der Domäne erstellen.
- Die PowerCenter-Repository-Codepage ist mit den Codepages für PowerCenter Client und alle Anwendungsdienste in der Informatica-Domäne kompatibel.
- Die Codepage für den PowerCenter-Integrationsdienst ist mit der Codepage des zugehörigen PowerCenter-Repositorys kompatibel.
- Die Metadata Manager-Repository-Codepage, die Codepage auf dem Computer, auf dem der zugehörige PowerCenter-Integrationsdienst läuft, und die Codepage der Datenbank-Management- und PowerCenter-Ressourcen, die Sie in das Metadata Manager-Warehouse laden möchten, müssen gleich sein.

Konfigurieren der lokalen Umgebungsvariablen unter UNIX

Stellen Sie sicher, dass die Gebietsschemaeinstellungen auf Computern mit Zugriff auf das Administrator Tool und die Informatica-Client-Tools mit der Codepage des PowerCenter-Repositorys kompatibel sind.

Konfigurieren der Bibliothekspfad-Umgebungsvariablen unter UNIX

Konfigurieren Sie die Bibliothekspfad-Umgebungsvariablen auf den Computern, auf denen folgende Dienste ausgeführt werden:

- Datenintegrationsdienst
- PowerCenter-Repository-Dienst
- PowerCenter-Integrationsdienst

Überprüfen Sie das Setup für 64-Bit-Windows.

Überprüfen Sie das Setup für 64-Bit-Windows für die folgenden Dienste:

- Datenintegrationsdienst
- PowerCenter-Repository-Dienst
- PowerCenter-Integrationsdienst

Erstellen von Verzeichnissen für den Analyst-Dienst

Erstellen Sie folgende Verzeichnisse auf dem Knoten, auf dem der Analyst-Dienst ausgeführt wird:

- Cache-Verzeichnis für Einfachdateien, in dem das Analyst Tool hochgeladene Einfachdateien speichert. Stellen Sie sicher, dass der Datenintegrationsdienst auch auf dieses Verzeichnis zugreifen kann.
- Temporäres Verzeichnis für Exportdateien, in dem die temporären Unternehmensglossardateien gespeichert werden, die der Unternehmensglossar-Exportprozess erstellt.

Erstellen Sie Verbindungen zu den Datenbanken, auf die die Anwendungsdienste über die native Konnektivität zugreifen.

Erstellen Sie im Administrator Tool Verbindungen zu den folgenden Datenbanken:

- Datenobjekt-Cache-Datenbank
- Profiling-Warehouse-Datenbank
- Referenzdaten-Warehouse
- Arbeitsablauf-Datenbank

Anwendungsdienst-Abhängigkeiten

Ein abhängiger Anwendungsdienst ist ein Anwendungsdienst, der mindestens einen anderen Anwendungsdienst benötigt. Vor dem Erstellen eines abhängigen Dienstes müssen Sie alle Anwendungsdienste erstellen, die der abhängige Dienst benötigt.

Beispiel: Der Datenintegrationsdienst ist vom Modellrepository-Dienst abhängig. Beim Erstellen eines Datenintegrationsdienstes müssen Sie im Administrator-Tool den Namen eines Modellrepository-Dienstes angeben. Daher müssen Sie vor dem Erstellen eines Datenintegrationsdienstes zunächst einen Modellrepository-Dienst erstellen.

Dienste, die auf Modellrepository-Objekte zugreifen, können voneinander abhängig sein. Darüber hinaus können Dienste, die auf PowerCenter-Repository-Objekte zugreifen, voneinander abhängig sein. Durch die Anwendungsdienst-Abhängigkeiten wird die Reihenfolge festgelegt, in der die Dienste erstellt werden müssen.

Dienste, die auf Modellrepository-Objekte zugreifen

Erstellen Sie die Anwendungsdienste, die auf Modellrepository-Objekte zugreifen, in folgender Reihenfolge:

1. Modellrepository-Dienst
   Der Modellrepository-Dienst hat keine Anwendungsdienst-Abhängigkeiten.
2. Datenintegrationsdienst.
   Der Datenintegrationsdienst ist vom Modellrepository-Dienst abhängig.
3. Analyst-Dienst.
   Der Analyst-Dienst ist vom Modellrepository-Dienst und vom Datenintegrationsdienst abhängig.

   Wenn Sie die Datenherkunft für Scorecards im Analyst-Tool ausführen möchten, ist der Analyst-Dienst vom Metadata Manager-Dienst abhängig. Sie können den Analyst-Dienst und den Metadata Manager-Dienst in beliebiger Reihenfolge erstellen. Es besteht die Möglichkeit, den Metadata Manager-Dienst, der die Datenherkunft für den Analyst-Dienst ausführt, beim Erstellen oder nach dem Erstellen des Analyst-Dienstes auszuwählen.
4. Content-Managementdienst.

Der Content-Managementdienst ist vom Modellrepository-Dienst und vom Datenintegrationsdienst abhängig.

5. Suchdienst.
   Der Suchdienst ist vom Modellrepository-Dienst, vom Datenintegrationsdienst und vom Analyst-Dienst abhängig.

Dienste, die auf PowerCenter-Repository-Objekte zugreifen

Erstellen Sie die Anwendungsdienste, die auf PowerCenter-Repository-Objekte zugreifen, in folgender Reihenfolge:

1. PowerCenter-Repository-Dienst
   Der PowerCenter-Repository-Dienst hat keine Anwendungsdienst-Abhängigkeiten.
2. PowerCenter-Integrationsdienst
   Der PowerCenter-Integrationsdienst ist vom PowerCenter-Repository-Dienst abhängig.
3. Metadata Manager-Dienst.
   Der Metadata Manager-Dienst ist vom PowerCenter-Repository-Dienst und vom PowerCenter-Integrationsdienst abhängig.
4. Webdienst-Hub.
   Der Webdienst-Hub-Dienst ist vom PowerCenter-Repository-Dienst abhängig.

Erstellen und Konfigurieren des Modellrepository-Dienstes

Der Modellrepository-Dienst ist ein Anwendungsdienst, der das Modellrepository verwaltet. Im Modellrepository werden die von Informatica-Clients und -Anwendungsdiensten erstellten Metadaten in einer relationalen Datenbank gespeichert, um die Zusammenarbeit zwischen den Clients und Diensten zu ermöglichen.

Wenn Sie auf ein Modellrepository-Objekt im Developer-Tool, Analyst-Tool, Administrator-Tool oder im Datenintegrationsdienst zugreifen, sendet der Client oder Dienst eine Anfrage an den Modellrepository-Dienst. Der Modellrepository-Dienst-Prozess ruft Metadaten aus den Modellrepository-Datenbanktabellen ab, fügt sie dort ein und aktualisiert sie.

Erstellen des Modellrepository-Dienstes

Erstellen Sie den Dienst mithilfe des Diensterstellungs-Assistenten im Administrator Tool.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie auf **Aktionen** > **Neu** > **Modellrepository-Dienst**.

   Das Dialogfeld **Neuer Modellrepository-Dienst** wird angezeigt.

3. Geben Sie auf der Seite **Neuer Modellrepository-Dienst – Schritt 1 von 2** die folgenden Eigenschaften ein:

Eigenschaft	Beschreibung
Name	Name des Diensts. 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 Diensts. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Domäne und Ordner, in der/dem der Dienst erstellt wurde. Um einen anderen Ordner auszuwählen, klicken Sie auf **Durchsuchen**. Sie können den Dienst nach dessen Erstellung verschieben.
Lizenz	Lizenzobjekt für die Verwendung des Diensts.
Knoten	Knoten, auf dem der Dienst ausgeführt wird.
Backup-Knoten	Wenn die Lizenz hohe Verfügbarkeit einschließt, sind dies die Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist.

4. Klicken Sie auf **Weiter**.

   Die Seite **Neuer Modellrepository-Dienst – Schritt 2 von 2** wird angezeigt.

5. Geben Sie die folgenden Eigenschaften für die Modellrepository-Datenbank ein:

Eigenschaft	Beschreibung
Datenbanktyp	Der Typ der Repository-Datenbank.
Benutzername	Der Datenbankbenutzername für das Repository.
Passwort	Passwort der Repository-Datenbank für den Datenbankbenutzer.
Datenbankschema	Für Microsoft SQL Server verfügbar. Name des Schemas, das die Modellrepository-Tabellen enthält.
Datenbank-Tablespace	Für IBM DB2 verfügbar. Der Name des Tablespace, in dem die Tabellen erstellt werden sollen. Bei einer IBM DB2-Datenbank mit mehreren Partitionen muss der Tablespace einen einzelnen Knoten und eine einzelne Partition umfassen.

6. Geben Sie die JDBC-Verbindungszeichenfolge ein, mit der der Dienst eine Verbindung zur Modellrepository-Datenbank herstellt.

Verwenden Sie die folgende Syntax für die Verbindungszeichenfolge für den ausgewählten Datenbanktyp:

Datenbanktyp	Syntax der Verbindungszeichenfolge
IBM DB2	`jdbc:informatica:db2:// <host_name>:<port_number>;DatabaseName=<database_name>;BatchPerformanceWorkaround=true;DynamicSections=3000`

Microsoft SQL Server	- Microsoft SQL Server, der die Standardinstanz verwendet
	`jdbc:informatica:sqlserver:// <host_name>:<port_number>;DatabaseName=<database_name>;SnapshotSerializable=true`
	- Microsoft SQL Server, der eine benannte Instanz verwendet
	`jdbc:informatica:sqlserver://<host_name> \<named_instance_name>;DatabaseName=<database_name>;SnapshotSerializable=true`

Oracle	`jdbc:informatica:oracle:// <host_name>:<port_number>;SID=<database_name>;MaxPooledStatements=20;CatalogOptions=0;BatchPerformanceWorkaround=true`

7. Wenn die Modellrepository-Datenbank mit dem SSL-Protokoll gesichert ist, müssen Sie die sicheren Datenbankparameter im Feld **Sichere JDBC-Parameter** eingeben.

   Geben Sie die Parameter als `name=value`-Paare, getrennt durch ein Semikolon (;) ein. Beispiel:

   ```
   param1=value1;param2=value2
   ```

   Geben Sie die folgenden sicheren Datenbankparameter ein:

Sicherer Datenbankparameter	Beschreibung
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 der Datenbankserver sendet. Wenn dieser Parameter auf TRUE gesetzt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat. Wenn Sie den HostNameInCertificate-Parameter angeben, validiert Informatica ebenfalls den Hostnamen im Zertifikat. Wenn dieser Parameter auf FALSE gesetzt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat nicht. Informatica ignoriert alle Truststore-Informationen, die Sie angeben.
HostNameInCertificate	Optional. Hostname des Computers, auf dem die sichere Datenbank gehostet wird. Wenn Sie einen Hostnamen angeben, validiert Informatica den Hostnamen in der Verbindungszeichenfolge mit dem Hostnamen im SSL-Zertifikat.
cryptoProtocolVersion	Erforderlich. Gibt das Kryptografieprotokoll an, das für die Verbindung mit einer sicheren Datenbank verwendet werden soll. Sie können je nach dem vom Datenbankserver verwendeten Kryptografieprotokoll den Parameter auf `cryptoProtocolVersion=TLSv1.1` oder `cryptoProtocolVersion=TLSv1.2` einstellen.

Sicherer Datenbankparameter	Beschreibung
TrustStore	Erforderlich. Pfad und Dateiname der Truststore-Datei, die das SSL-Zertifikat für die Datenbank enthält. Wenn Sie den Pfad für die Truststore-Datei nicht hinzufügen, sucht Informatica im folgenden Standardverzeichnis nach der Datei: `<Informatica-Installationsverzeichnis>/tomcat/bin`
TrustStorePassword	Erforderlich. Passwort der Truststore-Datei für die sichere Datenbank.

Hinweis: Informatica hängt die sicheren JDBC-Parameter an den JDBC-Verbindungsstring an. Wenn Sie die sicheren JDBC-Parameter direkt zur Verbindungszeichenfolge hinzufügen, geben Sie im Feld **Sichere JDBC-Parameter** keinen Parameter ein.

8. Klicken Sie auf **Testverbindung**, um zu überprüfen, ob Sie eine Verbindung zur Datenbank herstellen können.
9. Wählen Sie **Die angegebene Verbindungszeichenfolge weist keinen Inhalt auf. Erstellen Sie neue Inhalte.** aus.
10. Klicken Sie auf **Fertig stellen**.

    Die Domäne erstellt den Modellrepository-Dienst, erstellt Inhalt für das Modellrepository in der angegebenen Datenbank und aktiviert den Dienst.

    Hinweis: Wenn Sie die Eigenschaften des Modellrepository-Diensts aktualisieren, müssen Sie den Modellrepository- und den Katalogdienst neu starten, damit die Änderungen wirksam werden.

Nachdem Sie den Dienst mithilfe des Assistenten erstellt haben, können Sie die Eigenschaften bearbeiten oder andere Eigenschaften konfigurieren.

Nach dem Erstellen des Modellrepository-Dienstes

Führen Sie nach dem Erstellen des Modellrepository-Dienstes die folgenden Aufgaben durch:

- Erstellen des Modellrepository-Benutzers, wenn die Domäne keine Kerberos-Authentifizierung verwendet
- Erstellen anderer Anwendungsdienste

Erstellen des Modellrepository-Benutzers

Wenn die Domäne keine Kerberos-Authentifizierung verwendet, erfolgt die Authentifizierung anderer Anwendungsdienste, die Anfragen an den Modellrepository-Dienst stellen, in der Domäne mit einem Benutzerkonto. Sie müssen ein Benutzerkonto erstellen und dem Benutzer die Administratorrolle für den Modellrepository-Dienst zuweisen.

Wenn Sie einen Anwendungsdienst erstellen, der vom Modellrepository-Dienst abhängig ist, geben Sie den Namen des Modellrepository-Dienstes und dieses Modellrepository-Benutzers an.

1. Klicken Sie im Administrator-Tool auf die Registerkarte **Sicherheit**.
2. Klicken Sie im Menü „Sicherheitsaktionen“ auf **Benutzer erstellen** , um ein natives Benutzerkonto zu erstellen.

   Hinweis: Wenn Sie die LDAP-Authentifizierung in der Domäne einrichten, können Sie ein LDAP-Benutzerkonto für den Modellrepository-Benutzer verwenden.

3. Geben Sie folgende Eigenschaften für den Benutzer ein:

Eigenschaft	Beschreibung
Anmeldename	Der Anmeldename für das Benutzerkonto. Der Anmeldename für ein Benutzerkonto muss innerhalb der Sicherheitsdomäne, zu der er gehört, eindeutig sein. Beim Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden. Er darf nicht länger als 128 Zeichen sein. Er darf weder einen Tabulator noch ein Zeilenende-Zeichen noch folgende Sonderzeichen enthalten: ,, + " \ < > ; / * % ? & Der Name kann ein ASCII-Leerzeichen enthalten, jedoch nicht als erstes oder letztes Zeichen. Alle anderen Leerzeichen sind nicht zulässig.
Passwort	Das Passwort für das Benutzerkonto. Das Passwort kann zwischen 1 und 80 Zeichen lang sein.
Passwort bestätigen	Geben Sie das Passwort zur Bestätigung erneut ein. Sie müssen das Passwort noch einmal eingeben. Das Passwort darf nicht mit Kopieren und Einfügen eingegeben werden.
Vollständiger Name	Der vollständige Name für das Benutzerkonto. Der vollständige Name darf folgende Sonderzeichen nicht enthalten: < > “
Beschreibung	Die Beschreibung des Benutzerkontos. Die Beschreibung darf nicht länger als 765 Zeichen sein und keines der folgenden Sonderzeichen enthalten: < > “

4. Klicken Sie auf **OK**.

   Die Benutzereigenschaften werden angezeigt.
5. Klicken Sie auf die Registerkarte **Berechtigungen**.
6. Klicken Sie auf **Bearbeiten**.

   Das Dialogfeld **Rollen und Rechte bearbeiten** wird eingeblendet.
7. Erweitern Sie auf der Registerkarte der **Rollen** den Modellrepository-Dienst.
8. Wählen Sie unter **Systemdefinierte Rollen** „Administrator“ aus und klicken Sie auf **OK**.

Erstellen weiterer Dienste

Nach dem Erstellen des Modellrepository-Dienstes erstellen Sie die Anwendungsdienste, die vom Modellrepository-Dienst abhängig sind.

Erstellen Sie die abhängigen Dienste in der folgenden Reihenfolge:

1. Datenintegrationsdienst
2. Analyst-Dienst
3. Content-Managementdienst
4. Suchdienst

Erstellen und Konfigurieren des Datenintegrationsdienstes

Der Datenintegrationsdienst ist ein Anwendungsdienst, der Datenintegrationsaufgaben für das Analyst-Tool, das Developer-Tool und externe Clients übernimmt.

Bei der Vorschau oder Ausführung von Datenprofilen, SQL-Datendiensten und Mappings im Analyst-Tool oder Developer-Tool sendet der Client Anfragen zur Ausführung der Datenintegrationsaufgaben an den Datenintegrationsdienst. Wenn Sie SQL-Datendienste, Mappings und Arbeitsabläufe über das Befehlszeilenprogramm oder einen externen Client ausführen, sendet der Befehl die Anfrage an den Datenintegrationsdienst.

Erstellen des Datenintegrationsdienstes

Erstellen Sie den Dienst mithilfe des Diensterstellungs-Assistenten im Administrator Tool.

Stellen Sie vor dem Erstellen des Datenintegrationsdienstes sicher, dass Sie den Modellrepository-Dienst erstellt und aktiviert haben. Wenn die Domäne keine Kerberos-Authentifizierung verwendet, stellen Sie sicher, dass Sie einen Modellrepository-Benutzer erstellt haben, über den der Datenintegrationsdienst auf den Modellrepository-Dienst zugreifen kann.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie auf die Ansicht **Dienste und Knoten**.
3. Wählen Sie die Domäne im Domänennavigator aus.
4. Klicken Sie auf **Aktionen** > **Neu** > **Datenintegrationsdienst**.

   Der Assistent **Neuer Datenintegrationsdienst** wird angezeigt.
5. Geben Sie auf der Seite **Neuer Datenintegrationsdienst - Schritt 1 von 14** die folgenden Eigenschaften ein:

Eigenschaft	Beschreibung
Name	Name des Diensts. 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 Diensts. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Domäne und Ordner, in der/dem der Dienst erstellt wurde. Um einen anderen Ordner auszuwählen, klicken Sie auf **Durchsuchen**. Sie können den Dienst nach dessen Erstellung verschieben.
Lizenz	Lizenzobjekt für die Verwendung des Diensts.
Zuweisen	Wählen Sie **Knoten** aus, um den Dienst zur Ausführung auf einem Knoten zu konfigurieren. Wenn die Lizenz Gitter einschließt, können Sie ein Gitter erstellen und den auf dem Gitter auszuführenden Dienst zuweisen, nachdem Sie den Dienst erstellt haben.

Eigenschaft	Beschreibung
Knoten	Knoten, auf dem der Dienst ausgeführt wird.
Backup-Knoten	Wenn die Lizenz hohe Verfügbarkeit einschließt, sind dies die Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist.
Modellrepository-Dienst	Modellrepository-Dienst zum Zuweisen zum Dienst.
Benutzername	Benutzername, den der Dienst für den Zugriff auf den Modellrepository-Dienst verwendet. Geben Sie den Modellrepository-Benutzer ein, den Sie erstellt haben.
Passwort	Passwort für den Modellrepository-Benutzer.
Sicherheitsdomäne	LDAP-Sicherheitsdomäne für den Benutzer des Modellrepository. Das Feld wird angezeigt, wenn die Informatica-Domäne eine LDAP-Sicherheitsdomäne enthält. Nicht verfügbar für eine Domäne mit Kerberos-Authentifizierung.

6. Klicken Sie auf **Weiter**.

   Die Seite **Neuer Datenintegrationsdienst - Schritt 2 von 14** wird angezeigt.
7. Geben Sie die HTTP-Portnummer für den Datenintegrationsdienst ein.
8. Akzeptieren Sie für die restlichen Sicherheitseigenschaften die Standardwerte. Sie können die Sicherheitseigenschaften nach dem Erstellen des Datenintegrationsdiensts konfigurieren.
9. Wählen Sie **Dienst aktivieren** aus.

   Zum Aktivieren des Datenintegrationsdiensts muss der Modellrepository-Dienst ausgeführt werden.
10. Stellen Sie sicher, dass **Zur Plugin-Konfigurationsseite wechseln** nicht ausgewählt ist.
11. Klicken Sie auf **Weiter**.

    Die Seite **Neuer Datenintegrationsdienst - Schritt 3 von 14** wird angezeigt.
12. Stellen Sie die Eigenschaft **Joboptionen starten** auf einen der folgenden Werte ein:
    - Im Dienstprozess. Konfigurieren Sie diesen Wert, wenn Sie SQL-Datendienst- und Webdienstjobs ausführen. Die SQL-Datendienst- und Webdienstjobs erreichen in der Regel eine bessere Leistung, wenn der Datenintegrationsdienst Jobs im Dienstprozess ausführt.
    - In separaten lokalen Prozessen. Konfigurieren Sie diesen Wert, wenn Sie Mapping-, Profil- und Arbeitsablaufjobs ausführen. Wenn der Datenintegrationsdienst Jobs in separaten lokalen Prozessen ausführt, erhöht sich die Stabilität, weil eine unerwartete Unterbrechung eines Jobs keine Auswirkungen auf alle anderen Jobs hat.

    Wenn Sie den Datenintegrationsdienst nach der Erstellung des Diensts zur Ausführung auf einem Gitter konfigurieren, können Sie den Dienst zur Ausführung von Jobs in separaten Remoteprozessen konfigurieren.
13. Akzeptieren Sie die Standardwerte für die verbleibenden Ausführungsoptionen und klicken Sie auf **Weiter**.

    Die Seite **Neuer Datenintegrationsdienst - Schritt 4 von 14** wird angezeigt.
14. Wenn Sie die Datenobjekt-Cache-Datenbank für den Datenintegrationsdienst erstellt haben, klicken Sie auf **Auswählen** und wählen Sie die Cache-Verbindung aus. Wählen Sie die Datenobjekt-Cache-Verbindung aus, die Sie für den Dienst erstellt haben, um auf die Datenbank zuzugreifen.
15. Akzeptieren Sie für die restlichen Eigenschaften auf dieser Seite die Standardwerte und klicken Sie auf **Weiter**.

Die Seite **Neuer Datenintegrationsdienst - Schritt 5 von 14** wird angezeigt.

16. Für eine optimale Leistung aktivieren Sie die Datenintegrationsdienst-Module, die Sie verwenden möchten.

    In der folgenden Tabelle werden die Datenintegrationsdienst-Module aufgelistet, die Sie aktivieren können:

Modul	Beschreibung
Webdienstmodul	Führt Vorgangs-Mappings für Webdienste durch.
Zuordnungsdienstmodul	Führt Mappings und Vorschauen aus.
Profilerstellungsdienst-Modul	Führt Profile und Scorecards aus.
SQL-Dienstmodul	Führt SQL-Abfragen von Client-Tools anderer Hersteller an einen SQL-Datendienst aus.
Arbeitsablauf-Orchestration-Dienstmodul	Führt Arbeitsabläufe aus.

17. Klicken Sie auf **Weiter**.

    Die Seite **Neuer Datenintegrationsdienst - Schritt 6 von 14** wird angezeigt.

    Sie können Sie die HTTP-Proxyservereigenschaften so konfigurieren, dass die HTTP-Anfragen an den Datenintegrationsdienst umgeleitet werden. Sie können Sie die HTTP-Konfigurationseigenschaften so konfigurieren, dass Webdienst-Client-Computer, die Anfragen an den Datenintegrationsdienst senden können, gefiltert werden. Diese Eigenschaften können Sie nach dem Erstellen des Diensts konfigurieren.

18. Akzeptieren Sie die Standardwerte für die HTTP-Proxyserver- und HTTP-Konfigurationseigenschaften und klicken Sie auf **Weiter**.

    Die Seite **Neuer Datenintegrationsdienst - Schritt 7 von 14** wird angezeigt.

    Der Datenintegrationsdienst nutzt die Ergebnissatz-Cache-Eigenschaften, um zwischengespeicherte Ergebnisse für SQL-Datendienstabfragen und -Webdienstanfragen zu verwenden. Sie können die Eigenschaften nach dem Erstellen des Diensts konfigurieren.

19. Akzeptieren Sie die Standardwerte für die Eigenschaften des Ergebnissatz-Cache und klicken Sie auf **Weiter**.

    Die Seite **Neuer Datenintegrationsdienst - Schritt 8 von 14** wird angezeigt.

20. Wenn Sie die Profiling-Warehouse-Datenbank für den Datenintegrationsdienst erstellt haben, wählen Sie das Profilerstellungsdienst-Modul aus.

21. Wenn Sie die Arbeitsablauf-Datenbank für den Datenintegrationsdienst erstellt haben, wählen Sie das Arbeitsablauf-Orchestration-Dienstmodul aus.

22. Stellen Sie sicher, dass die restlichen Module nicht ausgewählt sind.

    Sie können die Eigenschaften für die restlichen Module nach dem Erstellen des Diensts konfigurieren.

23. Klicken Sie auf **Weiter**.

    Die Seite **Neuer Datenintegrationsdienst - Schritt 11 von 14** wird angezeigt.

24. Wenn Sie die Profiling-Warehouse-Datenbank für den Datenintegrationsdienst erstellt haben, klicken Sie auf **Auswählen**, um die Datenbankverbindung auszuwählen. Wählen Sie die Profiling-Warehouse-Verbindung aus, die Sie für den Dienst erstellt haben, um auf die Datenbank zuzugreifen.

25. Wählen Sie aus, ob die Profiling-Warehouse-Datenbank Inhalt aufweist oder nicht.

Wenn Sie eine neue Profiling-Warehouse-Datenbank erstellt haben, wählen Sie **Die angegebene Verbindungszeichenfolge weist keinen Inhalt auf** aus.

26. Klicken Sie auf **Weiter**.

    Die Seite **Neuer Datenintegrationsdienst - Schritt 12 von 14** wird angezeigt.

27. Akzeptieren Sie die Standardwerte für die erweiterten Profiling-Eigenschaften und klicken Sie auf **Weiter**.

    Die Seite **Neuer Datenintegrationsdienst - Schritt 14 von 14** wird angezeigt.

28. Wenn Sie die Arbeitsablauf-Datenbank für den Datenintegrationsdienst erstellt haben, klicken Sie auf **Auswählen**, um die Datenbankverbindung auszuwählen. Wählen Sie die Arbeitsablauf-Datenbankverbindung aus, die Sie für den Dienst erstellt haben, um auf die Datenbank zuzugreifen.

29. Klicken Sie auf **Fertig stellen**.

    Die Domäne erstellt und aktiviert den Datenintegrationsdienst.

Nachdem Sie den Dienst mithilfe des Assistenten erstellt haben, können Sie die Eigenschaften bearbeiten oder andere Eigenschaften konfigurieren.

Nach dem Erstellen des Datenintegrationsdienstes

Führen Sie nach dem Erstellen des Datenintegrationsdienstes die folgenden Aufgaben durch:

- Überprüfen der Hostdateikonfiguration unter UNIX
- Erstellen anderer Anwendungsdienste

Überprüfen der Hostdateikonfiguration unter UNIX

Wenn Sie den Datenintegrationsdienst unter UNIX zum Starten von Jobs als separate Prozesse konfiguriert haben, müssen Sie sicherstellen, dass die Hostdatei auf dem Knoten, auf dem der Dienst ausgeführt wird, einen localhost-Eintrag enthält. Andernfalls schlagen Jobs fehl, wenn die Eigenschaft **Jobs als separate Prozesse starten** für den Datenintegrationsdienst aktiviert ist.

Hinweis: Windows erfordert keinen localhost-Eintrag in der Hostdatei.

Erstellen weiterer Dienste

Nach dem Erstellen des Datenintegrationsdienstes erstellen Sie die Anwendungsdienste, die vom Datenintegrationsdienst abhängig sind.

Erstellen Sie die abhängigen Dienste in der folgenden Reihenfolge:

1. Analyst-Dienst
2. Content-Managementdienst
3. Suchdienst

Erstellen und Konfigurieren des Analyst-Dienstes

Der Analyst-Dienst ist ein Anwendungsdienst, der das Analyst-Tool in der Informatica-Domäne ausführt. Der Analyst-Dienst verwaltet die Verbindungen zwischen Dienstkomponenten und den Benutzern, die Zugriff auf das Analyst-Tool haben.

Beim Ausführen der Profile, Scorecards oder Mapping-Spezifikationen im Analyst-Tool stellt der Analyst-Dienst eine Verbindung zum Datenintegrationsdienst zur Durchführung der Datenintegrationsaufgaben her. Wenn Sie Human-Tasks im Analyst Tool durchführen, stellt der Analyst-Dienst eine Verbindung zum Datenintegrationsdienst her, um die Metadaten der Aufgabe aus der Arbeitsablauf-Datenbank abzurufen.

Wenn Sie ein Modellrepository-Objekt im Analyst-Tool anzeigen, erstellen oder löschen, stellt der Analyst-Dienst eine Verbindung zum Modellrepository-Dienst für den Zugriff auf die Metadaten her. Wenn Sie Datenherkunftsanalysen für Scorecards im Analyst-Tool anzeigen, sendet der Analyst-Dienst die Anfrage an den Metadata Manager-Dienst zum Ausführen der Datenherkunft.

Erstellen des Analyst-Dienstes

Erstellen Sie den Dienst mithilfe des Diensterstellungs-Assistenten im Administrator Tool.

Stellen Sie vor dem Erstellen des Analyst-Diensts sicher, dass Sie die folgenden Dienste erstellt und aktiviert haben:

- Modellrepository-Dienst

  Wenn die Domäne keine Kerberos-Authentifizierung verwendet, stellen Sie sicher, dass Sie einen Modellrepository-Benutzer erstellt haben, über den der Analyst-Dienst auf den Modellrepository-Dienst zugreifen kann.
- Datenintegrationsdienst

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie auf **Aktionen** > **Neu** > **Analyst-Dienst**.

   Das Dialogfeld **Neuer Analyst-Dienst** wird geöffnet.
3. Geben Sie auf der Seite **Neuer Analyst-Dienst – Schritt 1 von 6** die folgenden Eigenschaften ein:

Eigenschaft	Beschreibung
Name	Name des Diensts. 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 Diensts. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Domäne und Ordner, in der/dem der Dienst erstellt wurde. Um einen anderen Ordner auszuwählen, klicken Sie auf **Durchsuchen**. Sie können den Dienst nach dessen Erstellung verschieben.
Lizenz	Lizenzobjekt für die Verwendung des Diensts.
Knoten	Knoten, auf dem der Dienst ausgeführt wird.

4. Klicken Sie auf **Weiter**.

   Die Seite **Neuer Analyst-Dienst – Schritt 2 von 6** wird angezeigt.

5. Geben Sie die HTTP-Portnummer für die Kommunikation des Analyst Tools mit dem Analyst-Dienst ein.
6. Zum Aktivieren der sicheren Kommunikation zwischen dem Analyst Tool und dem Analyst-Dienst wählen Sie **Sichere Kommunikation aktivieren** aus.

   Geben Sie folgende Eigenschaften ein, um die sichere Kommunikation für den Analyst-Dienst zu konfigurieren:

Eigenschaft	Beschreibung
HTTPS-Port	Portnummer, auf der das Analyst Tool bei Aktivierung der sicheren Kommunikation ausgeführt wird. Verwenden Sie eine Portnummer, die sich von der HTTP-Portnummer unterscheidet.
Schlüsselspeicherdatei	Verzeichnis, in dem die Schlüsselspeicherdatei gespeichert wird, die die digitalen Zertifikate enthält.
Schlüsselspeicherpasswort	Klartext-Passwort für die Schlüsselspeicherdatei. Wenn diese Eigenschaft nicht festgelegt ist, verwendet der Analyst-Dienst das Standardpasswort `changeit`.
SSL-Protokoll	Optional. Gibt das zu verwendende Protokoll an. Legen Sie diese Eigenschaft auf `SSL` fest.

7. Wählen Sie **Dienst aktivieren** aus.

   Der Modellrepository-Dienst und der Datenintegrationsdienst müssen ausgeführt werden, um den Analyst-Dienst zu aktivieren.
8. Klicken Sie auf **Weiter**.

   Die Seite **Neuer Analyst-Dienst – Schritt 3 von 6** wird angezeigt.
9. Geben Sie die folgenden Eigenschaften ein, um den Modellrepository-Dienst mit dem Analyst-Dienst zu verbinden:

Beschreibung	Eigenschaft
Modellrepository-Dienst	Modellrepository-Dienst zum Zuweisen zum Dienst.
Benutzername	Benutzername, den der Dienst für den Zugriff auf den Modellrepository-Dienst verwendet. Geben Sie den Modellrepository-Benutzer ein, den Sie erstellt haben.
Passwort	Passwort für den Modellrepository-Benutzer.
Sicherheitsdomäne	LDAP-Sicherheitsdomäne für den Benutzer des Modellrepository. Das Feld wird angezeigt, wenn die Informatica-Domäne eine LDAP-Sicherheitsdomäne enthält. Nicht verfügbar für eine Domäne mit Kerberos-Authentifizierung.

10. Damit Benutzer des Analyst Tool mit Human-Task-Daten arbeiten können, legen Sie die **Datenintegrationsdienst**-Eigenschaft mit dem Datenintegrationsdienst fest, den Sie für das Ausführen von Arbeitsabläufen konfigurieren.

    Wenn die Benutzer des Analyst Tools keine Human Task-Datensätze bearbeiten müssen, konfigurieren Sie diese Eigenschaft nicht.
11. Klicken Sie auf **Weiter**.

    Die Seite **Neuer Analyst-Dienst – Schritt 4 von 6** wird angezeigt.

12. Geben Sie die folgenden Laufzeiteigenschaften für den Analyst-Dienst ein:

Eigenschaft	Beschreibung
Datenintegrationsdienst	Datenintegrationsdienst für die Zuordnung zum Dienst. Der Analyst-Dienst verwaltet die Verbindung zu einem Datenintegrationsdienst, mit dem Benutzer Datenvorschau-, Mappingspezifikations-, Scorecard- und Profil-Jobs im Analyst Tool durchführen können. Sie können den Analyst-Dienst mit dem Datenintegrationsdienst verbinden, den Sie für die Ausführung von Arbeitsabläufen konfiguriert haben. Oder Sie können den Analyst-Dienst für verschiedene Vorgänge verschiedenen Datenintegrationsdiensten zuordnen.
Verzeichnis des Einfachdatei-Cache	Verzeichnis des Einfachdatei-Cache, in dem das Analyst Tool hochgeladene Einfachdateien speichert. Der Datenintegrationsdienst muss auch in der Lage sein, auf dieses Verzeichnis zuzugreifen. Wenn der Analyst-Dienst und der Datenintegrationsdienst auf verschiedenen Knoten ausgeführt werden, konfigurieren Sie das Einfachdateiverzeichnis zur Verwendung eines freigegebenen Verzeichnisses.
Metadata Manager-Dienst	Wenn Sie einen Metadata Manager-Dienst erstellt haben, der die Datenherkunft für Scorecards im Analyst Tool ausführt, wählen Sie den Metadata Manager-Dienst aus. Oder Sie können den Metadata Manager-Dienst auswählen, der die Datenherkunft für das Analyst Tool ausführt, nachdem Sie den Analyst-Dienst erstellt haben. Wenn die Datenherkunft für Scorecards nicht ausgeführt werden soll, konfigurieren Sie diese Eigenschaft nicht.

13. Klicken Sie auf **Weiter**.

    Die Seite **Neuer Analyst-Dienst – Schritt 6 von 5** wird angezeigt.

14. Geben Sie das Verzeichnis zum Speichern der temporären Unternehmensglossardateien ein, die der Unternehmensglossar-Exportprozess erstellt. Geben Sie außerdem das Verzeichnis ein, in dem Dateien gespeichert werden sollen, die von Content-Managern den Glossarobjekten angehängt werden. Diese Verzeichnisse müssen sich auf dem Knoten befinden, auf dem der Analyst-Dienst ausgeführt wird.

15. Klicken Sie auf **Fertig stellen**.

    Die Domäne erstellt und aktiviert den Analyst-Dienst.

Nachdem Sie den Dienst mithilfe des Assistenten erstellt haben, können Sie die Eigenschaften bearbeiten oder andere Eigenschaften konfigurieren.

Nach dem Erstellen des Analyst-Dienstes

Nachdem Sie den Analyst-Dienst erstellt haben, erstellen Sie den Suchdienst, der vom Analyst-Dienst abhängig ist.

Erstellen und Konfigurieren des Content-Management-Dienstes

Der Content-Managementdienst ist ein Anwendungsdienst zum Verwalten der Referenzdaten. Ein Referenzdatenobjekt enthält einen Satz von Datenwerten, die Sie bei der Ausführung von Vorgängen zur

Datenqualität für Quelldaten suchen können. Der Content-Managementdienst kompiliert außerdem Regelspezifikationen in Mapplets. Ein Regelspezifikationsobjekt beschreibt die Datenanforderungen an eine Geschäftsregel in logischen Bedingungen.

Der Content-Managementdienst verwendet den Datenintegrationsdienst zum Ausführen von Mappings, die Daten zwischen Referenztabellen und externen Datenquellen übertragen. Der Content-Managementdienst enthält auch Umwandlungen, Mapping-Spezifikationen und Regelspezifikationen mit den folgenden Typen von Referenzdaten:

- Adressreferenzdaten
- Identitätspopulationen
- Probabilistische Modelle und Klassifizierungsmodelle
- Referenztabellen

Erstellen des Content-Management-Dienstes

Erstellen Sie den Dienst mithilfe des Diensterstellungs-Assistenten im Administrator Tool.

Stellen Sie vor dem Erstellen des Content-Management-Dienstes sicher, dass Sie die folgenden Dienste erstellt und aktiviert haben:

- Modellrepository-Dienst

  Wenn die Domäne keine Kerberos-Authentifizierung verwendet, stellen Sie sicher, dass Sie einen Modellrepository-Benutzer erstellt haben, über den der Content-Managementdienst auf den Modellrepository-Dienst zugreifen kann.
- Datenintegrationsdienst

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie auf **Aktionen** > **Neu** > **Content-Managementdienst**.

   Das Dialogfeld **Neuer Content-Managementdienst** wird angezeigt.
3. Geben Sie auf der Seite **Neuer Content-Managementdienst – Schritt 1 von 2** die folgenden Eigenschaften ein:

Eigenschaft	Beschreibung
Name	Name des Diensts. 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 Diensts. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Domäne und Ordner, in der/dem der Dienst erstellt wurde. Um einen anderen Ordner auszuwählen, klicken Sie auf **Durchsuchen**. Sie können den Dienst nach dessen Erstellung verschieben.
Lizenz	Lizenzobjekt für die Verwendung des Diensts.
Knoten	Knoten, auf dem der Dienst ausgeführt wird.

Eigenschaft	Beschreibung
HTTP-Port	HTTP-Portnummer für den Content-Managementdienst
Datenintegrationsdienst	Datenintegrationsdienst für die Zuordnung zum Dienst. Der Datenintegrationsdienst und der Content-Managementdienst müssen auf demselben Knoten ausgeführt werden.
Modellrepository-Dienst	Modellrepository-Dienst zum Zuweisen zum Dienst.
Benutzername	Benutzername, den der Dienst für den Zugriff auf den Modellrepository-Dienst verwendet. Geben Sie den Modellrepository-Benutzer ein, den Sie erstellt haben.
Passwort	Passwort für den Modellrepository-Benutzer.
Sicherheitsdomäne	LDAP-Sicherheitsdomäne für den Benutzer des Modellrepository. Das Feld wird angezeigt, wenn die Informatica-Domäne eine LDAP-Sicherheitsdomäne enthält. Nicht verfügbar für eine Domäne mit Kerberos-Authentifizierung.
Referenzdaten-Speicherort	Die Verbindung des Referenzdaten-Warehouse, die Sie für den Content-Managementdienst für den Zugriff auf das Referenzdaten-Warehouse erstellt haben. Klicken Sie auf **Auswählen**, um die Verbindung auszuwählen.

4. Klicken Sie auf **Weiter**.

   Die Seite **Neuer Content-Managementdienst – Schritt 2 von 2** wird angezeigt.
5. Übernehmen Sie die Standardwerte für die Sicherheitseigenschaften.
6. Wählen Sie **Dienst aktivieren** aus.

   Der Modellrepository-Dienst und der Datenintegrationsdienst müssen ausgeführt werden, um den Content-Managementdienst zu aktivieren.
7. Klicken Sie auf **Fertig stellen**.

   Die Domäne erstellt und aktiviert den Content-Managementdienst.

Nachdem Sie den Dienst mithilfe des Assistenten erstellt haben, können Sie die Eigenschaften bearbeiten oder andere Eigenschaften konfigurieren.

Erstellen und Konfigurieren des Suchdienstes

Der Suchdienst ist ein Anwendungsdienst, der Suchvorgänge im Analyst-Tool und in Business Glossary Desktop verwaltet.

Der Suchdienst gibt standardgemäß Suchergebnisse aus einem Modellrepository zurück, z. B. Datenobjekte, Mapping-Spezifikationen, Profile, Referenztabellen, Regeln, Scorecards und Unternehmensglossarbegriffe. Die Suchergebnisse können auch Ergebnisse für Spaltenprofile und Ergebnisse der Domänenerkennung aus einem Profiling Warehouse beinhalten.

Erstellen des Suchdienstes

Erstellen Sie den Dienst mithilfe des Diensterstellungs-Assistenten im Administrator Tool.

Stellen Sie vor dem Erstellen des Suchdienstes sicher, dass Sie die folgenden Dienste erstellt und aktiviert haben:

- Modellrepository-Dienst

  Wenn die Domäne keine Kerberos-Authentifizierung verwendet, stellen Sie sicher, dass Sie einen Modellrepository-Benutzer erstellt haben, über den der Suchdienst auf den Modellrepository-Dienst zugreifen kann.
- Datenintegrationsdienst
- Analyst-Dienst

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie auf**Aktionen** > **Neu** > **Suchdienst**.

   Das Dialogfeld **Neuer Suchdienst** wird geöffnet.
3. Geben Sie auf der Seite **Neuer Suchdienst – Schritt 1 von 2** die folgenden Eigenschaften ein:

Eigenschaft	Beschreibung
Name	Name des Diensts. 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 Diensts. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Domäne und Ordner, in der/dem der Dienst erstellt wurde. Um einen anderen Ordner auszuwählen, klicken Sie auf **Durchsuchen**. Sie können den Dienst nach dessen Erstellung verschieben.
Lizenz	Lizenzobjekt für die Verwendung des Diensts.
Knoten	Knoten, auf dem der Dienst ausgeführt wird.

4. Klicken Sie auf **Weiter**.

   Die Seite **Neuer Suchdienst – Schritt 2 von 2** wird angezeigt.
5. Geben Sie die folgenden Sucheigenschaften für den Suchdienst ein:

Beschreibung	Eigenschaft
Portnummer	Die Portnummer für den Suchdienst.
Indexspeicherort	Das Verzeichnis, das die Suchindex-Dateien enthält. Geben Sie ein Verzeichnis auf dem Computer ein, auf dem der Suchdienst ausgeführt wird. Wenn das Verzeichnis nicht existiert, erstellt Informatica das Verzeichnis beim Erstellen des Suchdienstes.
Extraktionsintervall	Das Intervall in Sekunden, in dem der Suchdienst aktualisierten Inhalt extrahiert und indiziert. Standardwert ist 60 Sekunden.

Beschreibung	Eigenschaft
Modellrepository-Dienst	Modellrepository-Dienst zum Zuweisen zum Dienst.
Benutzername	Benutzername, den der Dienst für den Zugriff auf den Modellrepository-Dienst verwendet. Geben Sie den Modellrepository-Benutzer ein, den Sie erstellt haben.
Passwort	Passwort für den Modellrepository-Benutzer.
Sicherheitsdomäne	LDAP-Sicherheitsdomäne für den Benutzer des Modellrepository. Das Feld wird angezeigt, wenn die Informatica-Domäne eine LDAP-Sicherheitsdomäne enthält. Nicht verfügbar für eine Domäne mit Kerberos-Authentifizierung.

6. Klicken Sie auf **Fertig stellen**.

   Die Domäne erstellt den Suchdienst. Die Domäne aktiviert den Suchdienst während des Diensterstellungsprozesses nicht. Sie müssen den Dienst aktivieren, bevor Benutzer Suchen im Analyst-Tool und im Business Glossary-Desktop durchführen können.

7. Wählen Sie zum Aktivieren des Suchdienstes den Dienst im Navigator aus und klicken Sie auf **Aktionen** > **Dienst aktivieren**.

   Sie können den Suchdienst nur aktivieren, wenn der Modellrepository-Dienst, der Datenintegrationsdienst und der Analyst-Dienst ausgeführt werden.

Nachdem Sie den Dienst mithilfe des Assistenten erstellt haben, können Sie die Eigenschaften bearbeiten oder andere Eigenschaften konfigurieren.

Erstellen und Konfigurieren des PowerCenter-Repository-Dienstes

Der PowerCenter-Repository-Dienst ist ein Anwendungsdienst, der das PowerCenter-Repository verwaltet. Das PowerCenter-Repository speichert vom PowerCenter Client und von Anwendungsdiensten erstellte Metadaten in einer relationalen Datenbank.

Wenn Sie im PowerCenter Client oder PowerCenter-Integrationsdienst auf ein PowerCenter-Repository-Objekt zugreifen, sendet der Client oder Dienst eine Anfrage an den PowerCenter-Repository-Dienst. Der PowerCenter-Repository-Dienst-Prozess ruft Metadaten aus den PowerCenter-Repository-Datenbanktabellen ab, fügt sie dort ein und aktualisiert sie.

Erstellen des PowerCenter-Repository-Dienstes

Erstellen Sie den Dienst mithilfe des Diensterstellungs-Assistenten im Administrator Tool.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie auf **Aktionen** > **Neu** > **PowerCenter-Repository-Dienst**.

   Das Dialogfeld **Neuer PowerCenter-Repository-Dienst** wird angezeigt.

3. Geben Sie auf der Seite **Neuer PowerCenter-Repository-Dienst – Schritt 1 von 2** die folgenden Eigenschaften ein:

Eigenschaft	Beschreibung
Name	Name des Diensts. 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 Diensts. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Domäne und Ordner, in der/dem der Dienst erstellt wurde. Um einen anderen Ordner auszuwählen, klicken Sie auf **Durchsuchen**. Sie können den Dienst nach dessen Erstellung verschieben.
Lizenz	Lizenzobjekt für die Verwendung des Diensts.
Knoten	Knoten, auf dem der Dienst ausgeführt wird.
Primärer Knoten	Wenn die Lizenz hohe Verfügbarkeit einschließt, ist dies der Knoten, auf dem der Dienst standardmäßig ausgeführt wird. Erforderlich, wenn Sie eine Lizenz mit hoher Verfügbarkeit ausgewählt haben.
Backup-Knoten	Wenn die Lizenz hohe Verfügbarkeit einschließt, sind dies die Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist.

4. Klicken Sie auf **Weiter**.

   Die Seite **Neuer PowerCenter-Repository-Dienst – Schritt 2 von 2** wird angezeigt.

5. Geben Sie die folgenden Eigenschaften für die PowerCenter-Repository-Datenbank ein:

Eigenschaft	Beschreibung
Datenbanktyp	Der Typ der Repository-Datenbank.
Benutzername	Der Datenbankbenutzername für das Repository.
Passwort	Passwort für den PowerCenter-Repository-Datenbankbenutzer. Muss in 7-Bit-ASCII kodiert sein.
Verbindungszeichenfolge	Native Verbindungszeichenfolge, die der PowerCenter-Repository-Dienst verwendet, um auf die Repository-Datenbank zuzugreifen. Verwenden Sie die folgende native Syntax der Verbindungszeichenfolge für jede unterstützte Datenbank: - `servername@databasename` für Microsoft SQL Server und Sybase. - `databasename.world` für Oracle - `databasename` für IBM DB2

Eigenschaft	Beschreibung
Codepage	Codepage der Repository-Datenbank. Der PowerCenter-Repository-Dienst verwendet zum Schreiben von Daten den in der Datenbank kodierten Datensatz. Nachdem Sie den PowerCenter-Repository-Dienst erstellt haben, können Sie die Codepage in den Eigenschaften des PowerCenter-Repository-Dienstes nicht mehr ändern.
Tablespace-Name	Name des Tablespace, in dem alle Repository-Datenbanktabellen erstellt werden sollen. Sie können im Tablespace-Namen keine Leerzeichen verwenden. Für IBM DB2- und Sybase-Datenbanken verfügbar. Um die Repository-Leistung bei IBM DB2 EEE-Repositorys zu verbessern, geben Sie einen Tablespace-Namen mit einem Knoten an.

6. Wählen Sie **Die angegebene Verbindungszeichenfolge weist keinen Inhalt auf. Erstellen Sie neue Inhalte.** aus.
7. Optional können Sie ein globales Repository auswählen.

   Nachdem Sie den Dienst erstellen, können Sie ein lokales Repository zu einem globalen Repository hochstufen. Ein globales Repository kann jedoch nicht in ein lokales Repository geändert werden
8. Wenn Ihre Lizenz über die teambasierte Entwicklungsoption verfügt, können Sie optional die Versionskontrolle des Repository aktivieren.

   Nachdem Sie den Dienst erstellt haben, können Sie ein versionsloses Repository in ein Repository mit Versionsangabe konvertieren. Ein Repository mit Versionsangabe in ein versionsloses Repository zu konvertieren, ist jedoch nicht möglich.
9. Klicken Sie auf **Fertig stellen**.

   Die Domäne erstellt den PowerCenter-Repository-Dienst, startet den Dienst und erstellt Inhalt für das PowerCenter-Repository.

Nachdem Sie den Dienst mithilfe des Assistenten erstellt haben, können Sie die Eigenschaften bearbeiten oder andere Eigenschaften konfigurieren.

Nach dem Erstellen des PowerCenter-Repository-Dienstes

Führen Sie nach dem Erstellen des PowerCenter-Repository-Dienstes die folgenden Aufgaben durch:

- Konfigurieren des PowerCenter-Repository-Dienstes zur Ausführung im normalen Modus
- Erstellen des PowerCenter-Repository-Benutzers, wenn die Domäne keine Kerberos-Authentifizierung verwendet
- Erstellen anderer Anwendungsdienste

Führen Sie den PowerCenter-Repository-Dienst im Normalmodus aus.

Nachdem Sie den PowerCenter-Repository-Dienst erstellt haben, wird er im exklusiven Modus gestartet. Der Zugriff ist auf den Administrator beschränkt. Bearbeiten Sie die Diensteigenschaften, um den Dienst im normalen Betriebsmodus auszuführen und anderen Benutzern Zugriff zu gewähren.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten**.
2. Im Navigator wählen Sie den PowerCenter-Repository-Dienst.
3. Klicken Sie auf **Eigenschaften**.
4. Klicken Sie auf **Repository-Eigenschaften bearbeiten**.

5. Wählen Sie „Normal“ im Feld **Betriebsmodus** aus.
6. Klicken Sie auf **OK.**

   Sie müssen den PowerCenter-Repository-Dienst recyceln, damit die Änderungen wirksam werden.
7. Wählen Sie **Aktionen** > **Dienst recyceln**.

Erstellen des PowerCenter-Repository-Benutzers

Wenn die Domäne keine Kerberos-Authentifizierung verwendet, wird die Authentifizierung anderer Anwendungsdienste, die Anfragen an den PowerCenter-Repository-Dienst stellen, mit einem Benutzerkonto durchgeführt. Sie müssen ein Benutzerkonto erstellen und dem Benutzer die Administratorrolle für den PowerCenter-Repository-Dienst zuweisen.

Wenn Sie einen Anwendungsdienst erstellen, der vom PowerCenter-Repository-Dienst abhängig ist, geben Sie den Namen des PowerCenter-Repository-Dienstes und des PowerCenter-Repository-Benutzers an.

1. Klicken Sie im Administrator-Tool auf die Registerkarte **Sicherheit**.
2. Klicken Sie im Menü „Sicherheitsaktionen“ auf **Benutzer erstellen** , um ein natives Benutzerkonto zu erstellen.

   Hinweis: Wenn Sie die LDAP-Authentifizierung in der Domäne einrichten, können Sie ein LDAP-Benutzerkonto für den PowerCenter-Repository-Benutzer verwenden.
3. Geben Sie folgende Eigenschaften für den Benutzer ein:

Eigenschaft	Beschreibung
Anmeldename	Der Anmeldename für das Benutzerkonto. Der Anmeldename für ein Benutzerkonto muss innerhalb der Sicherheitsdomäne, zu der er gehört, eindeutig sein. Beim Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden. Er darf nicht länger als 128 Zeichen sein. Er darf weder einen Tabulator noch ein Zeilenende-Zeichen noch folgende Sonderzeichen enthalten: ,, + " \ < > ; / * % ? & Der Name kann ein ASCII-Leerzeichen enthalten, jedoch nicht als erstes oder letztes Zeichen. Alle anderen Leerzeichen sind nicht zulässig.
Passwort	Das Passwort für das Benutzerkonto. Das Passwort kann zwischen 1 und 80 Zeichen lang sein.
Passwort bestätigen	Geben Sie das Passwort zur Bestätigung erneut ein. Sie müssen das Passwort noch einmal eingeben. Das Passwort darf nicht mit Kopieren und Einfügen eingegeben werden.
Vollständiger Name	Der vollständige Name für das Benutzerkonto. Der vollständige Name darf folgende Sonderzeichen nicht enthalten: < > “
Beschreibung	Die Beschreibung des Benutzerkontos. Die Beschreibung darf nicht länger als 765 Zeichen sein und keines der folgenden Sonderzeichen enthalten: < > “

4. Klicken Sie auf **OK**.

   Die Benutzereigenschaften werden angezeigt.
5. Klicken Sie auf die Registerkarte **Berechtigungen**.
6. Klicken Sie auf **Bearbeiten**.

Das Dialogfeld **Rollen und Rechte bearbeiten** wird eingeblendet.

7. Erweitern Sie auf der Registerkarte **Rollen** den PowerCenter-Repository-Dienst.
8. Wählen Sie unter **Systemdefinierte Rollen** „Administrator“ aus und klicken Sie auf **OK**.

Erstellen weiterer Dienste

Nach dem Erstellen des PowerCenter-Repository-Dienstes erstellen Sie die Anwendungsdienste, die vom PowerCenter-Repository-Dienst abhängig sind.

Sie können die folgenden Anwendungsdienste erstellen:

1. PowerCenter-Integrationsdienst
2. Metadata Manager-Dienst
3. Webdienst-Hub-Dienst

Erstellen und Konfigurieren des PowerCenter-Integrationsdienstes

Der PowerCenter-Integrationsdienst ist ein Anwendungsdienst, der Arbeitsabläufe und Sitzungen für den PowerCenter Client ausführt.

Wenn Sie einen Arbeitsablauf im PowerCenter Client ausführen, sendet der Client die Anfragen an den PowerCenter-Integrationsdienst. Der PowerCenter-Integrationsdienst stellt eine Verbindung zum PowerCenter-Repository-Dienst zum Abrufen von Metadaten aus dem PowerCenter-Repository her und führt anschließend die Sitzungen und Arbeitsabläufe aus und überwacht sie.

Erstellen des PowerCenter-Integrationsdienstes

Erstellen Sie den Dienst mithilfe des Diensterstellungs-Assistenten im Administrator Tool.

Stellen Sie vor dem Erstellen des PowerCenter-Integrationsdienstes sicher, dass Sie den PowerCenter-Repository-Dienst erstellt und aktiviert haben. Wenn die Domäne keine Kerberos-Authentifizierung verwendet, stellen Sie sicher, dass Sie einen PowerCenter-Repository-Benutzer erstellt haben, über den der PowerCenter-Integrationsdienst auf den PowerCenter-Repository-Dienst zugreifen kann.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie auf **Aktionen** > **Neu** > **PowerCenter-Integrationsdienst**.

   Das Dialogfeld **Neuer PowerCenter-Integrationsdienst** wird eingeblendet.

3. Geben Sie auf der Seite **Neuer PowerCenter-Integrationsdienst – Schritt 1 von 2** die folgenden Eigenschaften ein:

Eigenschaft	Beschreibung
Name	Name des Diensts. 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 Diensts. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Domäne und Ordner, in der/dem der Dienst erstellt wurde. Um einen anderen Ordner auszuwählen, klicken Sie auf **Durchsuchen**. Sie können den Dienst nach dessen Erstellung verschieben.
Lizenz	Lizenzobjekt für die Verwendung des Diensts.
Knoten	Knoten, auf dem der Dienst ausgeführt wird.
Zuweisen	Wählen Sie **Knoten** aus, um den Dienst zur Ausführung auf einem Knoten zu konfigurieren. Wenn die Lizenz Gitter einschließt, können Sie ein Gitter erstellen und den auf dem Gitter auszuführenden Dienst zuweisen, nachdem Sie den Dienst erstellt haben.
Primärer Knoten	Wenn die Lizenz hohe Verfügbarkeit einschließt, ist dies der Knoten, auf dem der Dienst standardmäßig ausgeführt wird. Erforderlich, wenn Sie eine Lizenz mit hoher Verfügbarkeit ausgewählt haben.
Backup-Knoten	Wenn die Lizenz hohe Verfügbarkeit einschließt, sind dies die Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist.

4. Klicken Sie auf **Weiter**.
5. Geben Sei auf der Seite **Neuer PowerCenter-Integrationsdienst – Schritt 2 von 2** die folgenden Eigenschaften ein:

Eigenschaft	Beschreibung
PowerCenter-Repository-Dienst	PowerCenter-Repository-Dienst, der dem Dienst zugeordnet werden soll.
Benutzername	Benutzername, den der Dienst für den Zugriff auf den PowerCenter-Repository-Dienst verwendet. Geben Sie den PowerCenter-Repository-Benutzer ein, den Sie erstellt haben. Erforderlich, wenn Sie dem Dienst einen PowerCenter-Repository-Dienst zuordnen. Nicht verfügbar für eine Domäne mit Kerberos-Authentifizierung.

Eigenschaft	Beschreibung
Passwort	Dem PowerCenter-Repository-Benutzer zugeordnetes Passwort. Nicht verfügbar für eine Domäne mit Kerberos-Authentifizierung.
Sicherheitsdomäne	LDAP-Sicherheitsdomäne für den Benutzer des PowerCenter-Repository. Das Feld **Sicherheitsdomäne** wird eingeblendet, wenn die Informatica-Domäne eine LDAP-Sicherheitsdomäne enthält. Erforderlich, wenn Sie dem Dienst einen PowerCenter-Repository-Dienst zuordnen. Nicht verfügbar für eine Domäne mit Kerberos-Authentifizierung.

6. Wählen Sie den Datenverschiebungsmodus aus, der bestimmt, wie der PowerCenter-Integrationsdienst Zeichendaten verarbeitet. Wählen Sie ASCII oder Unicode aus. Der Standardwert ist ASCII.

   Im ASCII-Modus erkennt der PowerCenter-Integrationsdienst 7-Bit-ASCII- und EBCDIC-Zeichen und speichert jedes Zeichen in einem einzelnen Byte. Im Unicode-Modus erkennt der PowerCenter-Integrationsdienst Multibyte-Zeichensätze, wie sie von unterstützten Codepages definiert sind. Verwenden Sie den Unicode-Modus, wenn Quellen oder Targets 8-Bit- oder Multibyte-Zeichensätze verwenden und Zeichendaten enthalten.
7. Klicken Sie auf **Fertig stellen**.
8. Weisen Sie im Dialogfeld **Codepages angeben** einen Code für den PowerCenter-Integrationsdienst zu.

   Die Codepage für den PowerCenter-Integrationsdienst muss kompatibel sein mit der Codepage des zugeordneten Repository.
9. Klicken Sie auf **OK**.

   Die Domäne erstellt den PowerCenter-Integrationsdienst. Die Domäne aktiviert den PowerCenter-Integrationsdienst während der Diensterstellung nicht.
10. Zum Aktivieren des PowerCenter-Integrationsdienstes wählen Sie den Dienst im Navigator aus und klicken Sie auf **Aktionen** > **Dienst aktivieren**. Der PowerCenter-Repository-Dienst muss ausgeführt werden, um den PowerCenter-Integrationsdienst zu aktivieren.

Nachdem Sie den Dienst mithilfe des Assistenten erstellt haben, können Sie die Eigenschaften bearbeiten oder andere Eigenschaften konfigurieren.

Nach dem Erstellen des PowerCenter-Integrationsdienstes

Nach dem Erstellen des PowerCenter-Integrationsdienstes erstellen Sie den Metadata Manager-Dienst, der vom PowerCenter-Integrationsdienst abhängig ist.

Erstellen und Konfigurieren des Metadata Manager-Dienstes

Der Metadata Manager-Dienst ist ein Anwendungsdienst, der den Metadata Manager-Web-Client in der Informatica-Domäne ausführt. Der Metadata Manager-Dienst verwaltet die Verbindungen zwischen Dienstkomponenten und den Benutzern, die Zugriff auf Metadata Manager haben.

Beim Laden von Metadaten in das Metadata Manager-Warehouse stellt der Metadata Manager-Dienst eine Verbindung zum PowerCenter-Integrationsdienst her. Der PowerCenter-Integrationsdienst führt die Arbeitsabläufe im PowerCenter-Repository aus, um aus Metadatenquellen zu lesen und Metadaten in das

Metadata Manager-Warehouse zu laden. Wenn Sie Metadata Manager verwenden, um Metadaten zu durchsuchen und zu analysieren, greift der Metadata Manager-Dienst auf die Metadaten aus dem Metadata Manager-Repository zu.

Erstellen des Metadata Manager-Dienstes

Erstellen Sie den Dienst mithilfe des Diensterstellungs-Assistenten im Administrator Tool.

Stellen Sie vor dem Erstellen des Metadata Manager-Dienstes sicher, dass Sie die folgenden Dienste erstellt und aktiviert haben:

- PowerCenter-Repository-Dienst
  Wenn die Domäne keine Kerberos-Authentifizierung verwendet, stellen Sie sicher, dass Sie einen PowerCenter-Repository-Benutzer erstellt haben, über den der Metadata Manager-Dienst auf den PowerCenter-Repository-Dienst zugreifen kann.
- PowerCenter-Integrationsdienst

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie auf **Aktionen** > **Neu** > **Metadata Manager-Dienst**.

   Das Dialogfeld **Neuer Metadata Manager-Dienst** erscheint.
3. Geben Sie auf der Seite **Neuer Metadata Manager-Dienst – Schritt 1 von 3** die folgenden Eigenschaften ein:

Eigenschaft	Beschreibung
Name	Name des Diensts. 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 Diensts. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Domäne und Ordner, in der/dem der Dienst erstellt wurde. Um einen anderen Ordner auszuwählen, klicken Sie auf **Durchsuchen**. Sie können den Dienst nach dessen Erstellung verschieben.
Lizenz	Lizenzobjekt für die Verwendung des Diensts.
Knoten	Knoten, auf dem der Dienst ausgeführt wird.

4. Geben Sie die folgenden Eigenschaften des zugehörigen Repository-Dienstes:

Eigenschaft	Beschreibung
Zugehöriger Integrationsdienst	Wählen Sie den PowerCenter-Integrationsdienst aus, über den der Metadata Manager Metadaten in das Metadata Manager-Warehouse lädt.
Repository-Benutzername	Benutzername, den der Dienst für den Zugriff auf den PowerCenter-Repository-Dienst verwendet. Geben Sie den PowerCenter-Repository-Benutzer ein, den Sie erstellt haben. Erforderlich, wenn Sie dem Dienst einen PowerCenter-Repository-Dienst zuordnen. Nicht verfügbar für eine Domäne mit Kerberos-Authentifizierung.
Repository-Passwort	Dem PowerCenter-Repository-Benutzer zugeordnetes Passwort. Nicht verfügbar für eine Domäne mit Kerberos-Authentifizierung.
Sicherheitsdomäne	LDAP-Sicherheitsdomäne für den Benutzer des PowerCenter-Repository. Das Feld **Sicherheitsdomäne** wird eingeblendet, wenn die Informatica-Domäne eine LDAP-Sicherheitsdomäne enthält. Erforderlich, wenn Sie dem Dienst einen PowerCenter-Repository-Dienst zuordnen. Nicht verfügbar für eine Domäne mit Kerberos-Authentifizierung.

5. Klicken Sie auf **Weiter**.

   Die Seite **Neuer Metadata Manager-Dienst – Schritt 2 von 3** wird angezeigt.

6. Geben Sie die folgenden Datenbankeigenschaften für das Metadata Manager-Repository ein:

Eigenschaft	Beschreibung
Datenbanktyp	Der Typ der Repository-Datenbank.
Codepage	Codepage für Metadaten Manager-Repository. Der Metadata Manager-Dienst und die Metadata Manager-Anwendung nutzen beim Schreiben von Daten in das Metadata Manager-Repository den Zeichensatz, der in der Repository-Codepage codiert ist. Sie können den Metadata Manager-Dienst erst nach Angabe der Codepage aktivieren.
Verbindungszeichenfolge	Native Verbindungszeichenfolge für die Metadata Manager-Repository-Datenbank. Der Metadata Manager-Dienst verwendet die Verbindungszeichenfolge, um ein Verbindungsobjekt zum Metadata Manager-Repository im PowerCenter-Repository zu erstellen. Verwenden Sie die folgende native Syntax der Verbindungszeichenfolge für jede unterstützte Datenbank: - `servername@databasename` für Microsoft SQL Server - `databasename.world` für Oracle - `databasename` für IBM DB2
Datenbankbenutzer	Der Datenbankbenutzername für das Repository.
Datenbankpasswort	Passwort für den Metadata Manager-Repository-Datenbankbenutzer. Muss in 7-Bit-ASCII kodiert sein.

Eigenschaft	Beschreibung
Tablespace-Name	Name des Tablespace, in dem alle Repository-Datenbanktabellen erstellt werden sollen. Sie können im Tablespace-Namen keine Leerzeichen verwenden. Für IBM DB2-Datenbanken. Um die Repository-Leistung bei IBM DB2 EEE-Repositorys zu verbessern, geben Sie einen Tablespace-Namen mit einem Knoten an.
Datenbankhostname	Name des Computers, der als Host für den Datenbankserver dient.
Datenbankport	Die Portnummer, mit der Sie den Listenerdienst für den Datenbankserver konfigurieren.
SID/Dienstname	Für Oracle-Datenbanken. Gibt an, ob die SID oder der Dienstname in der JDBC-Verbindungszeichenfolge verwendet werden soll. Für Oracle RAC-Datenbanken wählen Sie Oracle-SID oder Oracle-Dienstname. Für andere Oracle-Datenbanken wählen Sie die Oracle-SID aus.
Datenbankname	Der Name des Datenbankservers. Geben Sie den vollständigen Dienstnamen oder die SID für Oracle-Datenbanken, den Dienstnamen für IBM DB2-Datenbanken und den Datenbanknamen für Microsoft SQL Server-Datenbanken an.

7. Wenn Sie Parameter an die Datenbankverbindungs-URL anhängen, konfigurieren Sie zusätzliche Parameter im Feld **Zusätzliche JDBC-Parameter**. Geben Sie die Parameter als Name = Wertpaare, getrennt durch ein Semikolon (;) ein. Beispiel: `param1=value1;param2=value2`

Sie können diese Eigenschaft verwenden, um die folgenden Parameter anzugeben:

Parameter	Beschreibung
Speicherort des Sicherungsservers	Wenn Sie einen hochverfügbaren Datenbankserver wie zum Beispiel Oracle RAC verwenden, geben Sie den Speicherort eines Sicherungsservers ein.
Oracle ASO (Advanced Security Option)-Parameter	Wenn die Metadata Manager-Repository-Datenbank eine Oracle-Datenbank ist, die ASO verwendet, geben Sie die folgenden zusätzlichen Parameter ein: `EncryptionLevel=[encryption level];EncryptionTypes=[encryption types];DataIntegrityLevel=[data integrity level];DataIntegrityTypes=[data integrity types]` **Hinweis:** Die Parameterwerte müssen den Werten in der Datei `sqlnet.ora` auf dem Computer entsprechen, auf dem der Metadata Manager-Dienst ausgeführt wird.

Authentifizierungsinformationen für Microsoft SQL Server	Zum Authentifizieren der Benutzeranmeldedaten und Einrichten einer vertrauenswürdigen Verbindung zu einem Microsoft SQL Server-Repository geben Sie den folgenden Text ein:
	`AuthenticationMethod=ntlm;LoadLibraryPath=[directory containing DDJDBCx64Auth04.dll].`
	`jdbc:informatica:sqlserver://[host]:[port];DatabaseName=[DB name];AuthenticationMethod=ntlm;LoadLibraryPath=[directory containing DDJDBCx64Auth04.dll]`
	Wenn Sie eine vertrauenswürdige Verbindung verwenden, um eine Verbindung zu einer Microsoft SQL Server-Datenbank herzustellen, stellt der Metadata Manager-Dienst eine Verbindung zum Repository mit den Anmeldeinformationen des Benutzers her, der auf dem Computer angemeldet ist, auf dem der Dienst ausgeführt wird.
	Um den Metadata Manager-Dienst als Windows-Dienst mithilfe einer vertrauenswürdigen Verbindung zu starten, konfigurieren Sie die Eigenschaften des Windows-Dienstes so, dass die Anmeldung mit einem vertrauenswürdigen Benutzerkonto erfolgt.

8. Wenn das Metadata Manager-Repository für die sichere Kommunikation konfiguriert ist, können Sie zusätzliche JDBC-Parameter im Feld **Sichere JDBC-Parameter** konfigurieren.

   Verwenden Sie diese Eigenschaft, um sichere Verbindungsparameter wie Passwörter anzugeben. Das Administrator-Tool zeigt keine sicheren Parameter bzw. die Parameterwerte in den Eigenschaften des Metadata Manager-Diensts an. Geben Sie die Parameter als Name = Wertpaare, getrennt durch ein Semikolon (;) ein. Beispiel: `param1=value1;param2=value2`.
   Geben Sie die folgenden sicheren Datenbankparameter ein:

Sicherer Datenbankparameter	Beschreibung
EncryptionMethod	Erforderlich. Gibt an, ob Daten bei der Netzwerkübertragung verschlüsselt werden. Dieser Parameter muss auf `SSL` festgelegt werden.
TrustStore	Erforderlich. Pfad und Dateiname der TrustStore-Datei, die das SSL-Zertifikat des Datenbankservers enthält.
TrustStorePassword	Erforderlich. Passwort für den Zugriff auf die Truststore-Datei.

Sicherer Datenbankparameter	Beschreibung
HostNameInCertificate	Hostname des Computers, auf dem die sichere Datenbank gehostet wird. Wenn Sie einen Hostnamen angeben, vergleicht der Metadata Manager-Dienst den Hostnamen in der Verbindungszeichenfolge mit dem Hostnamen im SSL-Zertifikat.
ValidateServerCertificate	Optional. Gibt an, ob Informatica das Zertifikat validiert, das der Datenbankserver sendet. Wenn dieser Parameter auf TRUE gesetzt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat. Wenn Sie den HostNameInCertificate-Parameter angeben, validiert Informatica ebenfalls den Hostnamen im Zertifikat. Wenn dieser Parameter auf FALSE gesetzt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat nicht. Informatica ignoriert alle Truststore-Informationen, die Sie angeben.
KeyStore	Pfad und Dateiname der Schlüsselspeicherdatei mit den SSL-Zertifikaten, die der Metadata Manager-Dienst an den Datenbankserver sendet.
KeyStorePassword	Passwort für den Zugriff auf die Schlüsselspeicherdatei.

9. Klicken Sie auf **Weiter.**

   Die Seite **Neuer Metadata Manager-Dienst – Schritt 3 von 3** wird angezeigt.

10. Geben Sie die HTTP-Portnummer für den Dienst ein.

11. Zum Aktivieren der sicheren Kommunikation mit dem Metadata Manager-Dienst wählen Sie **Secured Socket Layer aktivieren** aus.

    Geben Sie die folgenden Eigenschaften ein, um die sichere Kommunikation für den Dienst zu konfigurieren:

Eigenschaft	Beschreibung
HTTPS-Port	Zu verwendende Portnummer für eine sichere Verbindung zum Dienst. Verwenden Sie eine Portnummer, die sich von der HTTP-Portnummer unterscheidet.
Schlüsselspeicherdatei	Pfad und Dateiname der Schlüsselspeicherdatei, die die privaten oder öffentlichen Schlüsselpaare und die zugeordneten Zertifikate enthält. Erforderlich, wenn Sie HTTPS-Verbindungen für den Dienst verwenden.
Schlüsselspeicher-Passwort	Klartext-Passwort für die Schlüsselspeicherdatei.

12. Klicken Sie auf **Fertig stellen**.

    Die Domäne erstellt den Metadata Manager-Dienst. Die Domäne aktiviert den Metadata Manager-Dienst während der Diensterstellung nicht.

13. Zum Aktivieren des Metadata Manager-Dienstes wählen Sie den Dienst im Navigator aus und klicken Sie auf **Aktionen** > **Dienst aktivieren**. Der PowerCenter-Repository-Dienst und der PowerCenter-Integrationsdienst müssen ausgeführt werden, um den Metadata Manager-Dienst zu aktivieren.

Nachdem Sie den Dienst mithilfe des Assistenten erstellt haben, können Sie die Eigenschaften bearbeiten oder andere Eigenschaften konfigurieren.

Nach dem Erstellen des Metadata Manager-Dienstes

Führen Sie nach dem Erstellen des Metadata Manager-Dienstes die folgenden Aufgaben durch:

- Erstellen der Inhalte für das Metadata Manager-Repository
- Erstellen anderer Anwendungsdienste

Beim Erstellen des Metadata Manager-Diensts erstellen Sie die Repository-Tabellen und importieren Modelle für Metadatenquellen.

1. Wählen Sie im Navigator den Metadata Manager-Dienst aus.
2. Klicken Sie auf **Aktionen** > **Repository-Inhalte** > **Erstellen**.
3. Klicken Sie auf **OK**.

Nach dem Erstellen des Metadata Manager-Dienstes erstellen Sie die Anwendungsdienste, die vom Metadata Manager-Dienst abhängig sind.

Erstellen und Konfigurieren des Webdienst-Hub-Dienstes

Der Webdienst-Hub-Dienst ist ein Anwendungsdienst in der Informatica-Domäne, der die PowerCenter-Funktionalität über Webdienste an externe Clients freigibt.

Der Webdienst-Hub-Dienst erhält Anfragen von Webdienst-Cients und gibt sie je nach Anfragetyp an den PowerCenter-Integrationsdienst oder den PowerCenter-Repository-Dienst weiter. Der PowerCenter-Integrationsdienst bzw. der PowerCenter-Repository-Dienst verarbeitet die Anfragen und sendet die Antwort an den Webdienst-Hub. Der Webdienst-Hub sendet eine Antwort zurück an den Webdienst-Client.

Erstellen des Webdienst-Hub-Dienstes

Erstellen Sie den Dienst mithilfe des Diensterstellungs-Assistenten im Administrator Tool.

Stellen Sie vor dem Erstellen des Webdienst-Hub-Dienstes sicher, dass Sie den PowerCenter-Repository-Dienst erstellt und aktiviert haben.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie auf **Aktionen** > **Neu** > **Webdienst-Hub**.

   Das Dialogfeld **Neuer Webdienst-Hub-Dienst** wird angezeigt.

3. Geben Sie die folgenden Eigenschaften ein:

Eigenschaft	Beschreibung
Name	Name des Diensts. 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 Diensts. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Domäne und Ordner, in der/dem der Dienst erstellt wurde. Um einen anderen Ordner auszuwählen, klicken Sie auf **Durchsuchen**. Sie können den Dienst nach dessen Erstellung verschieben.
Lizenz	Lizenzobjekt für die Verwendung des Diensts.
Knoten	Knoten, auf dem der Dienst ausgeführt wird.

4. Geben Sie die folgenden Eigenschaften des zugeordneten PowerCenter-Repository-Dienstes ein:

Eigenschaft	Beschreibung
Zugeordneter Repository-Dienst	PowerCenter-Repository-Dienst, der dem Dienst zugeordnet werden soll.
Repository-Benutzername	Benutzername, den der Dienst für den Zugriff auf den PowerCenter-Repository-Dienst verwendet. Geben Sie den PowerCenter-Repository-Benutzer ein, den Sie erstellt haben. Erforderlich, wenn Sie dem Dienst einen PowerCenter-Repository-Dienst zuordnen. Für den Webdienst-Hub-Dienst ist der Repository-Benutzername auch dann erforderlich, wenn die Kerberos-Authentifizierung aktiviert ist.
Repository-Passwort	Dem PowerCenter-Repository-Benutzer zugeordnetes Passwort. Für den Webdienst-Hub-Dienst ist das Repository-Passwort auch dann erforderlich, wenn die Kerberos-Authentifizierung aktiviert ist.
Sicherheitsdomäne	LDAP-Sicherheitsdomäne für den Benutzer des PowerCenter-Repository. Das Feld **Sicherheitsdomäne** wird eingeblendet, wenn die Informatica-Domäne eine LDAP-Sicherheitsdomäne enthält. Erforderlich, wenn Sie dem Dienst einen PowerCenter-Repository-Dienst zuordnen.

5. Klicken Sie auf **Weiter**.

6. Geben Sie die folgenden Diensteigenschaften ein:

Eigenschaft	Beschreibung
URL-Schema	Gibt das von Ihnen für den Webdienst-Hub konfigurierte Sicherheitsprotokoll an. Sie können eine der folgenden Optionen auswählen: - HTTP. Ausführen des Webdienst-Hub nur unter HTTP. - HTTPS. Ausführen des Webdienst-Hub nur unter HTTPS. - HTTP und HTTPS. Ausführen des Webdienst-Hub in den Modi HTTP und HTTPS.
Hub-Hostname	Der Name des Computers, auf dem der Webdienst-Hub gehostet wird.
Hub-Portnummer (HTTP)	Die Portnummer für den Webdienst-Hub, der unter HTTP ausgeführt wird. Standardwert ist 7333.
Hub-Portnummer (HTTPS)	Die Portnummer für den Webdienst-Hub, der unter HTTPS ausgeführt wird. Standardwert ist 7343.
Schlüsselspeicherdatei	Pfad und Dateiname der Schlüsselspeicherdatei, die die privaten oder öffentlichen Schlüsselpaare und die zugeordneten Zertifikate enthält. Erforderlich, wenn Sie HTTPS-Verbindungen für den Dienst verwenden.
Schlüsselspeicherpasswort	Klartext-Passwort für die Schlüsselspeicherdatei.
Interner Hostname	Optional. Der Hostname, mit dem der Webdienst-Hub Verbindungen vom PowerCenter-Integrationsdienst abhört.
Interne Portnummer	Portnummer, die der Webdienst-Hub bei Verbindungen vom PowerCenter-Integrationsdienst erwartet. Voreingestellt ist 15555.

7. Klicken Sie auf **Fertig stellen**.

   Die Domäne erstellt den Webdienst-Hub-Dienst. Die Domäne aktiviert den Webdienst-Hub-Dienst während des Diensterstellungsprozesses nicht.

8. Wählen Sie zum Aktivieren des Webdienst-Hub-Dienstes den Dienst im Navigator aus und klicken Sie auf **Aktionen** > **Dienst aktivieren**.

Nachdem Sie den Dienst mithilfe des Assistenten erstellt haben, können Sie die Eigenschaften bearbeiten oder andere Eigenschaften konfigurieren.

Teil V: Client-Installation

Dieser Teil enthält die folgenden Kapitel:

- Vor dem Installieren der Clients, 226
- Installieren der Clients, 228
- Nach dem Installieren der Informatica-Clients, 232
- Starten der Informatica-Clients, 235

KAPITEL 12

Vor dem Installieren der Clients

Dieses Kapitel umfasst die folgenden Themen:

- Vor dem Installieren der Clients - Übersicht, 226
- Überprüfen der Installationsanforderungen, 226
- Überprüfen des Bedarfs an Software von Drittanbietern, 227

Vor dem Installieren der Clients - Übersicht

Stellen Sie vor dem Installieren der Informatica-Clients unter Windows sicher, dass die minimalen System- und Drittanbietersoftware-Anforderungen erfüllt sind. Wenn der Computer, auf dem Sie die Informatica-Clients installieren möchten, nicht ordnungsgemäß konfiguriert ist, kann die Installation fehlschlagen.

Überprüfen der Installationsanforderungen

Überprüfen Sie vor dem Installieren der Informatica-Clients, ob die Installationsanforderungen zum Ausführen der Informatica-Client-Tools erfüllt sind.

Sie können alle Informatica-Client-Tools auf ein und demselben Computer oder auf separaten Computern installieren. Die Clients können ebenfalls auf mehreren Rechnern installiert werden. Die Anforderungen für die Informatica-Clients hängen von den Client-Tools ab, die Sie installieren.

Überprüfen Sie vor dem Installieren der Informatica-Clients die folgenden Installationsanforderungen:

Speicherplatz für die temporären Dateien

Das Installationsprogramm schreibt temporäre Dateien auf die Festplatte. Stellen Sie sicher, dass für die Installation 1 GB Speicherplatz auf dem Computer vorhanden ist. Nach Abschluss der Installation werden die temporären Dateien gelöscht und der Speicherplatz wird freigegeben.

Berechtigungen zum Installieren der Clients

Stellen Sie sicher, dass das Benutzerkonto, das Sie zum Installieren der Informatica-Clients verwenden, keine Schreibberechtigung für das Installationsverzeichnis und die Windows-Registrierung hat.

Mindestsystemanforderungen zum Ausführen der Informatica-Client-Tools

In der folgenden Tabelle werden die Mindestsystemanforderungen für das Ausführen des Informatica-Client-Tools aufgelistet:

Client	Prozessor	RAM	Festplattenspeicher
PowerCenter Client	1 CPU	1 GB	3 GB
Informatica Developer	1 CPU	1 GB	6 GB

Überprüfen des Bedarfs an Software von Drittanbietern

Stellen Sie vor dem Installieren der Informatica-Clients sicher, dass Sie die für die Clients erforderliche Software von Drittanbietern installiert haben.

PowerCenter Client-Anforderungen

Die PowerCenter Client-Installation enthält Mapping Architect for Visio und Mapping Analyst for Excel.

Wenn Sie Mapping Architect for Visio verwenden möchten, installieren Sie die folgende Software von Drittanbietern, bevor Sie den PowerCenter Client installieren:

- Version 2007 oder 2010 von Microsoft Visio
- Microsoft .NET Framework 4

Wichtig: Wenn Sie nicht die richtige Version und das richtige Service Pack von Microsoft .NET Framework installieren, wird Mapping Architect for Visio nicht ordnungsgemäß installiert.

Mapping Analyst for Excel enthält ein Excel-Add-In, das ein Metadatenmenü oder ein Menüband zu Microsoft Excel hinzufügt. Sie können das Add-In nur für Excel 2007 oder 2010 installieren. Wenn Sie Mapping Architect for Excel verwenden möchten, installieren Sie die folgende Software von Drittanbietern, bevor Sie den PowerCenter Client installieren:

- Version 2007 oder 2010 von Microsoft Office Excel
- Java-Version 1.8 oder höher

Anforderungen für Data Transformation

Wenn Sie planen, Datenprozessor- oder Umwandlungen von hierarchisch auf relational zu verwenden, installieren Sie .NET Framework 4.0 oder höher, bevor Sie das Developer Tool installieren.

KAPITEL 13

Installieren der Clients

Dieses Kapitel umfasst die folgenden Themen:

- Installieren der Clients - Übersicht, 228
- Installation im Grafikmodus, 229
- Automatische Installation, 230

Installieren der Clients - Übersicht

Sie können sie unter Windows im Grafikmodus oder automatisch installieren.

Führen Sie die Vorinstallationsaufgaben zur Vorbereitung auf die Installation durch. Sie können die Informatica-Clients auf mehreren Computern installieren. Zum Ausführen von Custom Metadata Configurator müssen Sie sowohl Informatica Developer als auch den PowerCenter Client installieren.

Beim Ausführen des Clientinstallationsprogramms können Sie die folgenden Informatica-Client-Tools auswählen:

Informatica Developer

Informatica Developer ist eine Clientanwendung, die Sie zum Erstellen von Datenobjekten und virtuellen Datenbanken sowie zum Erstellen und Ausführen von Zuordnungen verwenden. Sie können Informatica Developer außerdem verwenden, um Profile auszuführen und Datenerkennung durchzuführen. In Informatica Developer erstellte Objekte werden in einem Modellrepository gespeichert und von einem Datenintegrationsdienst ausgeführt.

PowerCenter Client

Der PowerCenter Client enthält mehrere Tools, die zum Verwalten des PowerCenter-Repositorys sowie von Zuordnungen und Sitzungen verwendet werden können. Der PowerCenter Client umfasst die folgenden Tools:

- Custom Metadata Configurator (für Metadata Manager)
- PowerCenter Designer
- PowerCenter Mapping Architect for Visio
- PowerCenter Repository Manager
- PowerCenter-Arbeitsablauf-Manager
- PowerCenter Workflow Monitor

Hinweis: Informatica empfiehlt, dass Sie die Informatica Services und den PowerCenter Client in verschiedenen Verzeichnissen installieren, weil bei einer Installation von Informatica Services und

PowerCenter Client im selben Verzeichnis die Programmdateien deinstalliert werden, wenn Sie den PowerCenter Client deinstallieren.

Installation im Grafikmodus

Sie können die Informatica-Clients im Grafikmodus unter Windows installieren.

1. Schließen Sie alle anderen Anwendungen.
2. Wechseln Sie in das Stammverzeichnis für die Installationsdateien und führen Sie die Datei „install.bat“ als Administrator aus.

   Klicken Sie zum Ausführen der Datei als Administrator mit der rechten Maustaste auf die Datei „install.bat“ und wählen Sie **Als Administrator ausführen** aus.

   Hinweis: Wenn Sie das Installationsprogramm nicht als Administrator ausführen, meldet der Windows-Systemadministrator möglicherweise Probleme, wenn Sie auf die Dateien im Informatica-Installationsverzeichnis zugreifen.

   Wenn beim Ausführen der Datei „install.bat“ im Root-Verzeichnis Probleme auftreten, führen Sie die folgende Datei aus: `<Verzeichnis der Installationsdateien>\client\install.exe`
3. Wählen Sie **Informatica <Version>-Clients installieren** aus und klicken Sie auf **Weiter**.

   Die Seite **Installationsvoraussetzungen** zeigt die Systemanforderungen an. Vergewissern Sie sich, dass alle Voraussetzungen für die Installation erfüllt sind, bevor Sie die Installation fortsetzen.
4. Klicken Sie auf **Weiter**.

   Wählen Sie auf der Seite **Anwendungs-Client-Auswahl** den Informatica-Client aus, den Sie installieren möchten.

   Die folgenden Informatica-Client-Anwendungen können auf ein und demselben Rechner installiert werden:

   - Informatica Developer
   - PowerCenter Client

   Sie können mehrere Clients gleichzeitig auswählen.
5. Geben Sie auf der Seite **Installationsverzeichnis** den absoluten Pfad für das Installationsverzeichnis ein.

   Das Installationsverzeichnis muss sich auf dem aktuellen Rechner befinden. Der Pfad darf maximal 260 Zeichen umfassen. Die Verzeichnisnamen in dem Pfad dürfen weder Leerzeichen noch die folgenden Sonderzeichen enthalten: @|* $ # ! % ( ) { } [ ] , ; '

   Hinweis: Informatica empfiehlt die Verwendung alphanumerischer Zeichen im Installationsverzeichnispfad. Wenn Sie ein Sonderzeichen wie zum Beispiel á oder € verwenden, können unerwartete Ergebnisse während der Laufzeit auftreten.
6. Klicken Sie auf **Weiter**.
7. Überprüfen Sie auf der Seite mit der **Vorinstallationsübersicht** die Installationsdaten und klicken Sie auf **Installieren**.

   Die Informatica-Client-Dateien werden in das Installationsverzeichnis kopiert.

   Die Nachinstallationsübersicht zeigt an, ob die Installation erfolgreich abgeschlossen wurde.
8. Klicken Sie auf **Fertig** zum Beenden des Installers.

In den Installations-Protokolldateien finden Sie weitere Informationen zu den vom Installer durchgeführten Aufgaben.

Automatische Installation

Beim automatischen Installieren der Informatica-Clients ist keinerlei Benutzereingriff erforderlich.

Geben Sie die Installationsoptionen mithilfe einer Eigenschaftendatei an. Das Installationsprogramm liest die Datei, um die Installationsoptionen festzustellen. Mit der automatischen Installation können Sie die Informatica-Clients auf mehreren Computern im Netzwerk installieren oder die Installation auf den verschiedenen Computern standardisieren.

Gehen Sie zum automatischen Installieren folgendermaßen vor:

1. Konfigurieren Sie die Installationseigenschaftendatei und geben Sie darin die Installationsoptionen an.
2. Führen Sie das Installationsprogramm mit der Installationseigenschaftendatei aus.

Konfigurieren der Eigenschaftendatei

Informatica liefert eine Beispiel-Eigenschaftendatei, die die vom Installationsprogramm benötigten Eigenschaften enthält. Passen Sie die Beispiel-Eigenschaftendatei an, um eine Eigenschaftendatei zu erstellen und legen Sie die Optionen für Ihre Installation fest. Führen Sie anschließend die Installation im Hintergrund aus.

Die Beispieldatei SilentInput.properties befindet sich im Root-Verzeichnis auf der DVD oder im Downloadverzeichnis des Installationsprogramms.

1. Wechseln Sie zum Verzeichnis-Root, der den Installer enthält.
2. Suchen Sie die Beispieldatei `SilentInput.properties`.
3. Erstellen Sie eine Sicherungskopie der Datei „SilentInput.properties“.
4. Verwenden Sie einen Texteditor, um die Datei zu öffnen, und ändern Sie die Werte der Eigenschaften.

   In der folgenden Tabelle werden die Installationseigenschaften beschrieben, die Sie ändern können:

Eigenschaftsname	Beschreibung
INSTALL_TYPE	Zeigt an, ob Informatica-Clients installiert oder aktualisiert werden müssen. Wenn der Wert 0 ist, werden die Informatica-Clients in dem von Ihnen festgelegten Verzeichnis installiert. Wenn der Wert 1 ist, werden die Informatica-Clients aktualisiert. Standard ist 0.
UPG_BACKUP_DIR	Verzeichnis der vorigen Version des Informatica-Clients, die Sie upgraden möchten.
USER_INSTALL_DIR	Informatica-Client-Installationsverzeichnis.

Eigenschaftsname	Beschreibung
DXT_COMP	Zeigt an, ob Informatica Developer installiert werden muss. Wenn der Wert 1 ist, wird das Developer-Tool installiert. Wenn der Wert 0 ist, wird das Developer-Tool nicht installiert. Standard ist 1.
CLIENT_COMP	Zeigt an, ob PowerCenter Client installiert werden muss. Wenn der Wert 1 ist, wird PowerCenter Client installiert. Wenn der Wert 0 ist, wird PowerCenter Client nicht installiert. Standard ist 1.

5. Speichern Sie die Eigenschaftendatei.

Ausführen des Installationsprogramms

Öffnen Sie nach dem Konfigurieren der Eigenschaftendatei eine Eingabeaufforderung, um die automatische Installation zu starten.

1. Öffnen Sie die Eingabeaufforderung.
2. Wechseln Sie zum Root-Verzeichnis, das die Installationsdateien enthält.
3. Stellen Sie sicher, dass das Verzeichnis die Datei SilentInput.properties enthält, die Sie bearbeitet und erneut gespeichert haben.
4. Zum Ausführen der automatischen Installation führen Sie silentInstall.bat aus.

   Die automatische Installation wird im Hintergrund ausgeführt. Der Vorgang kann eine Weile dauern. Die automatische Installation ist abgeschlossen, wenn die Datei „Informatica_<Version>_Client_InstallLog<Zeitstempel>.log“ im Installationsverzeichnis erstellt ist.

   Die automatische Installation schlägt fehl, wenn die Eigenschaftendatei nicht ordnungsgemäß konfiguriert oder der Zugriff auf das Installationsverzeichnis nicht möglich ist. Zeigen Sie die Installationsprotokolldateien an und korrigieren Sie die Fehler. Führen Sie die automatische Installation anschließend noch einmal aus.

KAPITEL 14

Nach dem Installieren der Informatica-Clients

Dieses Kapitel umfasst die folgenden Themen:

- Installieren von Sprachen, 232
- Konfigurieren des Client für eine sichere Domäne, 232
- Konfigurieren des Workspace-Verzeichnisses für das Developer-Tool, 233

Installieren von Sprachen

Um andere Sprachen als diejenigen des Gebietsschemas anzuzeigen und um mit Repositorys zu arbeiten, die eine UTF-8-Codepage nutzen, müssen unter Windows weitere Sprachen für die Verwendung in Verbindung mit den Informatica-Clients installiert werden.

Außerdem müssen Sie Sprachen für die Verwendung des Windows Input Method Editor (IME) installieren.

1. Klicken Sie auf **Starten** > **Einstellungen** > **Systemsteuerung**.
2. Klicken Sie auf **Region und Sprache**.
3. Wählen Sie unter den Spracheinstellungen für das System die zu installierenden Sprachen aus.
4. Klicken Sie auf **Anwenden**.

Wenn Sie das Systemgebietsschema beim Installieren der Sprache ändern, starten Sie den Windows-Computer neu.

Konfigurieren des Client für eine sichere Domäne

Wenn Sie sichere Kommunikation innerhalb der Domäne aktivieren, sichern Sie auch Verbindungen zwischen der Domäne und Informatica-Client-Anwendungen, wie z. B. dem Developer Tool. Basierend auf den verwendeten TrustStore-Dateien müssen Sie möglicherweise den Speicherort und das Passwort für die TrustStore-Dateien in Umgebungsvariablen auf jedem Client-Host angeben.

Möglicherweise müssen Sie die folgenden Umgebungsvariablen auf jedem Client-Host festlegen:

INFA_TRUSTSTORE

Legen Sie diese Variable auf das Verzeichnis fest, das die Truststore-Dateien für die SSL-Zertifikate enthält. Das Verzeichnis muss Truststore-Dateien mit der Bezeichnung `infa_truststore.jks` und `infa_truststore.pem` enthalten.

INFA_TRUSTSTORE_PASSWORD

Legen Sie diese Variable auf das Passwort für die Datei `infa_truststore.jks` fest. Das Passwort muss verschlüsselt werden. Verwenden Sie das Befehlszeilenprogramm pmpasswd zum Verschlüsseln des Passworts.

Informatica stellt ein SSL-Zertifikat zur Verfügung, das Sie zum Sichern der Domäne verwenden können. Wenn Sie die Informatica-Clients installieren, legt das Installationsprogramm die Umgebungsvariablen fest und installiert die TrustStore-Dateien standardmäßig im folgenden Verzeichnis: `<Informatica-Installationsverzeichnis>\clients\shared\security`.

Wenn Sie das SSL-Standardzertifikat von Informatica verwenden und `infa_truststore.jks` und `infa_truststore.pem` sich im Standardverzeichnis befinden, brauchen Sie die Umgebungsvariablen INFA_TRUSTSTORE oder INFA_TRUSTSTORE_PASSWORD nicht festzulegen.

In den folgenden Szenarios müssen Sie die Umgebungsvariablen INFA_TRUSTSTORE und INFA_TRUSTSTORE_PASSWORD auf jedem Client-Host festlegen:

Sie verwenden ein benutzerdefiniertes SSL-Zertifikat zum Sichern der Domäne.

Wenn Sie ein SSL-Zertifikat bereitstellen, um die Domäne zu sichern, kopieren Sie die TrustStore-Dateien `infa_truststore.jks` und `infa_truststore.pem` auf jeden Client-Host. Sie müssen den Speicherort der Dateien und das TrustStore-Passwort angeben.

Sie verwenden das SSL-Standardzertifikat von Informatica, aber die TrustStore-Dateien befinden sich nicht im Informatica-Standardverzeichnis.

Wenn Sie das SSL-Standardzertifikat von Informatica verwenden, aber sich die TrustStore-Dateien `infa_truststore.jks` und `infa_truststore.pem` nicht im Informatica-Standardverzeichnis befinden, müssen Sie den Speicherort der Dateien und das TrustStore-Passwort angeben.

Konfigurieren des Workspace-Verzeichnisses für das Developer-Tool

Konfigurieren Sie Informatica Developer so, dass die Workspace-Metadaten in den Computer geschrieben werden, auf dem der Benutzer angemeldet ist.

1. Wechseln Sie zum folgenden Verzeichnis: `<Informatica-Installationsverzeichnis>\clients\DeveloperClient\configuration\`
2. Suchen Sie die Datei config.ini.
3. Erstellen Sie eine Sicherungskopie der Datei config.ini.
4. Öffnen Sie die Datei config.ini in einem Texteditor.
5. Fügen Sie die Variable `osgi.instance.area.default` an das Ende der Datei config.ini an, und stellen Sie die Variable auf den Verzeichnisort ein, wo Sie die Workspace-Metadaten speichern möchten. Der Dateipfad darf keine Nicht-ANSI-Zeichen enthalten. Ordnernamen im Workspace-Verzeichnis dürfen nicht

das Nummernzeichen (#) enthalten. Wenn Ordnernamen im Workspace-Verzeichnis Leerzeichen enthalten, umschließen Sie das gesamte Verzeichnis mit doppelten Anführungszeichen.

- Wenn Sie Informatica Developer vom lokalen Computer aus ausführen, stellen Sie die Variable auf den absoluten Pfad des Workspace-Verzeichnisses ein:

  ```
  osgi.instance.area.default=<Drive>/<WorkspaceDirectory>
  ```

  oder

  ```
  osgi.instance.area.default=<Drive>\\<WorkspaceDirectory>
  ```

- Wenn Sie Informatica Developer von einem Remote-Computer aus ausführen, stellen Sie die Variable auf den Verzeichnisort des lokalen Computers ein:

  ```
  osgi.instance.area.default=\\\\<LocalMachine>/<WorkspaceDirectory>
  ```

  oder

  ```
  osgi.instance.area.default=\\\\<LocalMachine>\\<WorkspaceDirectory>
  ```

  Der Benutzer muss über eine Schreibberechtigung für das Workspace-Verzeichnis verfügen.

Informatica Developer schreibt die Workspace-Metadaten in das Workspace-Verzeichnis. Wenn Sie sich in Informatica Developer von einem lokalen Computer aus anmelden, schreibt Informatica Developer die Workspace-Metadaten in den lokalen Computer. Wenn das Workspace-Verzeichnis nicht auf dem Computer existiert, auf dem Sie angemeldet sind, erstellt Informatica Developer das Verzeichnis beim Schreiben der Dateien.

Sie können das Workspace-Verzeichnis überschreiben, wenn Sie Informatica Developer starten.

KAPITEL 15

Starten der Informatica-Clients

Dieses Kapitel umfasst die folgenden Themen:

- Starten des Developer Tools, 235
- Starten von PowerCenter Client, 236
- Fehlerbehebung bei der Client-Installation, 236

Starten des Developer Tools

Beim Starten des Developer Tools wird eine Verbindung zu einem Model-Repository hergestellt. Im Model-Repository werden im Developer Tool erstellte Metadaten gespeichert. Der Model Repository Service verwaltet das Model Repository. Stellen Sie daher eine Verbindung zum Repository her, bevor Sie ein Projekt erstellen.

1. Klicken Sie im Windows-Startmenü auf **Programme** > **Informatica[Version]** > **Client** > **Developer Client** > **Informatica Developer starten**.

   Beim ersten Ausführen des Developer Tools wird die Begrüßungsseite mit mehreren Symbolen angezeigt. Beim nachfolgenden Ausführen des Developer Tools wird die Begrüßungsseite nicht mehr angezeigt.
2. Klicken Sie auf **Workbench.**

   Beim ersten Starten des Entwiocklertools müssen Sie das Repository auswählen, in dem die Objekte, die Sie erstellen, gespeichert werden sollen
3. Klicken Sie auf **Datei** > **Mit Repository verbinden**.

   Das Dialogfeld **Mit Repository verbinden** wird eingeblendet.
4. Wenn Sie im Developer Tool keine Domäne konfiguriert haben, klicken Sie auf **Domänen konfigurieren**, um eine Domäne zu konfigurieren.

   Sie müssen eine Domäne konfigurieren, um auf einen Model Repository Service zugreifen zu können.
5. Klicken Sie auf **Hinzufügen**, um eine Domäne hinzuzufügen.

   Das Dialogfeld **Neue Domäne** wird eingeblendet
6. Geben Sie den Domänennamen, den Hostnamen und die Portnummer ein.
7. Klicken Sie auf **Fertigstellen**.
8. Klicken Sie auf **OK**.
9. Klicken Sie im Dialogfeld **Mit Repository verbinden** auf **Durchsuchen** und wählen Sie den Model Repository Service aus.
10. Klicken Sie auf **OK**.

11. Klicken Sie auf **Weiter**.
12. Geben Sie einen Benutzernamen und ein Passwort ein.
13. Klicken Sie auf **Fertigstellen**.

    Das Model Repository wird der Objekt-Explorer-Ansicht hinzugefügt. Beim nächsten Ausführen des Developer-Tools können Sie eine Verbindung zum selben Repository herstellen.

Starten von PowerCenter Client

Beim Starten von PowerCenter Client wird eine Verbindung zu einem PowerCenter-Repository hergestellt.

1. Klicken Sie im Windows-Startmenü auf **Programme** > **Informatica[Version]** > **Client** > **[Name des Client-Tools]**.

   Beim ersten Ausführen eines PowerCenter Client-Tools müssen Sie ein Repository hinzufügen und eine Verbindung dazu herstellen
2. Klicken Sie auf **Repository** > **Repository hinzufügen**.

   Das Dialogfeld **Repository hinzufügen** wird angezeigt.
3. Geben Sie den Repository- und den Benutzernamen ein.
4. Klicken Sie auf **OK**.

   Das Repository wird im Navigator angezeigt.
5. Klicken Sie auf **Repository** > **Verbinden**.

   Das Dialogfeld für das Verbinden mit dem Repository wird angezeigt.
6. Klicken Sie im Abschnitt mit den Verbindungseinstellungen auf **Hinzufügen**, um die Informationen zur Domänenverbindung einzugeben.

   Das Dialogfeld **Domäne hinzufügen** wird angezeigt.
7. Geben Sie den Domänennamen, den Gateway-Host und die Gateway-Portnummer ein.
8. Klicken Sie auf **OK**.
9. Geben Sie in das Dialogfeld **Mit Repository verbinden** das Passwort für den Administrator-Benutzer ein.
10. Wählen Sie die Sicherheitsdomäne.
11. Klicken Sie auf **Verbinden**.

    Nachdem die Verbindung zum Repository hergestellt wurde, können Sie Objekte erstellen.

Fehlerbehebung bei der Client-Installation

Ich habe PowerCenter Client installiert, Mapping Architect für Visio wird jedoch nicht im Windows-Startmenü angezeigt und der Ordner MappingTemplate im Client-Verzeichnis ist leer.

Sie müssen über die richtige Version und das richtige Service Pack des Microsoft .NET Framework verfügen, damit Mapping Architect für Visio ordnungsgemäß installiert wird.

Deinstallieren Sie PowerCenter Client, installieren Sie die richtige Version des Microsoft .NET Framework und installieren Sie anschließend PowerCenter Client neu.

Teil VI: Deinstallation

- Deinstallation, 238

KAPITEL 16

Deinstallation

Dieses Kapitel umfasst die folgenden Themen:

- Deinstallation - Übersicht, 238
- Regeln und Richtlinien für die Deinstallation, 239
- Deinstallation von Informatica Server, 239
- Deinstallation der Informatica-Clients, 242

Deinstallation - Übersicht

Informatica deinstallieren, um den Server oder die Clients von Informatica aus einem Computer zu entfernen.

Der Informatica-Deinstallationsvorgang löscht alle Informatica-Dateien und alle Informatica-Konfigurationen aus einem Computer. Dateien, die nicht mit Informatica installiert wurden, werden bei der Deinstallation nicht gelöscht. Beispiel: Beim Installationsvorgang werden temporäre Verzeichnisse erstellt. Bei der Deinstallation werden keine Aufzeichnungen zu diesen Verzeichnissen aufbewahrt, daher können sie nicht gelöscht werden. Zur Vervollständigung der Deinstallation müssen Sie diese Verzeichnisse manuell löschen.

Beim Installieren des Informatica-Servers oder von Informatica-Clients erstellt das Installationsprogramm ein Deinstallationsprogramm. Das Deinstallationsprogramm ist im Deinstallationsverzeichnis gespeichert.

In der nachstehenden Tabelle sind die Deinstallationsverzeichnisse zu den jeweiligen Installationsarten aufgeführt.

Installation	Name des Deinstallationsverzeichnisses
Informatica-Server	`<Informatica-Installationsverzeichnis>/Uninstaller_Server`
Informatica-Clients	`<Informatica-Installationsverzeichnis>/Uninstaller_Client`

Um Informatica zu deinstallieren, verwenden Sie das während der Installation erstellte Deinstallationsprogramm. Deinstallieren Sie Informatica unter UNIX über die Befehlszeile. Deinstallieren Sie Informatica unter Windows über das Windows-Startmenü oder die Systemsteuerung.

Warnhinweis: Wenn Sie den PowerCenter Client und die Informatica-Dienste im selben Installationsverzeichnis installiert haben, werden die Programmdateien deinstalliert, wenn Sie den PowerCenter Client deinstallieren.

Regeln und Richtlinien für die Deinstallation

Halten Sie sich an die folgenden Regeln und Richtlinien, wenn Sie Informatica-Komponenten deinstallieren:

- Der Deinstallations-Modus von Informatica hängt von dem Modus ab, den Sie zum Installieren des Informatica-Servers verwendet haben. Wenn Sie den Informatica-Server beispielsweise im Konsolenmodus installiert haben, dann wird das Deinstallationsprogramm ebenfalls im Konsolenmodus ausgeführt. Der Deinstallations-Modus der Informatica-Clients hängt nicht von dem Modus ab, den Sie zum Installieren der Informatica-Clients verwendet haben. Wenn Sie die Informatica-Clients beispielsweise im automatischen Modus installiert haben, dann wird das Deinstallationsprogramm im Grafikmodus oder ebenfalls im automatischen Modus ausgeführt.
- Die Deinstallation von Informatica hat keine Auswirkungen auf die Informatica-Repositories. Das Deinstallationsprogramm entfernt die Informatica-Dateien. Es entfernt keine Repositories von der Datenbank. Wenn Sie die Repositories verschieben müssen, können Sie eine Sicherung von ihnen erstellen und sie dann in einer anderen Datenbank wiederherstellen.
- Bei der Deinstallation von Informatica werden die Metadatentabellen von der Domänen-Konfigurationsdatenbank nicht entfernt. Wenn Sie Informatica erneut mit der gleichen Domänen-Konfigurationsdatenbank und dem gleichen Benutzerkonto installieren, müssen Sie die Tabellen manuell entfernen oder sie überschreiben. Sie können den Befehl infasetup BackupDomain ausführen, um die Domänen-Konfigurationsdatenbank zu sichern, bevor Sie die Metadatentabellen überschreiben. Führen Sie den Befehl infasetup DeleteDomain vor dem Deinstallationsprogramm aus, um die Metadatentabellen manuell zu entfernen.
- Bei der Deinstallation von Informatica werden alle Installationsdateien und Unterverzeichnisse aus dem Informatica-Installationsverzeichnis entfernt. Bevor Sie Informatica deinstallieren, halten Sie alle Informatica-Dienste und -Prozesse an und stellen Sie sicher, dass alle Dateien im Installationsverzeichnis geschlossen sind. Am Ende des Deinstallationsvorgangs zeigt das Deinstallationsprogramm die Namen der Dateien und Verzeichnisse an, die nicht entfernt werden konnten.
- Bei der Installation des Informatica-Servers wird für Dateien und Bibliotheken, die von mithilfe der Informatica Developer Platform-APIs erstellten Drittanbieteradaptern benötigt werden, der folgende Ordner erstellt:
  `<Informatica-Installationsverzeichnis>/services/shared/extensions`

  Bei der Deinstallation des Informatica-Servers werden dieser Ordner und alle erstellten Unterordner gelöscht. Wenn Sie Adapter-Dateien in dem Ordner /extensions gespeichert haben, dann müssen Sie von dem Ordner eine Sicherung erstellen, bevor Sie mit der Deinstallation beginnen.
- Falls Sie die Deinstallation auf einem Windows-Rechner ausführen, auf dem die Dienste und Clients installiert sind, müssen Sie vor der Deinstallation den ODBC-Ordner sichern. Stellen Sie den Ordner nach Abschluss der Deinstallation wieder her.

Deinstallation von Informatica Server

Sie können den Informatica-Server unter Windows im Grafikmodus oder im automatischen Modus und unter UNIX im Konsolenmodus oder im automatischen Modus deinstallieren.

Deinstallation unter Windows

Sind die Informatica-Dienste und -Clients auf demselben Windows-Rechner installiert, nutzen Sie denselben ODBC-Ordner. Wenn Sie den Client oder den Server deinstallieren, wird zugleich auch der ODBC-Ordner entfernt.

1. Bevor Sie die Informatica-Dienste oder -Clients deinstallieren, kopieren Sie das ODBC-Verzeichnis in ein temporäres Verzeichnis auf Ihrem lokalen Laufwerk.

   Wenn Sie beispielsweise die Informatica-Dienste deinstallieren, kopieren Sie das Verzeichnis `<Informatica-Installationsverzeichnis>\ODBC<version>` und seine Inhalte in `C:\temp`.
2. Führen Sie die Deinstallation durch.
3. Nachdem Sie die Informatica-Dienste oder -Clients deinstalliert haben, erstellen Sie den ODBC-Verzeichnispfad neu.
4. Kopieren Sie das ODBC-Verzeichnis aus dem temporären Verzeichnis in das neu erstellte Verzeichnis.

   Wenn Sie beispielsweise die Informatica-Dienste deinstalliert haben, kopieren Sie den ODBC-Ordner und seine Inhalte in das Informatica-Installationsverzeichnis.

Deinstallieren des Informatica-Servers im Grafikmodus

Wenn Sie den Informatica-Server im Grafikmodus installiert haben, dann deinstallieren Sie den Informatica-Server ebenfalls im Grafikmodus.

Deinstallieren des Informatica-Servers unter Windows im Grafikmodus

Bevor Sie das Deinstallationsprogramm auszuführen, halten Sie alle Informatica-Dienste und -Prozesse an und stellen Sie sicher, dass alle Dateien im Installationsverzeichnis geschlossen sind. Der Deinstallationsvorgang kann keine Dateien löschen, die geöffnet sind oder von einem gerade ausgeführten Dienst oder Prozess verwendet werden.

1. Klicken Sie auf **Start** > **Programmdateien** > **Informatica [Version]** > **Server** > **Deinstallationsprogramm**.

   Die Seite **Deinstallation** wird angezeigt.
2. Klicken Sie auf**Deinstallieren**, um die Deinstallation zu beginnen.

   Nachdem das Installationsprogramm alle Informatica-Dateien aus dem Verzeichnis gelöscht hat, wird die Seite **Deinstallations-Zusammenfassung** angezeigt.
3. Klicken Sie auf **Fertig**, um das Deinstallationsprogramm zu schließen.

Nachdem Sie den Informatica-Server deinstalliert haben, löschen Sie alle übrigen Ordner und Dateien aus dem Informatica-Installationsverzeichnis. Beispiel:

- Datei Informatica _<Version>_Client_InstallLog.log
- Datei Informatica_<Version>_Client.log

Melden Sie sich vom Computer ab und wieder an. Löschen Sie danach die Informatica-spezifischen CLASSPATH und PATH-Umgebungsvariablen.

Deinstallieren des Informatica-Servers im Konsolenmodus

Wenn Sie den Informatica-Server im Konsolenmodus installiert haben, dann deinstallieren Sie den Informatica-Server ebenfalls im Konsolenmodus.

Deinstallieren des Informatica-Servers unter UNIX im Konsolenmodus

Bevor Sie das Deinstallationsprogramm auszuführen, halten Sie alle Informatica-Dienste und -Prozesse an und stellen Sie sicher, dass alle Dateien im Installationsverzeichnis geschlossen sind. Der Deinstallationsvorgang kann keine Dateien löschen, die geöffnet sind oder von einem gerade ausgeführten Dienst oder Prozess verwendet werden.

1. Gehen Sie zu folgendem Verzeichnis:

   ```
   <Informatica-Installationsverzeichnis>/Uninstaller_Server
   ```

2. Geben Sie den folgenden Befehl ein, um das Deinstallationsprogramm auszuführen:

   ```
   ./uninstaller
   ```

   Wenn Sie den Informatica-Server im Konsolenmodus installiert haben, dann startet das Deinstallationsprogramm ebenfalls im Konsolenmodus.

Deinstallieren des Informatica-Servers im automatischen Modus

Wenn Sie den Informatica-Server im automatischen Modus installiert haben, dann deinstallieren Sie den Informatica-Server ebenfalls im automatischen Modus.

Deinstallieren des Informatica-Servers unter UNIX im automatischen Modus

Bevor Sie das Deinstallationsprogramm auszuführen, halten Sie alle Informatica-Dienste und -Prozesse an und stellen Sie sicher, dass alle Dateien im Installationsverzeichnis geschlossen sind. Der Deinstallationsvorgang kann keine Dateien löschen, die geöffnet sind oder von einem gerade ausgeführten Dienst oder Prozess verwendet werden.

1. Gehen Sie zu folgendem Verzeichnis:

   ```
   <Informatica-Installationsverzeichnis>/Uninstaller_Server
   ```

2. Geben Sie den folgenden Befehl ein, um das automatische Deinstallationsprogramm auszuführen:

   ```
   ./uninstaller.sh
   ```

   Wenn Sie den Informatica-Server im automatischen Modus installiert haben, dann startet das Deinstallationsprogramm ebenfalls im automatischen Modus. Die automatische Deinstallation wird im Hintergrund ausgeführt. Der Vorgang kann eine Weile dauern. Die automatische Deinstallation schlägt fehl, wenn kein Zugriff auf das Installationsverzeichnis besteht.

Nachdem Sie den Informatica-Server deinstalliert haben, löschen Sie alle übrigen Ordner und Dateien aus dem Informatica-Installationsverzeichnis. Beispiel:

- Informatica _<Version>_Services_InstallLog.log-Datei
- Informatica_<Version>_Services_<timestamp>.log-Datei

Deinstallieren des Informatica-Servers unter Windows im automatischen Modus

Bevor Sie das Deinstallationsprogramm auszuführen, halten Sie alle Informatica-Dienste und -Prozesse an und stellen Sie sicher, dass alle Dateien im Installationsverzeichnis geschlossen sind. Der Deinstallationsvorgang kann keine Dateien löschen, die geöffnet sind oder von einem gerade ausgeführten Dienst oder Prozess verwendet werden.

1. Öffnen Sie die Eingabeaufforderung.
2. Gehen Sie zu folgendem Verzeichnis:

   ```
   <Informatica-Installationsverzeichnis>\Uninstaller_Server
   ```

3. Führen Sie die folgende Datei zum Ausführen der automatischen Deinstallation aus:

   `Uninstall.bat`

   Die automatische Deinstallation wird im Hintergrund ausgeführt. Der Vorgang kann eine Weile dauern. Die automatische Deinstallation schlägt fehl, wenn kein Zugriff auf das Installationsverzeichnis besteht.

Nachdem Sie den Informatica-Server deinstalliert haben, löschen Sie alle übrigen Ordner und Dateien aus dem Informatica-Installationsverzeichnis. Beispiel:

- Informatica _<Version>_Services_InstallLog.log-Datei
- Informatica_<Version>_Services_<timestamp>.log-Datei

Melden Sie sich vom Computer ab und wieder an. Löschen Sie danach die Informatica-spezifischen CLASSPATH und PATH-Umgebungsvariablen.

Deinstallation der Informatica-Clients

Sie können die Informatica-Clients im Grafikmodus und automatischen Modus unter Windows deinstallieren.

Wenn Sie Informatica-Clients deinstallieren, entfernt das Installationsprogramm nicht die INFA_TRUSTSTORE-Umgebungsvariablen, die während der Installation erstellt werden. Wenn Sie eine neuere Version von Informatica-Clients installieren, müssen Sie die Umgebungsvariable bearbeiten, um auf den neuen Wert des SSL-Zertifikats zu zeigen.

Weitere Informationen zum Festlegen der Truststore-Umgebungsvariablen finden Sie im Kapitel 14, “Nach dem Installieren der Informatica-Clients” auf Seite 232.

Deinstallation unter Windows

Sind die Informatica-Dienste und -Clients auf demselben Windows-Rechner installiert, nutzen Sie denselben ODBC-Ordner. Wenn Sie den Client oder den Server deinstallieren, wird zugleich auch der ODBC-Ordner entfernt.

1. Bevor Sie die Informatica-Dienste oder -Clients deinstallieren, kopieren Sie das ODBC-Verzeichnis in ein temporäres Verzeichnis auf Ihrem lokalen Laufwerk.

   Wenn Sie beispielsweise die Informatica-Dienste deinstallieren, kopieren Sie das Verzeichnis `<Informatica-Installationsverzeichnis>\ODBC<version>` und seine Inhalte in `C:\temp`.
2. Führen Sie die Deinstallation durch.
3. Nachdem Sie die Informatica-Dienste oder -Clients deinstalliert haben, erstellen Sie den ODBC-Verzeichnispfad neu.
4. Kopieren Sie das ODBC-Verzeichnis aus dem temporären Verzeichnis in das neu erstellte Verzeichnis.

   Wenn Sie beispielsweise die Informatica-Dienste deinstalliert haben, kopieren Sie den ODBC-Ordner und seine Inhalte in das Informatica-Installationsverzeichnis.

Deinstallieren von Informatica-Clients im Grafikmodus

Wenn Sie die Informatica-Clients im Grafikmodus installiert haben, deinstallieren Sie die Informatica-Clients ebenfalls im Grafikmodus.

Deinstallieren von Informatica-Clients im Grafikmodus

1. Klicken Sie auf **Start** > **Programmdateien** > **Informatica [Version]** > **Client** > **Deinstallationsprogramm**.

   Die Seite **Deinstallation** wird angezeigt.
2. Klicken Sie auf **Weiter**.

   Die Seite **Auswahl zur Deinstallation des Anwendungs-Clients** wird angezeigt.
3. Wählen Sie die gewünschten Client-Anwendungen aus und klicken Sie auf **Deinstallieren**.
4. Klicken Sie auf **Fertig**, um das Deinstallationsprogramm zu schließen.

   Nach abgeschlossener Deinstallation werden auf der Seite **Deinstallations-Zusammenfassung** die Ergebnisse der Deinstallation angezeigt.

Nachdem Sie die Informatica-Clients deinstalliert haben, löschen Sie alle übrigen Ordner und Dateien aus dem Informatica-Installationsverzeichnis. Beispiel:

- Datei Informatica _<Version>_Client_InstallLog.log
- Datei Informatica_<Version>_Client.log

Melden Sie sich vom Computer ab und wieder an. Löschen Sie danach die Informatica-spezifischen CLASSPATH und PATH-Umgebungsvariablen.

Deinstallieren von Informatica-Clients im automatischen Modus

Wenn Sie die Informatica-Clients im automatischen Modus installiert haben, deinstallieren Sie die Informatica-Clients ebenfalls im automatischen Modus.

Konfigurieren der Eigenschaftendatei

Informatica liefert eine Beispiel-Eigenschaftendatei, die die vom Installer benötigten Eigenschaften enthält.

Passen Sie die Beispiel-Eigenschaftendatei an, um eine Eigenschaftendatei zu erstellen, und legen Sie die Optionen für Ihre Deinstallation fest. Führen Sie anschließend die automatische Deinstallation aus.

1. Wechseln Sie zu dem Verzeichnis `<Informatica-Installationsverzeichnis>/Uninstaller_Client`.
2. Suchen Sie die Beispieldatei `SilentInput.properties`.
3. Erstellen Sie eine Sicherungskopie der SilentInput.properties-Datei.
4. Verwenden Sie einen Texteditor, um die Werte der Eigenschaftendatei zu öffnen und zu ändern.

   In der folgenden Tabelle werden die Eigenschaften beschrieben, die Sie ändern können:

Eigenschaftsname	Beschreibung
DXT_COMP	Zeigt an, ob Informatica Developer deinstalliert werden muss. Wenn der Wert 1 ist, wird das Developer-Tool deinstalliert. Wenn der Wert 0 ist, wird das Developer-Tool nicht deinstalliert. Standard ist 1.
CLIENT_COMP	Zeigt an, ob PowerCenter Client deinstalliert werden muss. Wenn der Wert 1 ist, wird PowerCenter Client deinstalliert. Wenn der Wert 0 ist, wird PowerCenter Client nicht deinstalliert. Standard ist 1.

5. Speichern Sie die Datei `SilentInput.properties`.

Automatisches Deinstallationsprogramm ausführen

Führen Sie nach dem Konfigurieren der Eigenschaftendatei die automatische Deinstallation aus.

1. Wechseln Sie zu dem Verzeichnis `<Informatica-Installationsverzeichnis>/Uninstaller_Client`.
2. Zum Ausführen der automatischen Installation doppelklicken Sie auf die Datei `uninstaller.bat` oder `uninstaller.exe`.

   Die automatische Deinstallation wird im Hintergrund ausgeführt. Der Vorgang kann eine Weile dauern. Die automatische Deinstallation schlägt fehl, wenn die Eigenschaftendatei nicht ordnungsgemäß konfiguriert oder der Zugriff auf das Installationsverzeichnis nicht möglich ist.

Nachdem Sie die Informatica-Clients deinstalliert haben, löschen Sie alle übrigen Ordner und Dateien aus dem Informatica-Installationsverzeichnis. Beispiel:

- Datei Informatica _<Version>_Client_InstallLog.log
- Datei Informatica_<Version>_Client.log

Melden Sie sich vom Computer ab und wieder an. Löschen Sie danach die Informatica-spezifischen CLASSPATH und PATH-Umgebungsvariablen.

ANHANG A

Starten und Anhalten der Informatica-Dienste

Dieser Anhang umfasst die folgenden Themen:

- Starten und Anhalten der Informatica-Dienste - Übersicht, 245
- Starten und Anhalten von Informatica unter UNIX, 246
- Starten und Anhalten von Informatica unter Windows, 246
- Konfigurieren des Informatica-Windows-Diensts, 247
- Beenden von Informatica in Informatica Administrator, 248
- Regeln und Richtlinien zum Starten oder Beenden von Informatica, 248

Starten und Anhalten der Informatica-Dienste - Übersicht

Auf jedem Knoten, auf dem Informatica installiert wird, wird ein Windows-Dienst oder ein UNIX-Dämon für das Ausführen von Informatica erstellt. Wenn der Installationsvorgang erfolgreich abgeschlossen wurde, wird der Informatica-Dienst unter Windows bzw. der Informatica-Dämon unter UNIX gestartet.

Der Informatica-Dienst führt den Service Manager auf dem Knoten aus. Der Dienstmanager erweitert alle Domänenfunktionen und startet Anwendungsdienste, die zum Ausführen auf dem Knoten konfiguriert sind. Die Methode zum Starten oder Beenden von Informatica hängt vom Betriebssystem ab. Sie können mit Informatica Administrator einen Knoten ausschalten. Bei Ausschalten eines Knotens wird Informatica auf diesem Knoten beendet.

Sie können das Verhalten des Informatica-Dienstes unter Windows konfigurieren.

Der Informatica-Dienst führt auch Informatica Administrator aus. Mit Informatica Administrator können Sie die Informatica-Domänenobjekte und -Benutzerkonten verwalten. Melden Sie sich bei Informatica Administrator an, um die Benutzerkonten für Informatica-Benutzer zu erstellen und die Anwendungsdienste in der Domäne zu erstellen und zu konfigurieren.

Starten und Anhalten von Informatica unter UNIX

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

```
<Informatica installation directory>/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.

Starten und Anhalten von Informatica unter Windows

Sie können die Informatica-Dienste über das Fenster „Dienste“ in der Systemsteuerung, über das Startmenü oder über eine Eingabeaufforderung starten bzw. anhalten.

Starten oder Anhalten von Informatica über das Startmenü

Klicken Sie zum Starten von Informatica über das Windows-Startmenü auf **Programme** > **Informatica[Version]** > **Server**. Klicken Sie mit der rechten Maustaste auf **Informatica-Dienste starten** und wählen Sie **Als Administrator ausführen** aus.

Klicken Sie zum Anhalten von Informatica über das Windows-Startmenü auf **Programme** > **Informatica[Version]** > **Server**. Klicken Sie mit der rechten Maustaste auf **Informatica-Dienste anhalten**, und wählen Sie **Als Administrator ausführen** aus.

Starten oder Beenden von Informatica über die Systemsteuerung

Das Verfahren zum Starten oder Beenden des Informatica Windows-Dienstes ist das gleiche wie für alle anderen Windows-Dienste.

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

Starten bzw. Anhalten von Informatica über eine Eingabeaufforderung

Sie können „infaservice.bat“ aus der Befehlszeile zum Starten und Anhalten von Informatica-Diensten unter Windows ausführen.

infaservice.bat ist standardmäßig im folgenden Verzeichnis installiert:

```
<Informatica-Installationsverzeichnis>\tomcat\bin
```

1. Öffnen Sie eine Eingabeaufforderung als Administrator.
2. Gehen Sie zu dem Verzeichnis, in dem sich infaservice.bat befindet.
3. Geben Sie den folgenden Befehl zum Starten der Informatica-Dienste ein:

   ```
   infaservice.bat startup
   ```

   Geben Sie den folgenden Befehl zum Anhalten der Informatica-Dienste ein:

   ```
   infaservice.bat shutdown
   ```

Konfigurieren des Informatica-Windows-Diensts

Sie können das Verhalten des Informatica-Windows-Diensts beim Start des Betriebssystems oder beim Fehlschlagen des Diensts konfigurieren. Außerdem können Sie das Benutzerkonto konfigurieren, mit dem die Anmeldung beim Dienst erfolgt.

Regeln und Richtlinien für das Benutzerkonto

Beachten Sie beim Konfigurieren des Benutzerkontos, mit dem die Anmeldung beim Dienst erfolgt, die folgenden Richtlinien:

- Wenn Sie Dateien auf einem Netzlaufwerk speichern, verwenden Sie zum Ausführen des Informatica-Dienstes ein Systemkonto anstatt eines lokalen Systemkontos.
- Wenn Sie die gemeinsame Speichernutzung auf einem Netzlaufwerk zum Speichern von Dateien, die von der Domäne oder darin ausgeführten Anwendungsdiensten verwendet werden, konfigurieren, muss das Benutzerkonto, über das der Informatica-Dienst ausgeführt wird, über Zugriff auf den gemeinsamen Speicherort verfügen.
- Wenn Sie das lokale Systemkonto verwenden möchten, stellen Sie sicher, dass der Benutzer, der den Informatica-Dienst startet, auf den Netzwerkspeicherort zugreifen kann.
- Wenn der Benutzer, der den Informatica-Dienst startet, nicht auf den gemeinsamen Netzwerkspeicherort zugreifen kann, schlagen die Dienstprozesse auf dem Knoten fehl oder der Knoten oder die Domäne wird nicht gestartet.
- Wenn Sie ein Systembenutzerkonto konfigurieren, muss dieses über die Berechtigung *Als Betriebssystem fungieren* verfügen. Weitere Informationen erhalten Sie in der Windows-Dokumentation.

Konfigurieren des Informatica-Windows-Diensts

Verwenden Sie die Windows-Systemsteuerung zum Konfigurieren des Benutzerkontos, das sich beim Informatica Windows-Dienst anmeldet, und zum Konfigurieren der Neustartoptionen des Diensts.

1. Öffnen Sie die Windows-Systemsteuerung.

2. Wählen Sie **Verwaltung**.
3. Wählen Sie **Dienste**.
4. Doppelklicken Sie auf Informatica <Version>.

   Das Dialogfeld **Eigenschaften von Informatica <Version>** wird angezeigt.
5. Klicken Sie auf die Registerkarte **Anmelden**.
6. Wählen Sie **Dieses Konto**.
7. Geben Sie den Domänen- und den Benutzernamen ein oder klicken Sie auf **Durchsuchen**, um einen Systembenutzer zu suchen.
8. Geben Sie das Passwort für das ausgewählte Benutzerkonto ein und bestätigen Sie es.
9. Klicken Sie auf die Registerkarte **Wiederherstellung**. Wählen Sie die Optionen für den Neustart des Informatica-Diensts aus, falls der Dienst fehlschlägt.

Weitere Informationen zum Konfigurieren von Systemkonten für Dienste und zu Optionen für den Neustart von Diensten unter Windows finden Sie in der Windows-Dokumentation.

Beenden von Informatica in Informatica Administrator

Wenn Sie mithilfe von Informatica Administrator einen Knoten ausschalten, wird der Informatica-Dienst auf diesem Knoten beendet.

Sie können die laufenden Vorgänge abbrechen oder zum Abschluss bringen, bevor der Dienst geschlossen wird. Wenn Sie einen Knoten ausschalten und die Repository Service-Prozesse abbrechen, die auf dem Knoten ausgeführt werden, können Änderungen verloren gehen, die noch nicht in das Repository geschrieben wurden. Wenn Sie einen Knoten ausschalten, auf dem Integrations-Dienstvorgänge ausgeführt werden, werden die Arbeitsabläufe abgebrochen.

1. Melden Sie sich bei Informatica Administrator an.
2. Wählen Sie den zu schließenden Knoten im Navigator aus.
3. Klicken Sie auf der Registerkarte "Domäne" im Menü **Aktionen** auf **Knoten schließen**.

Regeln und Richtlinien zum Starten oder Beenden von Informatica

Beachten Sie beim Starten und Beenden von Informatica auf einem Knoten die folgenden Richtlinien:

- Wenn ein Knoten ausgeschaltet wird, ist dieser für die Domäne nicht verfügbar. Wenn ein Gateway-Knoten ausgeschaltet wird und es keinen anderen Gateway-Knoten in der Domäne gibt, ist die Domäne nicht verfügbar.
- Überprüfen Sie beim Starten von Informatica, ob der vom Dienst auf dem Knoten verwendete Port verfügbar ist. Beispiel: Wenn Sie Informatica auf einem Knoten beenden, vergewissern Sie sich vor dem Neustart, dass der Port von keinem anderen Prozess auf dem Rechner verwendet wird. Wenn der Port nicht verfügbar ist, schlägt der Start von Informatica fehl.

- Wenn Sie einen Knoten nicht mithilfe von Informatica Administrator ausschalten, werden auf dem Knoten ausgeführte Prozesse abgebrochen. Wenn Sie vor dem Ausschalten eines Knotens warten möchten, bis alle Prozesse abgeschlossen sind, verwenden Sie Informatica Administrator.
- Wenn es zwei Knoten in einer Domäne gibt, von denen einer als Primärknoten für einen Anwendungsdienst und der andere als Sicherungsknoten konfiguriert ist, starten Sie Informatica auf dem Primärknoten, bevor Sie den Sicherungsknoten starten. Andernfalls wird der Anwendungsdienst auf dem Sicherungsknoten, nicht auf dem Primärknoten ausgeführt.

ANHANG B

Verbinden zu Datenbanken unter Windows

Dieser Anhang umfasst die folgenden Themen:

- Verbinden zu Datenbanken unter Windows - Übersicht, 250
- Verbinden zu einer IBM DB2 Universal-Datenbank unter Windows, 251
- Herstellen einer Verbindung zu einer Informix-Datenbank unter Windows, 252
- Verbinden mit Microsoft Access und Microsoft Excel unter Windows, 252
- Verbinden mit einer Microsoft SQL Server-Datenbank von Windows aus, 253
- Verbinden zu einer Netezza-Datenbank unter Windows, 254
- Herstellen einer Verbindung zu einer Oracle-Datenbank unter Windows, 255
- Verbinden zu einer Sybase ASE-Datenbank unter Windows, 257
- Herstellen einer Verbindung zu einer Teradata-Datenbank über Windows, 258

Verbinden zu Datenbanken unter Windows - Übersicht

Konfigurieren Sie die Konnektivität, um die Kommunikation zwischen Clients, Diensten und anderen Komponenten in der Domäne zu aktivieren.

Zur Verwendung der nativen Konnektivität müssen Sie die Datenbank-Client-Software für die Datenbank, auf die Sie zugreifen möchten, installieren und konfigurieren. Um die Kompatibilität zwischen dem Anwendungsdienst und der Datenbank zu gewährleisten, installieren Sie eine Client-Software, die mit der Datenbankversion kompatibel ist, und verwenden Sie die entsprechenden Bibliotheken des Datenbank-Client. Um die Leistung zu erhöhen, verwenden Sie native Konnektivität.

Die Informatica-Installation enthält DataDirect-ODBC-Treiber. Wenn ODBC-Datenquellen bereits mit früheren Versionen der Treiber erstellt wurden, müssen Sie mit den neuen Treibern neue ODBC-Datenquellen erstellen. Konfigurieren Sie die ODBC-Verbindungen mithilfe der von Informatica mitgelieferten DataDirect-ODBC-Treiber oder mit ODBC-Treibern von Drittanbietern, die mit Level 2 oder höher kompatibel sind.

Die Informatica-Installation umfasst DataDirect JDBC-Treiber. Sie können diese Treiber ohne zusätzliche Schritte verwenden. Sie können auch JDBC-Treiber des Typs 4 von Drittanbietern herunterladen, um eine Verbindung zu Quellen und Zielen herzustellen. Sie können jeden beliebigen JDBC-Treiber mit JDBC 3.0 oder höher verwenden.

Sie müssen eine Datenbankverbindung für die folgenden Dienste in der Informatica-Domäne konfigurieren:

- PowerCenter-Repository-Dienst
- Modellrepository-Dienst
- Datenintegrationsdienst
- Analyst-Dienst

Verbinden zu einer IBM DB2 Universal-Datenbank unter Windows

Installieren Sie für eine native Konnektivität die Version von IBM DB2 Client Application Enabler (CAE), die für die IBM DB2-Datenbankserverversion geeignet ist. Verwenden Sie zur Gewährleistung der Kompatibilität zwischen Informatica und den Datenbanken die entsprechenden Datenbank-Client-Bibliotheken.

Konfigurieren der nativen Konnektivität

Sie können native Konnektivität für eine IBM DB2-Datenbank konfigurieren, um die Leistung zu erhöhen.

Die folgenden Schritte stellen eine Richtlinie zum Konfigurieren der nativen Konnektivität dar. Spezifische Anweisungen finden Sie in der Dokumentation zur Datenbank.

1. Überprüfen Sie, ob von IBM DB2 Client Application Enabler (CAE) die folgenden Einstellungen zu Umgebungsvariablen vorgenommen wurden:

   ```
   DB2HOME=C:\IBM\SQLLIB
   DB2INSTANCE=DB2
   DB2CODEPAGE=1208 (Sometimes required. Use only if you encounter problems. Depends on
   the locale, you may use other values.)
   ```

2. Überprüfen Sie, ob die Umgebungsvariable PATH das IBM DB2-bin-Verzeichnis enthält. Beispiel:

   ```
   PATH=C:\WINNT\SYSTEM32;C:\SQLLIB\BIN;...
   ```

3. Konfigurieren Sie den IBM DB2-Client so, dass eine Verbindung zur gewünschten Datenbank hergestellt wird. Konfigurieren des IBM DB2-Clients:

   a. Starten Sie den IBM DB2-Konfigurationsassistenten.

   b. Fügen Sie die Datenbankverbindung hinzu.

   c. Erstellen Sie eine Bindung an die Verbindung.

4. Führen Sie den folgenden Befehl im IBM DB2-Befehlszeilenprozessor aus, um sicherzustellen, dass eine Verbindung zur IBM DB2-Datenbank hergestellt werden kann:

   ```
   CONNECT TO <dbalias> USER <username> USING <password>
   ```

5. Wenn die Verbindung erfolgreich ist, führen Sie den Befehl TERMINATE aus, um die Verbindung zur Datenbank zu trennen. Falls die Verbindung fehlschlägt, ziehen Sie die Dokumentation zur Datenbank hinzu.

Herstellen einer Verbindung zu einer Informix-Datenbank unter Windows

Verwenden Sie ODBC zum Herstellen einer Verbindung zu einer Informix-Datenbank unter Windows. Erstellen Sie mithilfe des mit Informatica installierten DataDirect-ODBC-Treibers eine ODBC-Datenquelle. Verwenden Sie zur Gewährleistung der Kompatibilität zwischen Informatica und den Datenbanken die entsprechenden Datenbank-Client-Bibliotheken.

Hinweis: Bei Verwendung des von Informatica mitgelieferten DataDirect-ODBC-Treibers wird der Datenbank-Client nicht benötigt. Die ODBC-Drahtprotokolle benötigen die Datenbank-Client-Software nicht, um eine Verbindung zur Datenbank herzustellen.

Konfigurieren der ODBC-Konnektivität

Sie können ODBC-Konnektivität für eine Informix-Datenbank konfigurieren.

Die folgenden Schritte enthalten eine Richtlinie zum Konfigurieren der ODBC-Konnektivität. Spezifische Anweisungen finden Sie in der Dokumentation zur Datenbank.

1. Erstellen Sie eine ODBC-Datenquelle mithilfe des Treibers DataDirect ODBC Wire Protocol Treiber für Informix von Informatica.
2. Stellen Sie sicher, dass Sie mithilfe der ODBC-Datenquelle eine Verbindung zur Informix-Datenbank herstellen können.

Verbinden mit Microsoft Access und Microsoft Excel unter Windows

Konfigurieren Sie die Konnektivität zu den folgenden Informatica-Komponenten unter Windows.

Installieren Sie Microsoft Access oder Excel auf dem Computer, auf dem die Datenintegrationsdienst- und PowerCenter-Integrationsdienst-Prozesse ausgeführt werden. Erstellen Sie eine ODBC-Datenquelle für die Microsoft Access- oder Excel-Daten, auf die Sie zugreifen möchten.

Konfigurieren der ODBC-Konnektivität

Sie können ODBC-Konnektivität zu einer Microsoft Access- oder Excel-Datenbank konfigurieren.

Die folgenden Schritte enthalten eine Richtlinie zum Konfigurieren der ODBC-Konnektivität. Spezifische Anweisungen finden Sie in der Dokumentation zur Datenbank.

1. Erstellen Sie mithilfe des von Microsoft bereitgestellten Treibers eine ODBC-Datenquelle.
2. Damit keine leeren Zeichenfolgen oder Nullen verwendet werden, verwenden Sie bei der Herstellung einer Datenbankverbindung im Workflow Manager die reservierten Wörter PmNullUser für den Benutzernamen und PmNullPasswd für das Passwort.

Verbinden mit einer Microsoft SQL Server-Datenbank von Windows aus

In Informatica 10.0 können Sie mithilfe der ODBC-Datenquelle standardmäßig eine Verbindung zur Microsoft SQL Server-Datenbank aufbauen.

Sie können die Verbindung zur Microsoft SQL Server-Datenbank auch über einen Provider vom Typ OLEDB herstellen, allerdings ist dieser Provider veraltet. Die Unterstützung des Providertyps OLEDB wird in einer der zukünftigen Versionen aufgehoben.

Konfigurieren der nativen Konnektivität

In Informatica 10.0 können Sie mit dem Providertyp ODBC (Standard) oder OLEDB (veraltet) native Konnektivität zur Microsoft SQL Server-Datenbank konfigurieren.

Wenn Sie den Providertyp ODBC auswählen, können Sie die Option „DSN verwenden“ aktivieren, um den im Microsoft ODBC-Administrator konfigurierten DSN als Verbindungszeichenfolge zu verwenden. Falls Sie die Option „DSN verwenden“ nicht aktivieren, müssen Sie den Servernamen und den Datenbanknamen in den Verbindungseigenschaften angeben.

Wenn Sie den Providertyp OLEDB auswählen, müssen Sie Microsoft SQL Server 2012 Native Client installieren, um native Konnektivität zur Microsoft SQL Server-Datenbank zu konfigurieren. Wenn Sie keine Verbindung zu der Datenbank herstellen können, vergewissern Sie sich, dass Sie alle Konnektivitätsinformationen korrekt eingegeben haben.

Sie können Microsoft SQL Server 2012 Native Client von folgender Microsoft-Website herunterladen: http://www.microsoft.com/en-in/download/details.aspx?id=29065.

Nach dem Upgrade wird die Microsoft SQL Server-Verbindung standardmäßig auf den Providertyp OLEDB festgelegt. Es wird empfohlen, zur Verwendung des Providertyps ODBC alle Microsoft SQL Server-Verbindungen zu aktualisieren. Mithilfe der folgenden Befehle können Sie alle Ihre Microsoft SQL Server-Verbindungen auf den Providertyp ODBC aktualisieren:

- Wenn Sie PowerCenter verwenden, führen Sie den folgenden Befehl aus: pmrep upgradeSqlServerConnection
- Wenn Sie die Informatica-Plattform verwenden, führen Sie den folgenden Befehl aus: infacmd.sh isp upgradeSQLSConnection

Spezifische Anweisungen zur Konnektivität finden Sie in der Dokumentation zur Datenbank.

Regeln und Richtlinien für Microsoft SQL Server

Berücksichtigen Sie beim Konfigurieren der ODBC-Konnektivität zu einer Microsoft SQL Server-Datenbank die folgenden Regeln und Richtlinien:

- Falls Sie eine Microsoft SQL Server-Verbindung ohne Verwendung eines Datenquellennamens (Verbindung ohne DSN) nutzen möchten, müssen Sie die Umgebungsvariable „odbcinst.ini“ konfigurieren.
- Bei Verwendung einer DSN-Verbindung müssen Sie dem ODBC-DSN den Eintrag „EnableQuotedIdentifiers=1“ hinzufügen. Wenn Sie den Eintrag nicht hinzufügen, schlägt die Ausführung der Datenvorschau und des Mappings fehl.
- Sie können die NTLM-Authentifizierung von Microsoft SQL Server für eine Microsoft SQL Server-Verbindung ohne DSN auf der Microsoft Windows-Plattform verwenden.

- Wenn die Microsoft SQL Server-Tabelle einen UUID-Datentyp enthält und Sie Daten aus einer SQL-Tabelle lesen sowie Daten in eine Einfachdatei schreiben, ist das Datenformat zwischen den OLEDB- und ODBC-Verbindungstypen möglicherweise nicht konsistent.
- Für eine Verbindung ohne DSN können Sie keine SSL-Verbindung verwenden. Zur Nutzung von SSL müssen Sie die DSN-Verbindung verwenden. Aktivieren Sie die Option „DSN verwenden“ und konfigurieren Sie die SSL-Optionen in der Datei „odbc.ini“.
- Falls Microsoft SQL Server die Kerberos-Authentifizierung verwendet, müssen Sie die Eigenschaft „GSSClient“ festlegen, um auf die Kerberos-Bibliotheken von Informatica zu verweisen. Verwenden Sie den folgenden Pfad und Dateinamen: `<Informatica-Installationsverzeichnis>/server/bin/libgssapi_krb5.so.2`. Erstellen Sie für eine DSN-Verbindung in `odbc.ini` im Abschnitt für DSN-Einträge einen Eintrag für die Eigenschaft „GSSClient“ bzw. für eine Verbindung, bei der kein DSN verwendet wird, einen Eintrag in `odbcinst.ini` im Abschnitt für SQL Server Wire Protocol.

Konfigurieren von benutzerdefinierten Eigenschaften für Microsoft SQL Server

Zur Verbesserung der Bulk Load-Leistung können Sie benutzerdefinierte Eigenschaften für Microsoft SQL Server konfigurieren.

1. Starten Sie den PowerCenter-Client und stellen Sie eine Verbindung zum Workflow Manager her.
2. Öffnen Sie einen Arbeitsablauf und wählen Sie eine Sitzung aus, die Sie konfigurieren möchten.
3. Klicken Sie auf die Registerkarte **Konfig-Objekt**.
4. Ändern Sie den Wert der **Standard-Pufferblockgröße** in 5 MB. Sie können auch den folgenden Befehl verwenden: `$INFA_HOME/server/bin/./pmrep massupdate -t session_config_property -n "Default buffer block size" -v "5MB" -f $<folderName>`

   Wenn Sie für eine Zeilengröße von 1 KB einen optimalen Durchsatz erzielen möchten, müssen Sie die Pufferblockgröße auf 5 MB festlegen.
5. Klicken Sie auf die Registerkarte **Eigenschaften**.
6. Ändern Sie das **Commit-Intervall** in 100000, falls die Sitzung ein relationales Ziel enthält.
7. Legen Sie die **DTM-Puffergröße** fest. Die optimale DTM-Puffergröße ist ((10 x Pufferblockgröße) x Anzahl der Partitionen).

Verbinden zu einer Netezza-Datenbank unter Windows

Installieren und konfigurieren Sie ODBC auf den Computern, auf denen der PowerCenter-Integrationsdienst-Prozess ausgeführt wird und auf denen PowerCenter Client installiert wird. Sie müssen die Konnektivität zu folgenden Informatica-Komponenten unter Windows konfigurieren:

- **PowerCenter Integration Service** Installieren Sie den Netezza ODBC-Treiber auf dem Rechner, auf dem die PowerCenter Integration Service-Vorgänge ausgeführt werden. Verwenden Sie den Microsoft ODBC-Datenquellen-Administrator zum Konfigurieren der ODBC-Konnektivität.
- **PowerCenter Client.** Installieren Sie den ODBC-Treiber von Netezza auf jedem PowerCenter Client-Computer, der auf die Netezza-Datenbank zugreift. Verwenden Sie den Microsoft ODBC-Datenquellen-Administrator zum Konfigurieren der ODBC-Konnektivität. Verwenden Sie den Workflow Manager zum Erstellen eines Datenbankverbindungsobjekts für die Netezza-Datenbank.

Konfigurieren der ODBC-Konnektivität

Sie können ODBC-Konnektivität für eine Netezza-Datenbank konfigurieren.

Die folgenden Schritte enthalten eine Richtlinie zum Konfigurieren der ODBC-Konnektivität. Spezifische Anweisungen finden Sie in der Dokumentation zur Datenbank.

1. Erstellen Sie eine ODBC-Datenquelle für jede Netezza-Datenbank, auf die Sie zugreifen möchten.

   Erstellen Sie mithilfe des von Netezza bereitgestellten Treibers die ODBC-Datenquelle.

   Erstellen Sie einen System-DSN, wenn Sie den Informatica-Dienst mit einer Lokalen Systemkonto-Anmeldung starten. Erstellen Sie einen Benutzer-DSN, wenn Sie zum Starten des Informatica-Dienstes die Anmeldeoption "Dieses Konto" wählen.

   Konfigurieren Sie nach dem Erstellen der Datenquelle deren Eigenschaften.
2. Geben sie einen Namen für die neue ODBC-Datenquelle ein.
3. Geben Sie die IP-Adresse/den Hostnamen und die Portnummer für den Netezza-Server ein.
4. Geben Sie den Namen des Netezza-Schemas ein, in dem Sie Datenbankobjekte erstellen möchten.
5. Konfigurieren Sie den Pfad und den Dateinamen für die ODBC-Protokolldatei.
6. Überprüfen Sie, ob Sie eine Verbindung zur Netezza-Datenbank herstellen können.

   Sie können die Datenbankverbindung mit dem Microsoft ODBC-Datenquellen-Administrator testen. Zum Testen der Verbindung wählen Sie die Netezza-Datenquelle aus und klicken auf "Konfigurieren". Klicken Sie in der Registerkarte "Testen" auf "Verbindung testen" und geben Sie die Verbindungsdaten für das Netezza-Schema ein.

Herstellen einer Verbindung zu einer Oracle-Datenbank unter Windows

Installieren Sie für eine native Konnektivität die für die Oracle-Datenbankserverversion geeignete Version des Oracle-Client. Verwenden Sie zur Gewährleistung der Kompatibilität zwischen Informatica und den Datenbanken die entsprechenden Datenbank-Client-Bibliotheken.

Sie müssen kompatible Versionen des Oracle-Client und des Oracle-Datenbankservers installieren. Des Weiteren müssen Sie dieselbe Version des Oracle-Client auf allen Rechnern installieren, die ihn benötigen. Informationen zur Überprüfung der Kompatibilität erhalten Sie von Oracle.

Konfigurieren der nativen Konnektivität

Sie können native Konnektivität für eine Oracle-Datenbank konfigurieren, um die Leistung zu erhöhen.

Die folgenden Schritte stellen eine Richtlinie zum Konfigurieren der nativen Konnektivität mithilfe von Oracle Net Services oder Net8 dar. Spezifische Anweisungen zur Konnektivität finden Sie in der Dokumentation zur Datenbank.

1. Vergewissern Sie sich, dass das Basisverzeichnis von Oracle eingerichtet ist.

   Beispiel:

   ```
   ORACLE_HOME=C:\Oracle
   ```
2. Überprüfen Sie, ob die Umgebungsvariable PATH das Oracle-bin-Verzeichnis enthält.

Wenn Sie beispielsweise Net8 installieren, kann der Pfad den folgenden Eintrag enthalten:

```
PATH=C:\ORANT\BIN;
```

3. Konfigurieren Sie den Oracle-Client so, dass eine Verbindung zur gewünschten Datenbank hergestellt wird.

   Starten Sie das Dienstprogramm SQL*Net Easy Configuration oder bearbeiten Sie eine vorhandene `tnsnames.ora`-Datei im Basisverzeichnis und ändern Sie sie.

   Hinweis: Standardmäßig wird die Datei `tnsnames.ora` in folgendem Verzeichnis gespeichert: `<OracleInstallationDir>\network\admin`.

   Geben Sie die richtige Syntax für die Oracle-Verbindungszeichenfolge ein. Diese lautet normalerweise `databasename.world`. Vergewissern Sie sich, dass die eingegebene SID mit der auf dem Oracle-Server definierten ID der Datenbankserverinstanz übereinstimmt.

   Hier ist eine `tnsnames.ora`-Beispieldatei. Geben Sie die Informationen für die Datenbank ein.

```
mydatabase.world =
   (DESCRIPTION
   (ADDRESS_LIST =
        (ADDRESS =
           (COMMUNITY = mycompany.world
           (PROTOCOL = TCP)
           (Host = mymachine)
           (Port = 1521)
        )
   )
   (CONNECT_DATA =
      (SID = MYORA7)
      (GLOBAL_NAMES = mydatabase.world)
```

4. Stellen Sie die Umgebungsvariable NLS_LANG auf das Gebietsschema (Sprache, Region und Zeichensatz) ein, das der Datenbank-Client und -Server bei der Anmeldung verwenden sollen.

   Der Wert dieser Variable hängt von der Konfiguration ab. Lautet der Wert beispielsweise american_america.UTF8, müssen Sie die Variable folgendermaßen einstellen:

```
NLS_LANG=american_america.UTF8;
```

   Setzen Sie sich mit dem Datenbankadministrator in Verbindung, um den Wert dieser Variable zu bestimmen.

5. Geben Sie zum Einrichten der Zeitzone einer Standardsitzung die Umgebungsvariable ORA_SDTZ an, wenn der Datenintegrationsdienst Daten vom Typ „Zeitstempel mit lokaler Zeitzone“ liest oder schreibt.

   Sie können die Umgebungsvariable ORA_SDTZ auf einen der folgenden Werte festlegen:

   - Lokale Zeitzone des Betriebssystems ('OS_TZ')
   - Zeitzone der Datenbank ('DB_TZ')
   - Absoluter Versatz von UTC (z. B. '-05:00')
   - Name der Zeitzonenregion (z. B. 'America/Los_Angeles')

   Sie können die Umgebungsvariable auf dem Computer festlegen, auf dem der Informatica-Server ausgeführt wird.

6. Wenn sich die Datei tnsnames.ora nicht in demselben Speicherort wie das Oracle-Installationsverzeichnis befindet, legen Sie die TNS_ADMIN-Umgebungsvariable tnsnames.ora für das Verzeichnis fest, in dem sich die Datei tnsnames.ora befindet.

   Wenn sich die Datei tnsnames.ora beispielsweise im Verzeichnis C:\oracle\files befindet, legen Sie die Variable wie folgt fest:

```
TNS_ADMIN= C:\oracle\files
```

7. Vergewissern Sie sich, dass Sie eine Verbindung zu der Oracle-Datenbank herstellen können.

   Zum Herstellen der Verbindung zur Datenbank starten Sie SQL*Plus und geben die Konnektivitätsinformationen ein. Wenn Sie keine Verbindung zu der Datenbank herstellen können, vergewissern Sie sich, dass Sie alle Konnektivitätsinformationen korrekt eingegeben haben.

   Verwenden Sie die in der `tnsnames.ora`-Datei definierte Verbindungszeichenfolge.

Verbinden zu einer Sybase ASE-Datenbank unter Windows

Installieren Sie für eine native Konnektivität die für Ihre Datenbankversion geeignete Version von Open Client. Verwenden Sie zur Gewährleistung der Kompatibilität zwischen Informatica und den Datenbanken die entsprechenden Datenbank-Client-Bibliotheken.

Installieren Sie eine mit dem Sybase ASE-Datenbankserver kompatible Version von Open Client Sie müssen dieselbe Version von Open Client auf den Rechnern installieren, auf denen sich die Sybase ASE-Datenbank und Informatica befinden. Informationen zur Überprüfung der Kompatibilität erhalten Sie von Sybase.

Wenn Sie ein Sybase ASE-Repository erstellen, wiederherstellen oder upgraden möchten, setzen Sie *Nullen standardmäßig zulassen* auf der Datenbankebene auf TRUE Hiermit wird der Standard-Nulltyp der Spalte entsprechend dem SQL-Standard in Null geändert.

Konfigurieren der nativen Konnektivität

Sie können native Konnektivität für eine Sybase ASE-Datenbank konfigurieren, um die Leistung zu erhöhen.

Die folgenden Schritte stellen eine Richtlinie zum Konfigurieren der nativen Konnektivität dar. Spezifische Anweisungen finden Sie in der Dokumentation zur Datenbank.

1. Überprüfen Sie, ob die Umgebungsvariable SYBASE auf das Sybase ASE-Verzeichnis verweist.

   Beispiel:

   ```
   SYBASE=C:\SYBASE
   ```

2. Überprüfen Sie, ob die Umgebungsvariable PATH das Sybase ASE-Verzeichnis enthält.

   Beispiel:

   ```
   PATH=C:\SYBASE\OCS-15_0\BIN;C:\SYBASE\OCS-15_0\DLL
   ```

3. Konfigurieren Sie Sybase Open Client so, dass eine Verbindung zur gewünschten Datenbank hergestellt wird.

   Verwenden Sie SQLEDIT zum Konfigurieren des Sybase-Client oder kopieren Sie eine vorhandene SQL.INI-Datei (im Verzeichnis %SYBASE%\INI) und nehmen Sie etwaige erforderliche Änderungen vor.

   Wählen Sie NLWNSCK als Net-Library-Treiber und schließen Sie den Sybase ASE-Servernanem ein.

   Geben Sie Hostnamen und Portnummer für den Sybase ASE-Server ein. Wenn Ihnen Hostname und Portnummer nicht bekannt sind, wenden Sie sich an den Systemadministrator.

4. Stellen Sie sicher, dass Sie eine Verbindung zur Sybase ASE-Datenbank herstellen können.

   Zum Herstellen der Verbindung zur Datenbank starten Sie ISQL und geben die Konnektivitätsinformationen ein. Wenn die Verbindung zur Datenbank fehlschlägt, überprüfen Sie, ob Sie alle Konnektivitätsinformationen richtig eingegeben haben.

   Bei Benutzernamen und Datenbanknamen wird zwischen Groß- und Kleinschreibung unterschieden.

Herstellen einer Verbindung zu einer Teradata-Datenbank über Windows

Installieren und konfigurieren Sie native Client-Software auf den Computern, auf denen der Datenintegrationsdienst- und PowerCenter-Integrationsdienst-Prozess ausgeführt und auf denen Informatica Developer und PowerCenter Client installiert wird. Verwenden Sie zur Gewährleistung der Kompatibilität zwischen Informatica und den Datenbanken die entsprechenden Datenbank-Client-Bibliotheken. Sie müssen die Konnektivität zu folgenden Informatica-Komponenten unter Windows konfigurieren:

- **Integrationsdienst** Installieren Sie den Teradata-Client, den Teradata-ODBC-Treiber sowie weitere eventuell benötigte Teradata-Client-Software auf dem Computer, auf dem der Datenintegrationsdienst und der PowerCenter-Integrationsdienst ausgeführt wird. Außerdem müssen Sie die ODBC-Konnektivität konfigurieren.
- **Informatica Developer** Installieren Sie den Teradata-Client, den Teradata-ODBC-Treiber sowie weitere eventuell benötigte Teradata-Client-Software auf jedem Rechner, auf dem sich ein Developer Tool befindet, das auf Teradata zugreift. Außerdem müssen Sie die ODBC-Konnektivität konfigurieren.
- **PowerCenter Client** Installieren Sie den Teradata-Client, den Teradata-ODBC-Treiber sowie weitere eventuell benötigte Teradata-Client-Software auf jedem PowerClient-Rechner, der auf Teradata zugreift. Verwenden Sie den Workflow Manager zum Erstellen eines Datenbankverbindungsobjekts für die Teradata-Datenbank.

Hinweis: Entsprechend einer Empfehlung von Teradata verwendet Informatica ODBC für die Verbindung mit Teradata. ODBC ist eine native Schnittstelle für Teradata.

Konfigurieren der ODBC-Konnektivität

Sie können ODBC-Konnektivität für eine Teradata-Datenbank konfigurieren.

Die folgenden Schritte enthalten eine Richtlinie zum Konfigurieren der ODBC-Konnektivität. Spezifische Anweisungen finden Sie in der Dokumentation zur Datenbank.

1. Erstellen Sie eine ODBC-Datenquelle für jede Teradata-Datenbank, auf die Sie zugreifen möchten.

   Erstellen Sie mithilfe des von Teradata bereitgestellten Treibers die ODBC-Datenquelle.

   Erstellen Sie einen System-DSN, wenn Sie den Informatica-Dienst mit einer *Lokalen Systemkonto*-Anmeldung starten. Erstellen Sie einen Benutzer-DSN, wenn Sie zum Starten des Informatica-Dienstes die Anmeldeoption *Dieses Konto* wählen.

2. Geben Sie den Namen für die neue ODBC-Datenquelle und den Namen des Teradata-Servers oder dessen IP-Adresse ein.

   Geben Sie zum Konfigurieren einer Verbindung zu einer einzelnen Teradata-Datenbank den DefaultDatabase-Namen ein. Geben Sie zum Erstellen einer Einzelverbindung zur Standard-Datenbank den Benutzernamen und das Passwort ein. Zum Herstellen einer Verbindung zu mehreren Datenbanken mithilfe derselben ODBC-Datenquelle lassen Sie die Felder DefaultDatabase, Benutzername und Passwort leer.

3. Konfigurieren Sie die Datumsoptionen im Dialogfeld "Optionen".

   Geben Sie im Dialogfeld "Teradata-Optionen" AAA für das DateTime-Format an.

4. Konfigurieren Sie den Sitzungsmodus im Dialogfeld "Optionen".

   Wählen Sie bei Erstellung einer Zieldatenquelle den Sitzungsmodus ANSI. Beim ANSI-Sitzungsmodus führt Teradata bei Auftreten eines Zeilenfehlers kein Rollback der Transaktion durch. Beim Teradata-Sitzungsmodus führt Teradata bei Auftreten eines Zeilenfehlers ein Rollback der Transaktion durch. Im

Teradata-Modus kann der Integration Service das Rollback nicht erkennen und zeichnet ihn nicht im Sitzungsprotokoll auf.

5. Überprüfen Sie, ob Sie eine Verbindung zur Teradata-Datenbank herstellen können.

   Verwenden Sie zum Testen der Verbindung ein Teradata-Client-Programm wie WinDDI, BTEQ, Teradata Administrator oder Teradata SQL Assistant.

ANHANG C

Verbinden zu Datenbanken unter UNIX

Dieser Anhang umfasst die folgenden Themen:

- Verbinden zu Datenbanken unter UNIX - Übersicht, 260
- Verbinden zu einer IBM DB2 Universal-Datenbank unter UNIX, 261
- Verbinden zu einer Informix-Datenbank unter UNIX, 263
- Herstellen einer Verbindung zu Microsoft SQL Server unter UNIX, 264
- Verbinden zu einer Netezza-Datenbank unter UNIX, 266
- Herstellen einer Verbindung zu einer Oracle-Datenbank unter UNIX, 269
- Herstellen einer Verbindung zu einer Sybase ASE-Datenbank unter UNIX, 271
- Herstellen einer Verbindung zu einer Teradata-Datenbank über UNIX, 273
- Herstellen einer Verbindung zu einer ODBC-Datenquelle, 276
- odbc.ini-Beispieldatei, 278

Verbinden zu Datenbanken unter UNIX - Übersicht

Zur Verwendung der nativen Konnektivität müssen Sie die Datenbank-Client-Software für die Datenbank, auf die Sie zugreifen möchten, installieren und konfigurieren. Um die Kompatibilität zwischen dem Anwendungsdienst und der Datenbank zu gewährleisten, installieren Sie eine Client-Software, die mit der Datenbankversion kompatibel ist, und verwenden Sie die entsprechenden Bibliotheken des Datenbank-Client. Um die Leistung zu erhöhen, verwenden Sie native Konnektivität.

Die Informatica-Installation enthält DataDirect-ODBC-Treiber. Wenn ODBC-Datenquellen bereits mit früheren Versionen der Treiber erstellt wurden, müssen Sie mit den neuen Treibern neue ODBC-Datenquellen erstellen. Konfigurieren Sie die ODBC-Verbindungen mithilfe der von Informatica mitgelieferten DataDirect-ODBC-Treiber oder mit ODBC-Treibern von Drittanbietern, die mit Level 2 oder höher kompatibel sind.

Sie müssen eine Datenbankverbindung für die folgenden Dienste in der Informatica-Domäne konfigurieren:

- PowerCenter-Repository-Dienst
- Modellrepository-Dienst
- Datenintegrationsdienst
- Analyst-Dienst

Wenn Sie über Linux oder UNIX eine Verbindung zu Datenbanken herstellen, verwenden Sie native Treiber zum Herstellen einer Verbindung zu IBM DB2-, Oracle- oder Sybase ASE-Datenbanken. Mit ODBC können Sie eine Verbindung zu anderen Quellen und Zielen herstellen.

Verbinden zu einer IBM DB2 Universal-Datenbank unter UNIX

Installieren Sie für eine native Konnektivität die Version von IBM DB2 Client Application Enabler (CAE), die für die IBM DB2-Datenbankserverversion geeignet ist. Verwenden Sie zur Gewährleistung der Kompatibilität zwischen Informatica und den Datenbanken die entsprechenden Datenbank-Client-Bibliotheken.

Konfigurieren von nativer Konnektivität

Sie können native Konnektivität für eine IBM DB2-Datenbank konfigurieren, um die Leistung zu erhöhen.

Die folgenden Schritte stellen eine Richtlinie zum Konfigurieren der nativen Konnektivität dar. Spezifische Anweisungen finden Sie in der Dokumentation zur Datenbank.

1. Um die Konnektivität auf dem Computer zu konfigurieren, auf dem der Datenintegrationsdienst-, PowerCenter-Integrationsdienst- oder PowerCenter-Repository-Dienst-Prozess ausgeführt wird, melden Sie sich am Computer als ein Benutzer an, der einen Dienstprozess starten kann.
2. Setzen Sie die Umgebungsvariablen DB2INSTANCE, INSTHOME, DB2DIR und PATH.

   Die IBM DB2-Software für UNIX hat immer eine zugeordnete Benutzeranmeldung, meistens db2admin, die für Datenbankkonfigurationen benutzt wird. Der Benutzer besitzt die DB2-Instanz.

   DB2INSTANCE. Der Name des Instanzbesitzers.

   Bei Verwendung einer Bourne-Shell:

   ```
   $ DB2INSTANCE=db2admin; export DB2INSTANCE
   ```

   Bei Verwendung einer C-Shell:

   ```
   $ setenv DB2INSTANCE db2admin
   ```

   INSTHOME. Das ist ein db2admin-Basisverzeichnispfad.

   Bei Verwendung einer Bourne-Shell:

   ```
   $ INSTHOME=~db2admin
   ```

   Bei Verwendung einer C-Shell:

   ```
   $ setenv INSTHOME ~db2admin>
   ```

   DB2DIR. Legen Sie die Variable so fest, dass sie auf das Installationsverzeichnis von IBM DB2 CAE verweist. Wenn beispielsweise der Client im Verzeichnis /opt/IBM/db2/V9.7 installiert ist:

   Bei Verwendung einer Bourne-Shell:

   ```
   $ DB2DIR=/opt/IBM/db2/V9.7; export DB2DIR
   ```

   Bei Verwendung einer C-Shell:

   ```
   $ setenv DB2DIR /opt/IBM/db2/V9.7
   ```

   PATH. Legen Sie zum Ausführen der IBM DB2-Befehlszeilenprogramme die Variable so fest, dass sie das DB2-bin-Verzeichnis enthält.

   Bei Verwendung einer Bourne-Shell:

   ```
   $ PATH=${PATH}:$DB2DIR/bin; export PATH
   ```

Bei Verwendung einer C-Shell:

```
$ setenv PATH ${PATH}:$DB2DIR/bin
```

3. Legen Sie die Variable der gemeinsam genutzten Bibliothek so fest, dass sie das DB2-lib-Verzeichnis enthält.

   Die IBM DB2-Clientsoftware enthält eine Reihe von gemeinsam genutzten Bibliothekskomponenten, die die Datenintegrationsdienst-, PowerCenter-Integrationsdienst- und PowerCenter-Repository-Dienst-Prozesse dynamisch laden. Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek so fest, dass die Dienste die gemeinsam genutzten Bibliotheken zur Laufzeit suchen können.

   Der Pfad der gemeinsam genutzten Bibliothek muss außerdem das Informatica-Installationsverzeichnis *(server_dir)* enthalten.

   Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek basierend auf dem Betriebssystem fest.

   In der folgenden Tabelle werden die Variablen der gemeinsam genutzten Bibliothek für jedes Betriebssystem beschrieben:

Betriebssystem	Variable
Solaris	LD_LIBRARY_PATH
Linux	LD_LIBRARY_PATH
AIX	LIBPATH

   Benutzen Sie zum Beispiel die folgende Syntax für Solaris und Linux:

   - Bei Verwendung einer Bourne-Shell:

     ```
     $ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:$HOME/server_dir:$DB2DIR/lib; export
     LD_LIBRARY_PATH
     ```

   - Bei Verwendung einer C-Shell:

     ```
     $ setenv LD_LIBRARY_PATH ${LD_LIBRARY_PATH}:$HOME/server_dir:$DB2DIR/lib
     ```

   Für AIX:

   - Bei Verwendung einer Bourne-Shell:

     ```
     $ LIBPATH=${LIBPATH}:$HOME/server_dir:$DB2DIR/lib; export LIBPATH
     ```

   - Bei Verwendung einer C-Shell:

     ```
     $ setenv LIBPATH ${LIBPATH}:$HOME/server_dir:$DB2DIR/lib
     ```

4. Bearbeiten Sie die .cshrc- oder die .profile-Datei, um den gesamten Satz der Shell-Befehle einzubeziehen. Speichern Sie die Datei und melden Sie sich entweder erneut an oder führen Sie den Quellbefehl aus.

   Bei Verwendung einer Bourne-Shell:

   ```
   $ source .profile
   ```

   Bei Verwendung einer C-Shell:

   ```
   $ source .cshrc
   ```

5. Wenn sich die DB2-Datenbank auf demselben Computer befindet, auf dem der Datenintegrationsdienst-, PowerCenter-Integrationsdienst- oder PowerCenter-Repository-Dienst-Prozess läuft, konfigurieren Sie die DB2-Instanz als Remoteinstanz.

   Führen Sie den folgenden Befehl aus, um zu überprüfen, ob es einen Remote-Eintrag für die Datenbank gibt:

   ```
   DB2 LIST DATABASE DIRECTORY
   ```

Der Befehl listet neben allen Datenbanken, auf die der DB2-Client zugreifen kann, auch ihre Konfigurationseigenschaften auf. Wenn dieser Befehl einen Eintrag für „Verzeichnis-Eintragstyp“ von „Remote“ auflistet, fahren Sie mit Schritt 6 fort.

Wenn die Datenbank nicht als „Remote“ konfiguriert ist, dann führen Sie den folgenden Befehl aus, um zu überprüfen, ob ein TCP/IP-Knoten für den Host katalogisiert ist:

```
DB2 LIST NODE DIRECTORY
```

Wenn der Knotenname leer ist, können Sie beim Einrichten einer Remotedatenbank einen Knoten erstellen. Verwenden Sie den folgenden Befehl, um eine Remotedatenbank einzurichten und um ggfs. einen Knoten zu erstellen:

```
db2 CATALOG TCPIP NODE <nodename> REMOTE <hostname_or_address> SERVER <port number>
```

Führen Sie den folgenden Befehl aus, um die Datenbank zu katalogisieren:

```
db2 CATALOG DATABASE <dbname> as <dbalias> at NODE <nodename>
```

Weitere Informationen zu diesen Befehlen finden Sie in der Datenbankdokumentation.

6. Prüfen Sie, ob Sie eine Verbindung zu der DB2-Datenbank herstellen können. Öffnen Sie den DB2-Befehlszeilenprozessor und führen Sie folgenden Befehl aus:

   ```
   CONNECT TO <dbalias> USER <username> USING <password>
   ```

   Wenn die Verbindung erfolgreich hergestellt wurde, führen Sie mit den Befehlen `CONNECT RESET` oder `TERMINATE` eine Bereinigung durch.

Verbinden zu einer Informix-Datenbank unter UNIX

Verwenden Sie ODBC zum Herstellen einer Verbindung für eine Informix-Datenbank unter UNIX.

Konfigurieren der ODBC-Konnektivität

Sie können ODBC-Konnektivität für eine Informix-Datenbank konfigurieren.

Die folgenden Schritte enthalten eine Richtlinie zum Konfigurieren der ODBC-Konnektivität. Spezifische Anweisungen finden Sie in der Dokumentation zur Datenbank.

1. Legen Sie die Umgebungsvariablen ODBCHOME gemäß dem ODBC-Installationsverzeichnis fest. Beispiel:
   Bei Verwendung einer Bourne-Shell:

   ```
   $ ODBCHOME=<Informatica server home>/ODBC7.1; export ODBCHOME
   ```

   Bei Verwendung einer C-Shell:

   ```
   $ setenv ODBCHOME <Informatica server home>/ODBC7.1
   ```

2. Richten Sie die Umgebungsvariable ODBCINI auf den Speicherort der Datei odbc.ini ein. Die Datei odbc.ini befindet sich zum Beispiel im Verzeichnis $ODBCHOME:

   Bei Verwendung einer Bourne-Shell:

   ```
   ODBCINI=$ODBCHOME/odbc.ini; export ODBCINI
   ```

   Bei Verwendung einer C-Shell:

   ```
   $ setenv ODBCINI $ODBCHOME/odbc.ini
   ```

3. Bearbeiten Sie die bestehende Datei odbc.ini im Verzeichnis $ODBCHOME oder kopieren Sie die Datei odbc.ini in das UNIX-Basisverzeichnis und bearbeiten Sie sie dort.

   ```
   $ cp $ODBCHOME/odbc.ini $HOME/.odbc.ini
   ```

4. Fügen Sie einen Eintrag zu der Informix-Datenquelle unter dem Abschnitt [ODBC Data Sources] hinzu und konfigurieren Sie die Datenquelle. Beispiel:

```
[Informix Wire Protocol]
Driver=/export/home/Informatica/10.0.0/ODBC7.1/lib/DWifcl27.so
Description=DataDirect 7.1 Informix Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
CancelDetectInterval=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
HostName=<Informix_host>
LoadBalancing=0
LogonID=
Password=
PortNumber=<Informix_server_port>
ReportCodePageConversionErrors=0
ServerName=<Informix_server>
TrimBlankFromIndexName=1
```

5. Legen Sie die Umgebungsvariablen für PATH und für die geteilte Bibliothek durch Ausführen des Skripts odbc.sh oder odbc.csh im Verzeichnis $ODBCHOME fest.

   Bei Verwendung einer Bourne-Shell:

   ```
   sh odbc.sh
   ```

   Bei Verwendung einer C-Shell:

   ```
   source odbc.csh
   ```

6. Stellen Sie sicher, dass Sie mithilfe der ODBC-Datenquelle eine Verbindung zur Informix-Datenbank herstellen können. Falls die Verbindung fehlschlägt, lesen Sie die Dokumentation zur Datenbank.

Herstellen einer Verbindung zu Microsoft SQL Server unter UNIX

Über die Microsoft SQL Server-Verbindung können Sie an einem UNIX-Computer eine Verbindung zu einer Microsoft SQL Server-Datenbank herstellen.

Konfigurieren der nativen Konnektivität

Beim Konfigurieren einer Microsoft SQL Server-Verbindung müssen Sie ODBC als Providertyp auswählen. Der Providertyp OLEDB ist veraltet. Die Unterstützung des Providertyps OLEDB wird in einer der zukünftigen Versionen aufgehoben.

Der Servername und der Datenbankname werden aus der Verbindungszeichenfolge abgerufen, wenn Sie die Option „DSN verwenden“ aktivieren. Die Verbindungszeichenfolge ist der in der Datei „odbc.ini“ konfigurierte DSN. Falls Sie die Option „DSN verwenden“ nicht aktivieren, müssen Sie den Servernamen und den Datenbanknamen in den Verbindungseigenschaften angeben. Wenn Sie keine Verbindung zu der Datenbank herstellen können, vergewissern Sie sich, dass Sie alle Konnektivitätsinformationen korrekt eingegeben haben.

Nach dem Upgrade wird die Microsoft SQL Server-Verbindung standardmäßig auf den Providertyp OLEDB festgelegt. Es wird empfohlen, zur Verwendung des Providertyps ODBC alle Microsoft SQL Server-

Verbindungen zu aktualisieren. Mithilfe der folgenden Befehle können Sie alle Ihre Microsoft SQL Server-Verbindungen auf den Providertyp ODBC aktualisieren:

- Wenn Sie PowerCenter verwenden, führen Sie den folgenden Befehl aus: pmrep upgradeSqlServerConnection
- Wenn Sie die Informatica-Plattform verwenden, führen Sie den folgenden Befehl aus: infacmd.sh isp upgradeSQLSConnection

Nach der Ausführung des Upgrade-Befehls müssen Sie die Umgebungsvariable auf jedem Computer, auf dem das Developer Tool gehostet wird, und auf dem Computer, auf dem Informatica-Dienste gehostet werden, im folgenden Format festlegen:

```
ODBCINST=<INFA_HOME>/ODBC7.1/odbcinst.ini
```

Nachdem Sie die Umgebungsvariable festgelegt haben, müssen Sie den Knoten, auf dem die Informatica-Dienste gehostet werden, neu starten.

Spezifische Anweisungen zur Konnektivität finden Sie in der Dokumentation zur Datenbank.

Regeln und Richtlinien für Microsoft SQL Server

Berücksichtigen Sie beim Konfigurieren der ODBC-Konnektivität zu einer Microsoft SQL Server-Datenbank die folgenden Regeln und Richtlinien:

- Falls Sie eine Microsoft SQL Server-Verbindung ohne Verwendung eines Datenquellennamens (Verbindung ohne DSN) nutzen möchten, müssen Sie die Umgebungsvariable „odbcinst.ini“ konfigurieren.
- Bei Verwendung einer DSN-Verbindung müssen Sie dem ODBC-DSN den Eintrag „EnableQuotedIdentifiers=1“ hinzufügen. Wenn Sie den Eintrag nicht hinzufügen, schlägt die Ausführung der Datenvorschau und des Mappings fehl.
- Sie können die NTLM-Authentifizierung von Microsoft SQL Server für eine Microsoft SQL Server-Verbindung ohne DSN auf der Microsoft Windows-Plattform verwenden.
- Wenn die Microsoft SQL Server-Tabelle einen UUID-Datentyp enthält und Sie Daten aus einer SQL-Tabelle lesen sowie Daten in eine Einfachdatei schreiben, ist das Datenformat zwischen den OLEDB- und ODBC-Verbindungstypen möglicherweise nicht konsistent.
- Für eine Verbindung ohne DSN können Sie keine SSL-Verbindung verwenden. Zur Nutzung von SSL müssen Sie die DSN-Verbindung verwenden. Aktivieren Sie die Option „DSN verwenden“ und konfigurieren Sie die SSL-Optionen in der Datei „odbc.ini“.
- Falls Microsoft SQL Server die Kerberos-Authentifizierung verwendet, müssen Sie die Eigenschaft „GSSClient“ festlegen, um auf die Kerberos-Bibliotheken von Informatica zu verweisen. Verwenden Sie den folgenden Pfad und Dateinamen: `<Informatica-Installationsverzeichnis>/server/bin/libgssapi_krb5.so.2`. Erstellen Sie für eine DSN-Verbindung in `odbc.ini` im Abschnitt für DSN-Einträge einen Eintrag für die Eigenschaft „GSSClient“ bzw. für eine Verbindung, bei der kein DSN verwendet wird, einen Eintrag in `odbcinst.ini` im Abschnitt für SQL Server Wire Protocol.

Konfigurieren der SSL-Authentifizierung über ODBC

Sie können die SSL-Authentifizierung für Microsoft SQL Server über ODBC mit dem neuen SQL Server-Übertragungsprotokolltreiber von DataDirect konfigurieren.

1. Öffnen Sie die odbc.ini-Datei und fügen Sie einen Eintrag für die ODBC-Datenquelle und den neuen SQL Server-Übertragungsprotokolltreiber von DataDirect unter dem Abschnitt [ODBC Data Sources] hinzu.
2. Fügen Sie die Attribute in der odbc.ini-Datei zum Konfigurieren von SSL hinzu:

In der folgenden Tabelle werden die Attribute aufgelistet, die Sie bei der Konfiguration der SSL-Authentifizierung zur odbc.ini-Datei hinzufügen müssen:

Attribut	Beschreibung
EncryptionMethod	Die vom Treiber verwendete Methode zum Verschlüsseln der zwischen dem Treiber und dem Datenbankserver gesendeten Daten. Legen Sie den Wert auf 1 fest, um Daten mit SSL zu verschlüsseln.
ValidateServerCertificate	Bestimmt, ob der Treiber das vom Datenbankserver bei Aktivierung der SSL-Verschlüsselung gesendete Zertifikat validiert. Legen Sie den Wert für den Treiber auf 1 fest, um das Serverzertifikat zu validieren.
TrustStore	Der Speicherort und der Name der Trust Store-Datei. Die Trust Store-Datei enthält eine Liste mit Zertifizierungsstellen, die der Treiber für die SSL-Serverauthentifizierung verwendet.
TrustStorePassword	Das Passwort für den Zugriff auf den Inhalt der Trust Store-Datei.
HostNameInCertificate	Optional. Der Hostname, der vom SSL-Administrator für den Treiber eingerichtet ist, um den im Zertifikat enthaltenen Hostnamen zu validieren.

Konfigurieren von benutzerdefinierten Eigenschaften für Microsoft SQL Server

Zur Verbesserung der Bulk Load-Leistung können Sie benutzerdefinierte Eigenschaften für Microsoft SQL Server konfigurieren.

1. Starten Sie den PowerCenter-Client und stellen Sie eine Verbindung zum Workflow Manager her.
2. Öffnen Sie einen Arbeitsablauf und wählen Sie eine Sitzung aus, die Sie konfigurieren möchten.
3. Klicken Sie auf die Registerkarte **Konfig-Objekt**.
4. Ändern Sie den Wert der **Standard-Pufferblockgröße** in 5 MB. Sie können auch den folgenden Befehl verwenden: `$INFA_HOME/server/bin/./pmrep massupdate -t session_config_property -n "Default buffer block size" -v "5MB" -f $<folderName>`

   Wenn Sie für eine Zeilengröße von 1 KB einen optimalen Durchsatz erzielen möchten, müssen Sie die Pufferblockgröße auf 5 MB festlegen.
5. Klicken Sie auf die Registerkarte **Eigenschaften**.
6. Ändern Sie das **Commit-Intervall** in 100000, falls die Sitzung ein relationales Ziel enthält.
7. Legen Sie die **DTM-Puffergröße** fest. Die optimale DTM-Puffergröße ist ((10 x Pufferblockgröße) x Anzahl der Partitionen).

Verbinden zu einer Netezza-Datenbank unter UNIX

Installieren Sie den Netezza ODBC-Treiber auf dem Rechner, auf dem die PowerCenter Integration Service-Vorgänge ausgeführt werden. Verwenden Sie den DataDirect-Treiber-Manager im DataDirect-Treiberpaket (im Lieferumfang von Informatica enthalten) zum Konfigurieren der Netezza-Datenquellendetails in der Datei odbc.ini.

Konfigurieren der ODBC-Konnektivität

Sie können ODBC-Konnektivität für eine Netezza-Datenbank konfigurieren.

Die folgenden Schritte enthalten eine Richtlinie zum Konfigurieren der ODBC-Konnektivität. Spezifische Anweisungen finden Sie in der Dokumentation zur Datenbank.

1. Um die Konnektivität für den Integration-Service-Prozess zu konfigurieren, melden Sie sich am Computer als Benutzer an, der einen Dienstprozess starten kann.
2. Setzen Sie die Umgebungsvariablen ODBCHOME, NZ_ODBC_INI_PATH und PATH.

   ODBCHOME. Legen Sie die Variable auf das ODBC-Installationsverzeichnis fest. Beispiel:

   Bei Verwendung einer Bourne-Shell:

   ```
   $ ODBCHOME=<Informatica server home>/ODBC7.1; export ODBCHOME
   ```

   Bei Verwendung einer C-Shell:

   ```
   $ setenv ODBCHOME =<Informatica server home>/ODBC7.1
   ```

   PATH. Legen Sie die Variable auf das Verzeichnis ODBCHOME/bin fest. Beispiel:

   Bei Verwendung einer Bourne-Shell:

   ```
   PATH="${PATH}:$ODBCHOME/bin"
   ```

   Bei Verwendung einer C-Shell:

   ```
   $ setenv PATH ${PATH}:$ODBCHOME/bin
   ```

   NZ_ODBC_INI_PATH. Legen Sie die Variable so fest, dass sie auf das Verzeichnis verweist, das die Datei odbc.ini enthält. Die Datei odbc.ini befindet sich zum Beispiel im Verzeichnis $ODBCHOME:

   Bei Verwendung einer Bourne-Shell:

   ```
   NZ_ODBC_INI_PATH=$ODBCHOME; export NZ_ODBC_INI_PATH
   ```

   Bei Verwendung einer C-Shell:

   ```
   $ setenv NZ_ODBC_INI_PATH $ODBCHOME
   ```

3. Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek fest.

   Der Pfad der gemeinsam genutzten Bibliothek muss die ODBC-Bibliotheken enthalten. Er muss außerdem das Installationsverzeichnis der Informatica-Dienste `(server_dir)` enthalten.

   Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek basierend auf dem Betriebssystem fest. Setzen Sie den Ordner der Netezza-Bibliothek auf <NetezzaInstallationDir>/lib64.

   In der folgenden Tabelle werden die Variablen der gemeinsam genutzten Bibliothek für jedes Betriebssystem beschrieben:

Betriebssystem	Variable
Solaris	LD_LIBRARY_PATH
Linux	LD_LIBRARY_PATH
AIX	LIBPATH

   Benutzen Sie zum Beispiel die folgende Syntax für Solaris und Linux:

   - Bei Verwendung einer Bourne-Shell:

     ```
     $ LD_LIBRARY_PATH="${LD_LIBRARY_PATH}:$HOME/server_dir:$ODBCHOME/
     lib:<NetezzaInstallationDir>/lib64”
     export LD_LIBRARY_PATH
     ```

- Bei Verwendung einer C-Shell:

```
$ setenv LD_LIBRARY_PATH "${LD_LIBRARY_PATH}:$HOME/server_dir:$ODBCHOME/
lib:<NetezzaInstallationDir>/lib64"
```

Für AIX

- Bei Verwendung einer Bourne-Shell:

```
$ LIBPATH=${LIBPATH}:$HOME/server_dir:$ODBCHOME/lib:<NetezzaInstallationDir>/
lib64; export LIBPATH
```

- Bei Verwendung einer C-Shell:

```
$ setenv LIBPATH ${LIBPATH}:$HOME/server_dir:$ODBCHOME/
lib:<NetezzaInstallationDir>/lib64
```

4. Bearbeiten Sie die vorhandene odbc.ini-Datei oder kopieren Sie die odbc.ini-Datei in das Basisverzeichnis und bearbeiten Sie sie.

   Die Datei befindet sich im Verzeichnis $ODBCHOME.

```
$ cp $ODBCHOME/odbc.ini $HOME/.odbc.ini
```

   Fügen Sie einen Eintrag zu der Netezza-Datenquelle unter dem Abschnitt [ODBC Data Sources] hinzu und konfigurieren Sie die Datenquelle.

   Beispiel:

```
[NZSQL]
Driver = /export/home/appsqa/thirdparty/netezza/lib64/libnzodbc.so
Description = NetezzaSQL ODBC
Servername = netezza1.informatica.com
Port = 5480
Database = infa
Username = admin
Password = password
Debuglogging = true
StripCRLF = false
PreFetch = 256
Protocol = 7.0
ReadOnly = false
ShowSystemTables = false
Socket = 16384
DateFormat = 1
TranslationDLL =
TranslationName =
TranslationOption =
NumericAsChar = false
```

   Weitere Informationen zur Netezza-Konnektivität finden Sie in der Netezza-ODBC-Treiber-Dokumentation.

5. Prüfen Sie, ob der letzte Eintrag in der odbc.ini-Datei InstallDir ist und lassen Sie ihn auf das ODBC-Installationsverzeichnis verweisen.

   Beispiel:

```
InstallDir=<Informatica install directory>/<ODBCHOME directory>
```

6. Bearbeiten Sie die .cshrc- oder die .profile-Datei, um den gesamten Satz der Shell-Befehle einzubeziehen.
7. Starten Sie die Informatica-Dienste neu.

Herstellen einer Verbindung zu einer Oracle-Datenbank unter UNIX

Installieren Sie für eine native Konnektivität die für die Oracle-Datenbankserverversion geeignete Version des Oracle-Client. Verwenden Sie zur Gewährleistung der Kompatibilität zwischen Informatica und den Datenbanken die entsprechenden Datenbank-Client-Bibliotheken.

Sie müssen kompatible Versionen des Oracle-Client und des Oracle-Datenbankservers installieren. Des Weiteren müssen Sie dieselbe Version des Oracle-Client auf allen Rechnern installieren, die ihn benötigen. Informationen zur Überprüfung der Kompatibilität erhalten Sie von Oracle.

Konfigurieren der nativen Konnektivität

Sie können native Konnektivität für eine Oracle-Datenbank konfigurieren, um die Leistung zu erhöhen.

Die folgenden Schritte enthalten eine Richtlinie zum Konfigurieren der nativen Konnektivität über Oracle Net Services oder Net8. Spezifische Anweisungen finden Sie in der Dokumentation zur Datenbank.

1. Um die Konnektivität für den Datenintegrationsdienst-, PowerCenter-Integrationsdienst- oder PowerCenter-Repository-Dienst-Prozess zu konfigurieren, melden Sie sich am Computer als Benutzer an, der den Serverprozess starten kann.
2. Legen Sie die Umgebungsvariablen ORACLE_HOME, NLS_LANG, TNS_ADMIN und PATH fest.

   ORACLE_HOME. Legen Sie die Variable so fest, dass sie auf das Installationsverzeichnis des Oracle-Client verweist. Wenn der Client beispielsweise im Verzeichnis /HOME2/oracle installiert ist, legen Sie die Variable wie folgt fest:

   Bei Verwendung einer Bourne-Shell:

   ```
   $ ORACLE_HOME=/HOME2/oracle; export ORACLE_HOME
   ```

   Bei Verwendung einer C-Shell:

   ```
   $ setenv ORACLE_HOME /HOME2/oracle
   ```

   NLS_LANG. Legen Sie die Variable auf das Gebietsschema fest (Sprache, Gebiet, Zeichensatz), das der Datenbank-Client und der Server beim Anmelden benutzen sollen. Der Wert dieser Variable hängt von der Konfiguration ab. Wenn es sich bei dem Wert beispielsweise um american_america.UTF8 handelt, legen Sie die Variable wie folgt fest:

   Bei Verwendung einer Bourne-Shell:

   ```
   $ NLS_LANG=american_america.UTF8; export NLS_LANG
   ```

   Bei Verwendung einer C-Shell:

   ```
   $ NLS_LANG american_america.UTF8
   ```

   Kontaktieren Sie den Administrator, um den Wert dieser Variablen zu ermitteln.

   ORA_SDTZ. Geben Sie zum Einrichten der Zeitzone einer Standardsitzung die Umgebungsvariable ORA_SDTZ an, wenn der Datenintegrationsdienst Daten vom Typ „Zeitstempel mit lokaler Zeitzone“ liest oder schreibt.

   Sie können die Umgebungsvariable ORA_SDTZ auf einen der folgenden Werte festlegen:

   - Lokale Zeitzone des Betriebssystems ('OS_TZ')
   - Zeitzone der Datenbank ('DB_TZ')
   - Absoluter Versatz von UTC (z. B. '-05:00')
   - Name der Zeitzonenregion (z. B. 'America/Los_Angeles')

Sie können die Umgebungsvariable auf dem Computer festlegen, auf dem der Informatica-Server ausgeführt wird.

TNS_ADMIN. Wenn sich die Datei tnsnames.ora nicht in demselben Speicherort wie das Oracle-Installationsverzeichnis befindet, legen Sie die TNS_ADMIN-Umgebungsvariable tnsnames.ora für das Verzeichnis fest, in dem sich die Datei tnsnames.ora befindet. Wenn sich die Datei beispielsweise im Verzeichnis /HOME2/oracle/files befindet, legen Sie die Variable wie folgt fest:

Bei Verwendung einer Bourne-Shell:

```
$ TNS_ADMIN=$HOME2/oracle/files; export TNS_ADMIN
```

Bei Verwendung einer C-Shell:

```
$ setenv TNS_ADMIN=$HOME2/oracle/files
```

Hinweis: Die Datei `tnsnames.ora` ist standardmäßig in folgendem Verzeichnis gespeichert: `$ORACLE_HOME/network/admin`.

PATH. Zum Ausführen der Oracle-Befehlszeilenprogramme, legen Sie die Variable so fest, dass sie das Oracle-bin-Verzeichnis enthält.

Bei Verwendung einer Bourne-Shell:

```
$ PATH=${PATH}:$ORACLE_HOME/bin; export PATH
```

Bei Verwendung einer C-Shell:

```
$ setenv PATH ${PATH}:ORACLE_HOME/bin
```

3. Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek fest.

   Die Oracle-Clientsoftware enthält eine Reihe von gemeinsam genutzten Bibliothekskomponenten, die die Datenintegrationsdienst-, PowerCenter-Integrationsdienst- und PowerCenter-Repository-Dienst-Prozesse dynamisch laden. Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek fest, um die gemeinsam genutzten Bibliotheken während der Laufzeit zu suchen.

   Der Pfad der gemeinsam genutzten Bibliothek muss außerdem das Informatica-Installationsverzeichnis `(server_dir)` enthalten.

   Legen Sie die Umgebungsvariable der gemeinsamen Bibliothek auf LD_LIBRARY_PATH fest.

   Verwenden Sie zum Beispiel die folgende Syntax:

   - Bei Verwendung einer Bourne-Shell:

     ```
     $ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:$HOME/server_dir:$ORACLE_HOME/lib; export
     LD_LIBRARY_PATH
     ```

   - Bei Verwendung einer C-Shell:

     ```
     $ setenv LD_LIBRARY_PATH ${LD_LIBRARY_PATH}:$HOME/server_dir:$ORACLE_HOME/lib
     ```

4. Bearbeiten Sie die .cshrc- oder die .profile-Datei, um den gesamten Satz der Shell-Befehle einzubeziehen. Speichern Sie die Datei und melden Sie sich entweder erneut an oder führen Sie den Quellbefehl aus.

   Bei Verwendung einer Bourne-Shell:

   ```
   $ source .profile
   ```

   Bei Verwendung einer C-Shell:

   ```
   $ source .cshrc
   ```

5. Vergewissern Sie sich, dass der Orcale-Client so konfiguriert ist, dass er auf die Datenbank zugreifen kann.

   Verwenden Sie das Dienstprogramm SQL*Net Easy Configuration oder kopieren Sie eine bestehende `tnsnames.ora`-Datei in das Basisverzeichnis und verändern Sie diese.

   Die Datei `tnsnames.ora` ist in folgendem Verzeichnis gespeichert: `$ORACLE_HOME/network/admin`.

Geben Sie die richtige Syntax für die Oracle-Verbindungszeichenfolge ein. Diese lautet normalerweise `databasename.world`.

Hier ist eine `tnsnames.ora`-Beispieldatei. Geben Sie die Informationen für die Datenbank ein.

```
mydatabase.world =
   (DESCRIPTION
   (ADDRESS_LIST =
        (ADDRESS =
           (COMMUNITY = mycompany.world
           (PROTOCOL = TCP)
           (Host = mymachine)
           (Port = 1521)
        )
   )
   (CONNECT_DATA =
      (SID = MYORA7)
      (GLOBAL_NAMES = mydatabase.world)
```

6. Vergewissern Sie sich, dass Sie eine Verbindung zu der Oracle-Datenbank herstellen können.

   Um eine Verbindung zu der Oracle-Datenbank herzustellen, starten Sie SQL*Plus und geben Sie dann die Konnektivitätsinformationen ein. Wenn Sie keine Verbindung zu der Datenbank herstellen können, vergewissern Sie sich, dass Sie alle Konnektivitätsinformationen korrekt eingegeben haben.

   Geben Sie den in der `tnsnames.ora`-Datei definierten Benutzernamen und die Verbindungszeichenfolge ein.

Herstellen einer Verbindung zu einer Sybase ASE-Datenbank unter UNIX

Installieren Sie für eine native Konnektivität die für Ihre Datenbankversion geeignete Version von Open Client. Verwenden Sie zur Gewährleistung der Kompatibilität zwischen Informatica und den Datenbanken die entsprechenden Datenbank-Client-Bibliotheken.

Installieren Sie eine mit dem Sybase ASE-Datenbankserver kompatible Version von Open Client Sie müssen dieselbe Version von Open Client auf den Rechnern installieren, auf denen sich die Sybase ASE-Datenbank und Informatica befinden. Informationen zur Überprüfung der Kompatibilität erhalten Sie von Sybase.

Wenn Sie ein Sybase ASE-Repository erstellen, wiederherstellen oder upgraden möchten, setzen Sie *Nullen standardmäßig zulassen* auf der Datenbankebene auf TRUE Hiermit wird der Standard-Nulltyp der Spalte entsprechend dem SQL-Standard in Null geändert.

Konfigurieren von nativer Konnektivität

Sie können native Konnektivität für eine Sybase ASE-Datenbank konfigurieren, um die Leistung zu erhöhen.

Die folgenden Schritte stellen eine Richtlinie zum Konfigurieren der nativen Konnektivität dar. Spezifische Anweisungen finden Sie in der Dokumentation zur Datenbank.

1. Um die Konnektivität für den Datenintegrationsdienst-, PowerCenter-Integrationsdienst- oder PowerCenter-Repository-Dienst-Prozess zu konfigurieren, melden Sie sich am Computer als Benutzer an, der den Serverprozess starten kann.
2. Setzen Sie die Umgebungsvariablen SYBASE und PATH.

Sybase Legen Sie die Variable so fest, dass sie auf das Installationsverzeichnis von Sybase Open Client verweist. Wenn zum Beispiel der Client im Verzeichnis /usr/sybase installiert ist:

Bei Verwendung einer Bourne-Shell:

```
$ SYBASE=/usr/sybase; export SYBASE
```

Bei Verwendung einer C-Shell:

```
$ setenv SYBASE /usr/sybase
```

PATH. Zum Ausführen der Sybase-Befehlszeilenprogramme legen Sie die Variable so fest, dass sie das Sybase OCS-bin-Verzeichnis enthält.

Bei Verwendung einer Bourne-Shell:

```
$ PATH=${PATH}:/usr/sybase/OCS-15_0/bin; export PATH
```

Bei Verwendung einer C-Shell:

```
$ setenv PATH ${PATH}:/usr/sybase/OCS-15_0/bin
```

3. Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek fest.

   Die Sybase Open Client-Software enthält eine Reihe von gemeinsam genutzten Bibliothekskomponenten, die die Datenintegrationsdienst-, PowerCenter-Integrationsdienst- und PowerCenter-Repository-Dienst-Prozesse dynamisch laden. Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek so fest, dass die Dienste die gemeinsam genutzten Bibliotheken zur Laufzeit suchen können.

   Der Pfad der gemeinsam genutzten Bibliothek muss außerdem das Installationsverzeichnis der Informatica-Dienste *(server_dir)* enthalten.

   Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek basierend auf dem Betriebssystem fest.

   In der folgenden Tabelle werden die Variablen der gemeinsam genutzten Bibliothek für jedes Betriebssystem beschrieben.

Betriebssystem	Variable
Solaris	LD_LIBRARY_PATH
Linux	LD_LIBRARY_PATH
AIX	LIBPATH

   Benutzen Sie zum Beispiel die folgende Syntax für Solaris und Linux:

   - Bei Verwendung einer Bourne-Shell:

     ```
     $ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:$HOME/server_dir:$SYBASE/OCS-15_0/lib;
     $SYBASE/OCS-15_0/lib3p;$SYBASE/OCS-15_0/lib3p64; export LD_LIBRARY_PATH
     ```

   - Bei Verwendung einer C-Shell:

     ```
     $ setenv LD_LIBRARY_PATH ${LD_LIBRARY_PATH}:$HOME/server_dir:$SYBASE/OCS-15_0/lib;
     $SYBASE/OCS-15_0/lib3p;$SYBASE/OCS-15_0/lib3p64;
     ```

   Für AIX

   - Bei Verwendung einer Bourne-Shell:

     ```
     $ LIBPATH=${LIBPATH}:$HOME/server_dir:$SYBASE/OCS-15_0/lib;$SYBASE/OCS-15_0/lib3p;
     $SYBASE/OCS-15_0/lib3p64; export LIBPATH
     ```

   - Bei Verwendung einer C-Shell:

     ```
     $ setenv LIBPATH ${LIBPATH}:$HOME/server_dir:$SYBASE/OCS-15_0/lib;$SYBASE/
     OCS-15_0/lib3p;$SYBASE/OCS-15_0/lib3p64;
     ```

4. Bearbeiten Sie die .cshrc- oder die .profile-Datei, um den gesamten Satz der Shell-Befehle einzubeziehen. Speichern Sie die Datei und melden Sie sich entweder erneut an oder führen Sie den Quellbefehl aus.

   Bei Verwendung einer Bourne-Shell:

   ```
   $ source .profile
   ```

   Bei Verwendung einer C-Shell:

   ```
   $ source .cshrc
   ```

5. Überprüfen Sie den Sybase-ASE-Servernamen in der im Verzeichnis $SYBASE gespeicherten Sybase-Schnittstellendatei.
6. Prüfen Sie, ob Sie eine Verbindung zu der Sybase-ASE-Datenbank herstellen können.

   Um eine Verbindung zu der Sybase-ASE-Datenbank herzustellen, starten Sie ISQL und geben Sie dann die Konnektivitätsinformationen ein. Wenn Sie keine Verbindung zu der Datenbank herstellen können, vergewissern Sie sich, dass Sie alle Konnektivitäts-Informationen korrekt eingegeben haben.

   Bei Benutzernamen und Datenbanknamen bitte die Groß-/Kleinschreibung beachten.

Herstellen einer Verbindung zu einer Teradata-Datenbank über UNIX

Installieren und konfigurieren Sie native Clientsoftware auf den Computern, auf denen der Datenintegrationsdienst- oder PowerCenter-Integrationsdienst-Prozess ausgeführt wird. Verwenden Sie zur Gewährleistung der Kompatibilität zwischen Informatica und den Datenbanken die entsprechenden Datenbank-Client-Bibliotheken.

Installieren Sie den Teradata-Client, den Teradata-ODBC-Treiber sowie weitere eventuell benötigte Teradata-Client-Software auf dem Computer, auf dem der Datenintegrationsdienst oder der PowerCenter-Integrationsdienst ausgeführt wird. Außerdem müssen Sie die ODBC-Konnektivität konfigurieren.

Hinweis: Entsprechend einer Empfehlung von Teradata verwendet Informatica ODBC für die Verbindung mit Teradata. ODBC ist eine native Schnittstelle für Teradata.

Konfigurieren der ODBC-Konnektivität

Sie können ODBC-Konnektivität für eine Teradata-Datenbank konfigurieren.

Die folgenden Schritte enthalten eine Richtlinie zum Konfigurieren der ODBC-Konnektivität. Spezifische Anweisungen finden Sie in der Dokumentation zur Datenbank.

1. Um die Konnektivität für den Integration-Service-Prozess zu konfigurieren, melden Sie sich am Computer als Benutzer an, der einen Dienstprozess starten kann.
2. Setzen Sie die Umgebungsvariablen TERADATA_HOME, ODBCHOME und PATH.

   TERADATA_HOME. Legen Sie die Variable so fest, dass sie auf das Installationsverzeichnis des Teradata-Treibers verweist. Die Standardeinstellungen sind wie folgt:

   Bei Verwendung einer Bourne-Shell:

   ```
   $ TERADATA_HOME=/opt/teradata/client/<version>; export TERADATA_HOME
   ```

   Bei Verwendung einer C-Shell:

   ```
   $ setenv TERADATA_HOME /opt/teradata/client/<version>
   ```

ODBCHOME. Legen Sie die Variable so fest, dass sie auf das ODBC-Installationsverzeichnis verweist. Beispiel:

Bei Verwendung einer Bourne-Shell:

```
$ ODBCHOME=$INFA_HOME/ODBC<version>; export ODBCHOME
```

Bei Verwendung einer C-Shell:

```
$ setenv ODBCHOME $INFA_HOME/ODBC<version>
```

PATH. Um das Hilfsprogramm *ddtestlib* auszuführen, damit überprüft wird, ob der DataDirect ODBC-Treibermanager die Treiberdateien laden kann, legen Sie die Variable folgendermaßen fest:

Bei Verwendung einer Bourne-Shell:

```
PATH="${PATH}:$ODBCHOME/bin:$TERADATA_HOME/bin"
```

Bei Verwendung einer C-Shell:

```
$ setenv PATH ${PATH}:$ODBCHOME/bin:$TERADATA_HOME/bin
```

3. Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek fest.

   Die Teradata-Clientsoftware enthält mehrere gemeinsam genutzte Bibliothekkomponenten, die der Integrationsdienst-Prozess dynamisch lädt. Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek so fest, dass die Dienste die gemeinsam genutzten Bibliotheken zur Laufzeit suchen können.

   Der Pfad der gemeinsam genutzten Bibliothek muss außerdem das Installationsverzeichnis des Informatica-Dienstes *(server_dir)* enthalten.

   Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek basierend auf dem Betriebssystem fest.

   In der folgenden Tabelle werden die Variablen der gemeinsam genutzten Bibliothek für jedes Betriebssystem beschrieben:

Betriebssystem	Variable
Solaris	LD_LIBRARY_PATH
Linux	LD_LIBRARY_PATH
AIX	LIBPATH

   Benutzen Sie zum Beispiel die folgende Syntax für Solaris und Linux:

   - Bei Verwendung einer Bourne-Shell:

     ```
     $ LD_LIBRARY_PATH="${LD_LIBRARY_PATH}:$HOME/server_dir:$ODBCHOME/lib:

     $TERADATA_HOME/lib64:$TERADATA_HOME/odbc_64/lib";

     export LD_LIBRARY_PATH
     ```

   - Bei Verwendung einer C-Shell:

     ```
     $ setenv LD_LIBRARY_PATH "${LD_LIBRARY_PATH}:$HOME/server_dir:$ODBCHOME/lib:
     $TERADATA_HOME/lib64:

     $TERADATA_HOME/odbc_64/lib"
     ```

   Für AIX

   - Bei Verwendung einer Bourne-Shell:

     ```
     $ LIBPATH=${LIBPATH}:$HOME/server_dir:$ODBCHOME/lib:$TERADATA_HOME/
     lib64:$TERADATA_HOME/odbc_64/lib; export LIBPATH
     ```

- Bei Verwendung einer C-Shell:

```
$ setenv LIBPATH ${LIBPATH}:$HOME/server_dir:$ODBCHOME/lib:$TERADATA_HOME/lib64:
$TERADATA_HOME/odbc_64/lib
```

4. Bearbeiten Sie die vorhandene odbc.ini-Datei oder kopieren Sie die odbc.ini-Datei in das Basisverzeichnis und bearbeiten Sie sie.

   Die Datei befindet sich im Verzeichnis $ODBCHOME.

```
$ cp $ODBCHOME/odbc.ini $HOME/.odbc.ini
```

   Fügen Sie einen Eintrag zu der Teradata-Datenquelle unter dem Abschnitt [ODBC-Datenquellen] hinzu und konfigurieren Sie die Datenquelle.

   Beispiel:

```
MY_TERADATA_SOURCE=Teradata Driver
[MY_TERADATA_SOURCE]
Driver=/u01/app/teradata/td-tuf611/odbc/drivers/tdata.so
Description=NCR 3600 running Teradata V1R5.2
DBCName=208.199.59.208
DateTimeFormat=AAA
SessionMode=ANSI
DefaultDatabase=
Username=
Password=
```

5. Setzen Sie das DateTimeFormat in der Teradata-Daten-ODBC-Konfiguration auf AAA.
6. Optional können Sie den SessionMode auf ANSI setzen. Wenn Sie den ANSI-Sitzungsmodus verwenden, führt Teradata bei einem Zeilenfehler kein Rollback der Transaktion aus.

   Wenn Sie den Teradata-Sitzungsmodus verwenden, führt Teradata bei einem Zeilenfehler ein Rollback der Transaktion aus. Der Integration-Service-Prozess kann im Teradata-Modus das Rollback nicht entdecken und meldet dies nicht im Sitzungs-Log.
7. Um eine Verbindung zu einer einzelnen Teradata-Datenbank zu konfigurieren, geben Sie den Namen der Standarddatenbank ein. Um eine einzelne Verbindung zu der Standard-Datenbank herzustellen, geben Sie den Benutzernamen und das Passwort ein. Lassen Sie das Feld für die Standarddatenbank leer, um eine Verbindung zu mehreren Datenbanken mit dem gleichen ODBC-DSN herzustellen.

   Weitere Informationen zur Teradata-Konnektivität finden Sie in der Teradata-ODBC-Treiber-Dokumentation.
8. Prüfen Sie, ob der letzte Eintrag in der odbc.ini-Datei InstallDir ist und lassen Sie ihn auf das ODBC-Installationsverzeichnis verweisen.

   Beispiel:

```
InstallDir=<Informatica installation directory>/ODBC<version>
```

9. Bearbeiten Sie die .cshrc- oder die .profile-Datei, um den gesamten Satz der Shell-Befehle einzubeziehen.
10. Speichern Sie die Datei und melden Sie sich entweder erneut an oder führen Sie den Quellbefehl aus.

    Bei Verwendung einer Bourne-Shell:

```
$ source .profile
```

    Bei Verwendung einer C-Shell:

```
$ source .cshrc
```

11. Machen Sie sich für jede Datenquelle, die Sie verwenden, eine Notiz des Dateinamens unter „Driver=<parameter>“ in dem Datenquelleneintrag in odbc.ini. Verwenden Sie das Hilfsprogramm *ddtestlib*, um sicherzustellen, dass der DataDirect ODBC-Treibermanager die Treiberdatei laden kann.

    Sie haben zum Beispiel den Treibereintrag:

```
Driver=/u01/app/teradata/td-tuf611/odbc/drivers/tdata.so
```

Führen Sie den folgenden Befehl aus:

```
ddtestlib /u01/app/teradata/td-tuf611/odbc/drivers/tdata.so
```

12. Testen Sie die Verbindung mit BTEQ oder einem anderen Teradata-Client-Tool.

Herstellen einer Verbindung zu einer ODBC-Datenquelle

Installieren und konfigurieren Sie native Clientsoftware auf dem Computer, auf dem der Datenintegrationsdienst, PowerCenter-Integrationsdienst und PowerCenter-Repository-Dienst ausgeführt werden. Installieren und konfigurieren Sie außerdem die zugrunde liegende Clientzugriff-Software, die der ODBC-Treiber benötigt. Um die Kompatibilität zwischen Informatica und den Datenbanken sicherzustellen, verwenden Sie die entsprechenden Datenbank-Client-Bibliotheken.

Die Informatica-Installation beinhaltet DataDirect ODBC-Treiber. Wenn die odbc.ini-Datei Verbindungen enthält, die frühere Versionen des ODBC-Treibers verwenden, aktualisieren Sie die Verbindungsinformationen, um die neuen Treiber zu verwenden. Verwenden Sie System-DSN, um eine ODBC-Datenquelle unter Windows anzugeben.

1. Melden Sie sich am Computer, auf dem der Anwendungsdienst ausgeführt wird, als Benutzer an, der einen Dienstprozess starten kann.
2. Legen Sie die Umgebungsvariablen ODBCHOME und PATH fest.

   ODBCHOME. Legen Sie die Variablen für das DataDirect ODBC-Installationsverzeichnis fest. Wenn das Verzeichnis beispielsweise folgendermaßen lautet: `/export/home/Informatica/10.0.0/ODBC7.1`.

   Bei Verwendung einer Bourne-Shell:

   ```
   $ ODBCHOME=/export/home/Informatica/10.0.0/ODBC7.1; export ODBCHOME
   ```

   Bei Verwendung einer C-Shell:

   ```
   $ setenv ODBCHOME /export/home/Informatica/10.0.0/ODBC7.1
   ```

   PATH. Zum Ausführen der ODBC-Befehlszeilenprogramme, z. B. *ddtestlib*, legen Sie die Variable so fest, dass sie das ODBC-bin-Verzeichnis enthält.

   Bei Verwendung einer Bourne-Shell:

   ```
   $ PATH=${PATH}:$ODBCHOME/bin; export PATH
   ```

   Bei Verwendung einer C-Shell:

   ```
   $ setenv PATH ${PATH}:$ODBCHOME/bin
   ```

   Führen Sie das Hilfsprogramm *ddtestlib* aus, um sicherzustellen, dass der DataDirect ODBC-Treibermanager die Treiberdateien laden kann.
3. Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek fest.

   Die ODBC-Clientsoftware enthält eine Reihe von gemeinsam genutzten Bibliothekkomponenten, die die Dienstprozesse dynamisch laden. Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek so fest, dass die Dienste die gemeinsam genutzten Bibliotheken zur Laufzeit suchen können.

   Der Pfad der gemeinsam genutzten Bibliothek muss außerdem das Informatica-Installationsverzeichnis *(server_dir)* enthalten.

   Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek basierend auf dem Betriebssystem fest.

In der folgenden Tabelle werden die Variablen der gemeinsam genutzten Bibliothek für jedes Betriebssystem beschrieben:

Betriebssystem	Variable
Solaris	LD_LIBRARY_PATH
Linux	LD_LIBRARY_PATH
AIX	LIBPATH

Benutzen Sie zum Beispiel die folgende Syntax für Solaris und Linux:

- Bei Verwendung einer Bourne-Shell:

  ```
  $ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:$HOME/server_dir:$ODBCHOME/lib; export
  LD_LIBRARY_PATH
  ```

- Bei Verwendung einer C-Shell:

  ```
  $ setenv LD_LIBRARY_PATH $HOME/server_dir:$ODBCHOME:${LD_LIBRARY_PATH}
  ```

Für AIX

- Bei Verwendung einer Bourne-Shell:

  ```
  $ LIBPATH=${LIBPATH}:$HOME/server_dir:$ODBCHOME/lib; export LIBPATH
  ```

- Bei Verwendung einer C-Shell:

  ```
  $ setenv LIBPATH ${LIBPATH}:$HOME/server_dir:$ODBCHOME/lib
  ```

4. Bearbeiten Sie die vorhandene odbc.ini-Datei oder kopieren Sie die odbc.ini-Datei in das Basisverzeichnis und bearbeiten Sie sie.

   Die Datei befindet sich im Verzeichnis $ODBCHOME.

   ```
   $ cp $ODBCHOME/odbc.ini $HOME/.odbc.ini
   ```

   Fügen Sie einen Eintrag zu der ODBC-Datenquelle unter dem Abschnitt [ODBC Data Sources] hinzu und konfigurieren Sie die Datenquelle.

   Beispiel:

   ```
   MY_MSSQLSERVER_ODBC_SOURCE=<Driver name or data source description>
   [MY_SQLSERVER_ODBC_SOURCE]
   Driver=<path to ODBC drivers>
   Description=DataDirect 7.1 SQL Server Wire Protocol
   Database=<SQLServer_database_name>
   LogonID=<username>
   Password=<password>
   Address=<TCP/IP address>,<port number>
   QuoteId=No
   AnsiNPW=No
   ApplicationsUsingThreads=1
   ```

   Diese Datei existiert möglicherweise bereits, wenn Sie eine oder mehrere ODBC-Datenquellen konfiguriert haben.

5. Prüfen Sie, ob der letzte Eintrag in der odbc.ini-Datei InstallDir ist und lassen Sie ihn auf das ODBC-Installationsverzeichnis verweisen.

   Beispiel:

   ```
   InstallDir=/export/home/Informatica/10.0.0/ODBC7.1
   ```

6. Wenn Sie die odbc.ini-Datei im Basisverzeichnis verwenden, setzen Sie die Umgebungsvariable ODBCINI.

   Bei Verwendung einer Bourne-Shell:

   ```
   $ ODBCINI=/$HOME/.odbc.ini; export ODBCINI
   ```

Bei Verwendung einer C-Shell:

```
$ setenv ODBCINI $HOME/.odbc.ini
```

7. Bearbeiten Sie die .cshrc- oder die .profile-Datei, um den gesamten Satz der Shell-Befehle einzubeziehen. Speichern Sie die Datei und melden Sie sich entweder erneut an oder führen Sie den Quellbefehl aus.

   Bei Verwendung einer Bourne-Shell:

   ```
   $ source .profile
   ```

   Bei Verwendung einer C-Shell:

   ```
   $ source .cshrc
   ```

8. Verwenden Sie das Hilfsprogramm *ddtestlib*, um zu überprüfen, ob der DataDirect ODBC-Treibermanager die Treiberdatei laden kann, die Sie für die Datenquelle in der Datei „odbc.ini“ festgelegt haben.

   Sie haben zum Beispiel den Treibereintrag:

   ```
   Driver = /export/home/Informatica/10.0.0/ODBC7.1/lib/DWxxxxnn.so
   ```

   Führen Sie den folgenden Befehl aus:

   ```
   ddtestlib /export/home/Informatica/10.0.0/ODBC7.1/lib/DWxxxxnn.so
   ```

9. Installieren und konfigurieren Sie jede zugrunde liegende Clientzugriffs-Software, die der ODBC-Treiber benötigt.

   Hinweis: Einige ODBC-Treiber sind eigenständig und haben alle Informationen in der odbc.ini-Datei; bei den meisten ist dies jedoch nicht der Fall. Wenn Sie beispielsweise einen ODBC-Treiber verwenden möchten, um auf Sybase IQ zuzugreifen, müssen Sie Sybase IQ Netzwerk-Clientsoftware installieren und die entsprechenden Umgebungsvariablen setzen.

   Legen Sie zur Verwendung der Informatica ODBC-Treiber (DWxxxxnn.so) die Umgebungsvariablen für PATH und gemeinsam genutzte Bibliothekspfade manuell fest. Führen Sie alternativ das Skript „odbc.sh“ oder das Skript „odbc.csh“ im Ordner $ODBCHOME aus. Dieses Skript richtet die erforderlichen Umgebungsvariablen für PATH und gemeinsam genutzte Bibliothekspfade für die ODBC-Treiber ein, die von Informatica bereitgestellt werden.

odbc.ini-Beispieldatei

Das folgende Beispiel zeigt die Einträge für die ODBC-Treiber in der Datei ODBC.ini:

```
[ODBC Data Sources]
SQL Server Legacy Wire Protocol=DataDirect 7.1 SQL Server Legacy Wire Protocol
DB2 Wire Protocol=DataDirect 7.1 DB2 Wire Protocol
Informix Wire Protocol=DataDirect 7.1 Informix Wire Protocol
Oracle Wire Protocol=DataDirect 7.1 Oracle Wire Protocol
Sybase Wire Protocol=DataDirect 7.1 Sybase Wire Protocol
SQL Server Wire Protocol=DataDirect 7.1 SQL Server Wire Protocol
MySQL Wire Protocol=DataDirect 7.1 MySQL Wire Protocol
PostgreSQL Wire Protocol=DataDirect 7.1 PostgreSQL Wire Protocol
Greenplum Wire Protocol=DataDirect 7.1 Greenplum Wire Protocol

[ODBC]
IANAAppCodePage=4
InstallDir=/<Informatica installation directory>/ODBC7.1
Trace=0
TraceFile=odbctrace.out
TraceDll=/<Informatica installation directory>/ODBC7.1/lib/DWtrc27.so

[DB2 Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWdb227.so
Description=DataDirect 7.1 DB2 Wire Protocol
AccountingInfo=
AddStringToCreateTable=
```

```
AlternateID=
AlternateServers=
ApplicationName=
ApplicationUsingThreads=1
AuthenticationMethod=0
BulkBinaryThreshold=32
BulkCharacterThreshold=-1
BulkLoadBatchSize=1024
BulkLoadFieldDelimiter=
BulkLoadRecordDelimiter=
CatalogSchema=
CharsetFor65535=0
ClientHostName=
ClientUser=
#Collection applies to z/OS and iSeries only
Collection=
ConcurrentAccessResolution=0
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
CurrentFuncPath=
#Database applies to DB2 UDB only
Database=<database_name>
DefaultIsolationLevel=1
DynamicSections=1000
EnableBulkLoad=0
EncryptionMethod=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
GrantAuthid=PUBLIC
GrantExecute=1
GSSClient=native
HostNameInCertificate=
IpAddress=<DB2_server_host>
KeyPassword=
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
#Location applies to z/OS and iSeries only
Location=<location_name>
LogonID=
MaxPoolSize=100
MinPoolSize=0
Password=
PackageCollection=NULLID
PackageNamePrefix=DD
PackageOwner=
Pooling=0
ProgramID=
QueryTimeout=0
ReportCodePageConversionErrors=0
TcpPort=50000
TrustStore=
TrustStorePassword=
UseCurrentSchema=0
ValidateServerCertificate=1
WithHold=1
XMLDescribeType=-10

[Informix Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWifcl27.so
Description=DataDirect 7.1 Informix Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
CancelDetectInterval=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
HostName=<Informix_host>
```

```
LoadBalancing=0
LogonID=
Password=
PortNumber=<Informix_server_port>
ServerName=<Informix_server>
TrimBlankFromIndexName=1
UseDelimitedIdentifiers=0

[Oracle Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWora27.so
Description=DataDirect 7.1 Oracle Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
AccountingInfo=
Action=
ApplicationName=
ArraySize=60000
AuthenticationMethod=1
BulkBinaryThreshold=32
BulkCharacterThreshold=-1
BulkLoadBatchSize=1024
BulkLoadFieldDelimiter=
BulkLoadRecordDelimiter=
CachedCursorLimit=32
CachedDescLimit=0
CatalogIncludesSynonyms=1
CatalogOptions=0
ClientHostName=
ClientID=
ClientUser=
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
DataIntegrityLevel=0
DataIntegrityTypes=MD5,SHA1
DefaultLongDataBuffLen=1024
DescribeAtPrepare=0
EditionName=
EnableBulkLoad=0
EnableDescribeParam=0
EnableNcharSupport=0
EnableScrollableCursors=1
EnableStaticCursorsForLongData=0
EnableTimestampWithTimeZone=0
EncryptionLevel=0
EncryptionMethod=0
EncryptionTypes=AES128,AES192,AES256,DES,3DES112,3DES168,RC4_40,RC4_56,RC4_128,
RC4_256
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
FetchTSWTZasTimestamp=0
GSSClient=native
HostName=<Oracle_server>
HostNameInCertificate=
InitializationString=
KeyPassword=
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
LocalTimeZoneOffset=
LockTimeOut=-1
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
Module=
Password=
Pooling=0
PortNumber=<Oracle_server_port>
```

```
ProcedureRetResults=0
ProgramID=
QueryTimeout=0
ReportCodePageConversionErrors=0
ReportRecycleBin=0
ServerName=<server_name in tnsnames.ora>
ServerType=0
ServiceName=
SID=<Oracle_System_Identifier>
TimestampeEscapeMapping=0
TNSNamesFile=<tnsnames.ora_filename>
TrustStore=
TrustStorePassword=
UseCurrentSchema=1
ValidateServerCertificate=1
WireProtocolMode=2

[Sybase Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWase27.so
Description=DataDirect 7.1 Sybase Wire Protocol
AlternateServers=
ApplicationName=
ApplicationUsingThreads=1
ArraySize=50
AuthenticationMethod=0
BulkBinaryThreshold=32
BulkCharacterThreshold=-1
BulkLoadBatchSize=1024
BulkLoadFieldDelimiter=
BulkLoadRecordDelimiter=
Charset=
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
CursorCacheSize=1
Database=<database_name>
DefaultLongDataBuffLen=1024
EnableBulkLoad=0
EnableDescribeParam=0
EnableQuotedIdentifiers=0
EncryptionMethod=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
GSSClient=native
HostNameInCertificate=
InitializationString=
Language=
LoadBalancing=0
LoadBalanceTimeout=0
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
NetworkAddress=<Sybase_host,Sybase_server_port>
OptimizePrepare=1
PacketSize=0
Password=
Pooling=0
QueryTimeout=0
RaiseErrorPositionBehavior=0
ReportCodePageConversionErrors=0
SelectMethod=0
ServicePrincipalName=
TruncateTimeTypeFractions=0
TrustStore=
TrustStorePassword=
ValidateServerCertificate=1
WorkStationID=

[SQL Server Wire Protocol]
```

```
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWsqls27.so
Description=DataDirect 7.1 SQL Server Wire Protocol
AlternateServers=
AlwaysReportTriggerResults=0
AnsiNPW=1
ApplicationName=
ApplicationUsingThreads=1
AuthenticationMethod=1
BulkBinaryThreshold=32
BulkCharacterThreshold=-1
BulkLoadBatchSize=1024
BulkLoadOptions=2
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
EnableBulkLoad=0
EnableQuotedIdentifiers=0
EncryptionMethod=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
FetchTSWTZasTimestamp=0
FetchTWFSasTime=1
GSSClient=native
HostName=<SQL_Server_host>
HostNameInCertificate=
InitializationString=
Language=
LoadBalanceTimeout=0
LoadBalancing=0
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
PacketSize=-1
Password=
Pooling=0
PortNumber=<SQL_Server_server_port>
QueryTimeout=0
ReportCodePageConversionErrors=0
SnapshotSerializable=0
TrustStore=
TrustStorePassword=
ValidateServerCertificate=1
WorkStationID=
XML Describe Type=-10

[MySQL Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWmysql27.so
Description=DataDirect 7.1 MySQL Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
DefaultLongDataBuffLen=1024
EnableDescribeParam=0
EncryptionMethod=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
HostName=<MySQL_host>
HostNameInCertificate=
InteractiveClient=0
LicenseNotice=You must purchase commercially licensed MySQL database software or
a MySQL Enterprise subscription in order to use the DataDirect Connect for ODBC
for MySQL Enterprise driver with MySQL software.
KeyStore=
KeyStorePassword=
```

```
LoadBalanceTimeout=0
LoadBalancing=0
LogonID=
LoginTimeout=15
MaxPoolSize=100
MinPoolSize=0
Password=
Pooling=0
PortNumber=<MySQL_server_port>
QueryTimeout=0
ReportCodepageConversionErrors=0
TreatBinaryAsChar=0
TrustStore=
TrustStorePassword=
ValidateServerCertificate=1

[PostgreSQL Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWpsql27.so
Description=DataDirect 7.1 PostgreSQL Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
DefaultLongDataBuffLen=2048
EnableDescribeParam=1
EncryptionMethod=0
ExtendedColumnMetadata=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
FetchTSWTZasTimestamp=0
FetchTWFSasTime=0
HostName=<PostgreSQL_host>
HostNameInCertificate=
InitializationString=
KeyPassword=
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
Password=
Pooling=0
PortNumber=<PostgreSQL_server_port>
QueryTimeout=0
ReportCodepageConversionErrors=0
TransactionErrorBehavior=1
TrustStore=
TrustStorePassword=
ValidateServerCertificate=1
XMLDescribeType=-10

[Greenplum Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWgplm27.so
Description=DataDirect 7.1 Greenplum Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
DefaultLongDataBuffLen=2048
EnableDescribeParam=0
EnableKeysetCursors=0
EncryptionMethod=0
ExtendedColumnMetadata=0
```

```
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
FetchTSWTZasTimestamp=0
FetchTWFSasTime=0
HostName=<Greenplum_host>
InitializationString=
KeyPassword=
KeysetCursorOptions=0
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
Password=
Pooling=0
PortNumber=<Greenplum_server_port>
QueryTimeout=0
ReportCodepageConversionErrors=0
TransactionErrorBehavior=1
XMLDescribeType=-10

[SQL Server Legacy Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWmsss27.so
Description=DataDirect 7.1 SQL Server Legacy Wire Protocol
Address=<SQLServer_host, SQLServer_server_port>
AlternateServers=
AnsiNPW=Yes
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
FetchTSWTZasTimestamp=0
FetchTWFSasTime=0
LoadBalancing=0
LogonID=
Password=
QuotedId=No
ReportCodepageConversionErrors=0
SnapshotSerializable=0
```

ANHANG D

Aktualisieren des DynamicSections-Parameters einer DB2-Datenbank

Dieser Anhang umfasst die folgenden Themen:

- DynamicSections-Parameter - Übersicht, 285
- Aktualisieren des DynamicSections-Parameters, 285

DynamicSections-Parameter - Übersicht

IBM DB2-Pakete enthalten die SQL-Anweisungen, die auf dem Datenbankserver ausgeführt werden sollen. Mit dem Parameter DynamicSections einer DB2-Datenbank wird die Höchstzahl der ausführbaren Anweisungen festgelegt die es für einen Datenbanktreiber in einem Paket geben darf Sie können den Wert des Parameters DynamicSections erhöhen, um eine größere Anzahl ausführbarer Anweisungen in einem DB2-Paket zu ermöglichen. Zum Ändern des Parameters DynamicSections stellen Sie mit einem Systemadministrator-Benutzerkonto mit BINDADD-Berechtigung eine Verbindung zur Datenbank her.

Aktualisieren des DynamicSections-Parameters

Verwenden Sie das Dienstprogramm DataDirect Connect für JDBC, um den Wert des DynamicSections-Parameters in der DB2-Datenbank zu erhöhen.

Gehen Sie zum Aktualisieren des DynamicSections-Parameters mithilfe des Dienstprogramms DataDirect Connect für JDBC folgendermaßen vor:

- Laden Sie das Dienstprogramm DataDirect Connect für JDBC herunter und installieren Sie es.
- Führen Sie den Test für das JDBC-Tool aus.

Herunterladen und Installieren des Dienstprogramms DataDirect Connect für JDBC

Laden Sie das Dienstprogramm DataDirect Connect für JDBC von der DataDirect-Download-Website auf einen Rechner herunter, der auf den DB2-Datenbankserver zugreifen kann. Extrahieren Sie den Inhalt des Dienstprogramms und führen Sie das Installationsprogramm aus.

1. Wechseln Sie zur DataDirect-Download-Site: http://www.datadirect.com/support/product-documentation/downloads
2. Wählen Sie den Treiber Connect für JDBC für eine IBM DB2-Datenquelle aus.
3. Registrieren Sie sich, um das Dienstprogramm DataDirect Connect für JDBC herunterzuladen.
4. Laden Sie das Dienstprogramm auf einen Computer herunter, der auf den DB2-Datenbankserver zugreifen kann.
5. Extrahieren Sie den Inhalt des Dienstprogramms in ein temporäres Verzeichnis.
6. Führen Sie in dem Verzeichnis, in dem Sie die Datei extrahiert haben, das Installationsprogramm aus.

Das Installationsprogramm erstellt einen Ordner mit dem Namen „testforjdbc“ im Installationsverzeichnis.

Ausführen des Test für JDBC-Tools

Führen Sie nach dem Installieren des Dienstprogramms DataDirect Connect für JDBC das Test für JDBC-Tool aus, um eine Verbindung zur DB2-Datenbank herzustellen. Zum Herstellen einer Verbindung zur Datenbank müssen Sie das Systemadministrator-Benutzerkonto mit der BINDADD-Berechtigung verwenden.

1. Richten Sie in der DB2-Datenbank ein Systemadministrator-Benutzerkonto mit der BINDADD-Berechtigung ein.
2. Führen Sie im Verzeichnis,in dem Sie das Dienstprogramm DataDirect Connect für JDBC installiert haben, den Test für das JDBC-Tool aus.

   Führen Sie unter Windows testforjdbc.bat aus. Führen Sie unter UNIX testforjdbc.sh aus.
3. Klicken Sie im Fenster zum Test für das JDBC-Tool auf "Zum Fortsetzen hier klicken".
4. Klicken Sie auf Verbindung > Zu DB verbinden.
5. Geben Sie in das Datenbank-Feld den folgenden Text ein:

   ```
   jdbc:datadirect:db2:// HostName:PortNumber;databaseName=DatabaseName;CreateDefaultPackage=TRUE;ReplacePackage=TRUE;DynamicSections=3000
   ```

   HostName stellt den Namen des Rechners dar, auf dem sich der DB2-Datenbankserver befindet.

   PortNumber stellt die Portnummer der Datenbank dar.

   DatabaseName stellt den Namen der DB2-Datenbank dar.
6. Geben Sie in die Felder für den Benutzernamen und das Passwort den Systemadministrator-Benutzernamen und das Passwort ein, das Sie zum Verbinden mit der DB2-Datenbank verwenden.
7. Klicken Sie auf "Verbinden" und schließen Sie anschließend das Fenster.

ANHANG E

Konfiguration einer geteilten Domäne für Metadata Manager

Dieser Anhang umfasst die folgenden Themen:

- Konfiguration einer geteilten Domäne für Metadata Manager - Übersicht, 287
- Geteilte Domäne - Beispiel, 288
- Konfiguration der Anwendungsdienste, 289
- Produktinstallation für eine geteilte Domäne, 289

Konfiguration einer geteilten Domäne für Metadata Manager - Übersicht

In einer geteilten Domäne werden die mit den Hauptkomponenten Ihres Produktpakets verknüpften Anwendungsdienste in einer Domäne ausgeführt und die mit Metadata Manager verknüpften Anwendungsdienste in einer anderen, sekundären Domäne. Sie können beide Domänen auf demselben Computer oder auf verschiedenen Computern erstellen.

Ihr Produktpaket umfasst beispielsweise PowerCenter und Metadata Manager. In einer geteilten Domäne werden die Anwendungsdienste, die Sie zum Durchführen von Datenintegrationsvorgängen mit PowerCenter verwenden, in der Hauptdomäne ausgeführt. Deshalb enthält die Hauptdomäne einen PowerCenter-Repository-Dienst und einen PowerCenter-Integrationsdienst.

Die Anwendungsdienste, die Sie zum Durchführen einer Metadatenextraktion mit Metadata Manager verwenden, werden in der sekundären Domäne ausgeführt. Deshalb enthält die sekundäre Domäne einen Metadata Manager-Dienst. Sie enthält außerdem einen separaten PowerCenter-Repository-Dienst und einen PowerCenter-Integrationsdienst, die Metadatenextraktionsvorgänge unterstützen, für Datenintegrationsvorgänge aber nicht verwendet werden.

Wenn Sie eine geteilte Domäne erstellen, müssen Sie bestimmte Repositorys doppelt erstellen. Sie müssen beispielsweise ein separates Domänenkonfigurations-Repository in jeder Domäne erstellen. Wenn Ihr Produktpaket PowerCenter und Metadata Manager enthält, müssen Sie außerdem ein separates PowerCenter-Repository in jeder Domäne erstellen. Sie müssen jedes Repository in einem separaten Datenbankschema erstellen.

Hinweis: Unter Umständen beschränkt Ihre Lizenz die duplizierbaren Anwendungsdienste sowie alle Produktkomponenten, die in den Domänen ausgeführt werden. Wenn sich das Produktpaket beispielsweise aus PowerCenter und Metadata Manager zusammensetzt, können Sie Datenintegrationsvorgänge nicht in

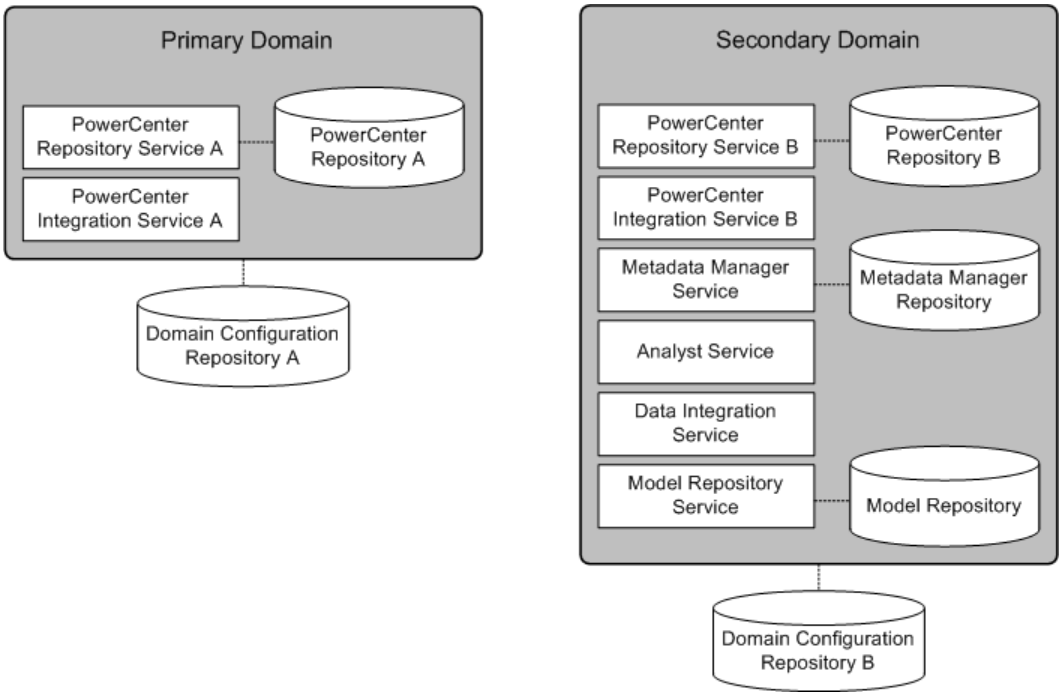
beiden Domänen ausführen. Bei Fragen zur Konfiguration einer geteilten Domäne ohne Verletzung des Lizenzvertrags wenden Sie sich an einen Vertreter für Informatica-Produkte.

Geteilte Domäne - Beispiel

Konfigurieren Sie eine geteilte Domäne, wenn Sie Metadata Manager verwenden und aktualisieren möchten, ohne andere Komponenten im Produktpaket zu aktualisieren.

Im Lieferumfang Ihres Produktpakets befinden sich beispielsweise PowerCenter, Metadata Manager und Informatica Analyst (Analyst Tool). Sie verwenden PowerCenter für die Datenintegration. Sie verwenden Metadata Manager für die Metadatenextraktion und Datenverlaufskontrolle. Sie verwenden das Analyst Tool zum Erstellen und Verwalten von Unternehmensglossaren.

Die folgende Abbildung zeigt die Konfiguration für jede Domäne:



In dieser Konfiguration werden alle Datenintegrationsvorgänge in der Hauptdomäne durchgeführt. Die PowerCenter-Dienste in der sekundären Domäne unterstützen die Metadata Manager-Arbeitsabläufe, bei denen Metadaten extrahiert und in das Metadata Manager-Repository geladen werden. Sie können die PowerCenter-Dienste in der sekundären Domäne nicht für die Datenintegration verwenden. Der Analyst-, Datenintegrations- und Modellrepository-Dienst in der sekundären Domäne unterstützen die Erstellung und Verwaltung von Unternehmensglossaren. Sie können diese Dienste nicht für die Datenintegration verwenden.

Konfiguration der Anwendungsdienste

Wenn Sie eine geteilte Domäne für Metadata Manager konfigurieren, gehen die von Ihnen erstellten Anwendungsdienste möglicherweise in eine Domäne oder in beide Domänen.

In der folgenden Tabelle finden Sie eine Auflistung der Anwendungsdienste, die Sie konfigurieren können, und der Domänen, in denen dies möglich ist:

Dienste	Domänen
Analyst-Dienst, Datenintegrationsdienst, Modellrepository-Dienst	Konfigurieren Sie diese Dienste in den folgenden Domänen: - Primäre Domäne, wenn Sie diese Dienste für die Datenintegration verwenden - Sekundäre Domäne, wenn Sie keine Datenintegrationsvorgänge durchführen, jedoch Geschäftsglossare verwenden oder die Datenherkunft für Scorecards ausführen - Beide Domänen, wenn Sie die Datenintegration in der primären Domäne durchführen und Geschäftsglossare in der sekundären Domäne verwenden **Hinweis:** Sie können in der sekundären Domäne keine Datenintegration durchführen, und Sie können in der primären Domäne keine Geschäftsglossare erstellen.
Content-Management-Dienst, Suchdienst	Konfigurieren Sie diese Dienste in derselben Domäne wie den Datenintegrationsdienst und den Modellrepository-Dienst.
Metadata Manager-Dienst	Konfigurieren Sie diesen Dienst in der sekundären Domäne.
PowerCenter-Integrationsdienst, PowerCenter-Repository-Dienst	Konfigurieren Sie diese Dienste in beiden Domänen. **Hinweis:** In der sekundären Domäne können Sie diese Dienste für die Datenintegration nicht verwenden.
Webdienst-Hub	Konfigurieren Sie diesen Dienst in der primären Domäne.

Produktinstallation für eine geteilte Domäne

Beim Konfigurieren einer geteilten Domäne führen Sie das Installationsprogramm der Informatica-Dienste jedes Mal aus, wenn Sie eine Domäne erstellen. Wenn Sie eine Domäne erstellen, konfigurieren Sie die Benutzerauthentifizierungsmethode und das Sicherheitsprotokoll und erstellen Sie das Domänenkonfigurations-Repository. Anschließend erstellen Sie die erforderlichen Benutzer und Gruppen in der Domäne.

Sie können die Domänen auf einem oder auf zwei verschiedenen Computern erstellen. Wenn Sie die Domänen auf einem Computer erstellen, müssen Sie mögliche Konflikte beim Port, Knotennamen und Verzeichnis vermeiden.

Geben Sie bei der Installation der Informatica-Dienste die Benutzerauthentifizierungsmethode und das Sicherheitsprotokoll für die Domäne an. Jede Domäne kann eine andere Benutzerauthentifizierungsmethode und ein anderes Sicherheitsprotokoll aufweisen. Die Verwaltung der Domänen gestaltet sich jedoch einfacher, wenn die Benutzerauthentifizierungsmethoden und Sicherheitsprotokolle identisch sind.

Während der Installation erstellen Sie das Domänenkonfigurations-Repository. Sie müssen jedes Domänenkonfigurations-Repository in einem separaten Datenbankschema mit verschiedenen Benutzerkonten erstellen. Die Repositorys können sich in derselben Datenbankinstanz befinden.

Unter Umständen müssen Sie bestimmte Benutzer oder Gruppen in den verschiedenen Domänenkonfiguration-Repositorys doppelt erstellen. Wenn ein Benutzer beispielsweise PowerCenter-Zuordnungen in der Hauptdomäne erstellt und Metadata Manager für die Datenverlaufskontrolle in der sekundären Domäne verwendet, muss dieser Benutzer im Domänenkonfigurations-Repository beider Domänen vorhanden sein.

Vor der Installation einer geteilten Domäne durchzuführende Aufgaben

Überprüfen Sie vor der Installation der Informatica-Dienste in einer geteilten Domäne die Produktlizenz und erstellen Sie die erforderlichen Datenbankbenutzerkonten und -schemas.

Führen Sie die folgenden Aufgaben durch:

- Stellen Sie sicher, dass gemäß Lizenzvereinbarung die Duplizierung der benötigten Anwendungsdienste zulässig ist.
- Stellen Sie sicher, dass die Lizenzvereinbarung die zu implementierende Computerkonfiguration auf einem oder auf zwei Computern unterstützt.
- Wenn Sie für jede Domäne eine andere Lizenzdatei benötigen, stellen Sie sicher, dass beide Lizenzdateien verfügbar sind.
- Erstellen Sie ein zusätzliches Benutzerkonto für die Domänenkonfigurations-Repositorys der beiden Domänen.
- Erstellen Sie separate Datenbankschemas für die beiden Domänenkonfigurations-Repositorys und für andere duplizierte Repositorys.

Regeln und Richtlinien für Einzelcomputer

Wenn Sie beide Domänen auf einem Computer erstellen, müssen bestimmte Regeln und Richtlinien beachtet werden.

Beachten Sie die folgenden Regeln und Richtlinien:

- Der Computer muss über genügend Arbeits- und Festplattenspeicher verfügen, um die Anforderungen von zwei Installationen zu erfüllen.
- Das Installationsverzeichnis für jede Domäne muss eindeutig sein.

  Beispiel: `C:\Informatica\10.1.0_PC` und `C:\Informatica\10.1.0_MM`.
- Der Name für jede Domäne muss eindeutig sein.
- Sie müssen sicherstellen, dass keine Portkonflikte vorhanden sind.

  Wenn Sie beispielsweise den Standardknotenport 6005 in der Hauptdomäne übernehmen, müssen Sie einen anderen Knotenport in der sekundären Domäne angeben.
- Unter Windows müssen Sie einen der Windows-Dienste unter Umständen manuell starten.

  Wenn in den Domänen dieselben Haupt- und Nebenversionen, aber verschiedene Hotfixes verwendet werden, sind die Namen der Informatica-Dienste identisch. Deshalb startet Windows nur eine Instanz der Informatica-Dienste beim Start des Betriebssystems. Führen Sie zum Starten der anderen Instanz folgenden Befehl an der Eingabeaufforderung aus:

  ```
  <Informatica services installation directory>\tomcat\bin\infaservice.bat startup
  ```

ANHANG F

Installations- und Konfigurations-Checkliste

Dieser Anhang umfasst die folgenden Themen:

- Checkliste für die Installation - Übersicht, 291
- Planen der Domäne, 292
- Vorbereiten von Datenbanken für die Informatica-Domäne, 293
- Single Sign-On für Informatica-Webanwendungen, 294
- Vorbereiten der Kerberos-Authentifizierung, 294
- Vor der Installation der Dienste unter Windows, 294
- Vor der Installation von Diensten unter UNIX, 295
- Installation von Informatica-Diensten, 296
- Durchführen der Domänenkonfiguration, 296
- Vorbereiten zum Erstellen der Anwendungsdienste, 297
- Erstellen der Anwendungsdienste, 297
- Vor dem Installieren der Clients, 298
- Installieren der Clients, 298
- Nach dem Installieren der Informatica-Clients, 299

Checkliste für die Installation - Übersicht

Die Checkliste für die Installation und Konfiguration enthält eine Zusammenfassung der Aufgaben, die Sie durchführen müssen, um die Installation abzuschließen.

Planen der Domäne

Führen Sie zum Planen der Domäne die folgenden Aufgaben durch:

- ❑ Planen Sie die Anwendungsdienste, die in der Domäne ausgeführt werden sollen. Sie müssen außerdem die zugeordneten Dienste berücksichtigen, die eine Verbindung zum Anwendungsdienst und den relationalen Datenbanken herstellen, die für die Erstellung des Anwendungsdiensts erforderlich sind.
- ❑ Entscheiden Sie, ob Sie nur eine Domäne oder eine geteilte Domäne erstellen möchten. Möglicherweise ist es empfehlenswert, eine geteilte Domäne zu erstellen, sodass Sie Metadata Manager aktualisieren können, ohne die primären Komponenten Ihres Installationspakets gleichzeitig aktualisieren zu müssen.
- ❑ Erstellen Sie einen Plan für die folgenden Anwendungsdienste basierend auf dem Lizenzschlüssel, der für Ihr Unternehmen generiert wurde:
  - Analyst-Dienst
  - Content-Managementdienst
  - Datenintegrationsdienst
  - Metadata Manager-Dienst
  - Modellrepository-Dienst
  - PowerCenter-Integrationsdienst
  - PowerCenter-Repository-Dienst
  - Suchdienst
  - Webdienst-Hub
- ❑ Überprüfen Sie, ob Ihr System die Mindestsystemanforderungen für die Installation der Informatica-Dienste erfüllt.
- ❑ Stellen Sie sicher, dass für die Installation genügend Speicherplatz auf dem Computer vorhanden ist.
- ❑ Stellen Sie sicher, dass die zu verwendenden Portnummern für die Anwendungsdienstprozesse auf den Computern verfügbar sind, auf denen Sie die Informatica-Dienste installieren.
- ❑ Stellen Sie sicher, dass der Datenbankserver über ausreichend Speicherplatz für das Domänen-Konfigurations-Repository und für die anderen für die Anwendungsdienste erforderlichen Datenbanken verfügt.
- ❑ Stellen Sie sicher, dass die Knoten in der Domäne über ausreichend Hardware für den Dienstmanager und die Anwendungsdienste verfügen, die auf dem Knoten ausgeführt werden.
- ❑ Erfassen Sie die Informationen über die Domäne, Knoten und Anwendungsdienste, die Sie erstellen möchten.

Verwandte Themen:

- "Planen der Domäne" auf Seite 19

Vorbereiten von Datenbanken für die Informatica-Domäne

Führen Sie zur Vorbereitung der Datenbanken für die Informatica-Domäne die folgenden Aufgaben durch:

- ❑ Richten Sie eine Datenbank und das Benutzerkonto für das Domänen-Konfigurations-Repository und für die Repository-Datenbanken ein, die mit den Anwendungsdiensten verbunden sind.
- ❑ Überprüfen Sie die Datenbankanforderungen für die Datenbanken, die Sie benötigen:
  - Domänenkonfigurations-Repository. Speichert Konfigurations- und Benutzerinformationen in einem Domänen-Konfigurations-Repository.
  - Datenobjekt-Cache-Datenbank. Speichert zwischengespeicherte logische Datenobjekte und virtuelle Tabellen für den Datenintegrationsdienst.
  - Ausnahmeverwaltungs-Audit-Datenbank. Speichert Daten, die die Arbeit von Analyst-Tool-Benutzern an Human-Task-Instanzen beschreiben.
  - Metadata Manager-Repository. Speichert das Metadata Manager-Warehouse und Modelle.
  - Modellrepository. Speichert Daten und Metadaten, die zu den Informatica-Diensten und -Clients gehören.
  - PowerCenter-Repository. Speichert eine Sammlung von Datenbanktabellen, die Metadaten enthalten.
  - Profiling-Warehouse. Speichert die Profiling und Scorecard-Ergebnisse.
  - Referenzdaten-Warehouse. Speichert die Datenwerte für die Referenztabellenobjekte, die Sie im Modellrepository definieren.
  - Arbeitsablauf-Datenbank. Speichert Laufzeit-Metadaten für Arbeitsabläufe.
- ❑ Installieren Sie die Datenbank-Clients auf dem Computer, auf dem alle Dienste laufen basierend auf den Datenbanken, auf die der Dienst zugreift.
- ❑ Konfigurieren Sie die Datenbank-Client-Umgebungsvariablen auf den Computern, auf denen die folgenden Dienste ausgeführt werden:
  - Datenintegrationsdienst
  - PowerCenter-Integrationsdienst
  - PowerCenter-Repository-Dienst

Verwandte Themen:

- " Vorbereiten von Datenbanken für die Informatica-Domäne " auf Seite 49

Single Sign-On für Informatica-Webanwendungen

Um Single Sign-On für Informatica Web Applications zu aktivieren, führen Sie die folgenden Aufgaben aus:

- Erstellen Sie eine Sicherheitsdomäne für das Benutzerkonto der Webanwendung.
- Exportieren Sie das Assertionssignaturzertifikat aus AD FS.
- Importieren Sie das Assertionssignaturzertifikat in die Truststore-Standarddatei von Informatica auf allen Gateway-Knoten in der Informatica-Domäne.
- Konfigurieren Sie AD FS zur Ausgabe von SAML-Token an Informatica-Webanwendungen.
- Fügen Sie die URL für jede Informatica-Webanwendung mithilfe von Single Sign-On zu AD FS hinzu.
- Abrufen der Identity Provider-URL

Vorbereiten der Kerberos-Authentifizierung

Führen Sie zur Vorbereitung der Kerberos-Authentifizierung die folgenden Aufgaben durch:

- ❑ Richten Sie die Kerberos-Konfigurationsdatei ein.
- ❑ Führen Sie die folgenden Aufgaben durch, um das Namensformat für den Dienstprinzipal und die Keytab-Datei zu generieren:
  - Legen Sie den Dienstprinzipal je nach Ihren Anforderungen auf die Knotenebene oder Prozessebene fest.
  - Führen Sie den Kerberos SPN-Formatgenerator von Informatica aus.
- ❑ Überprüfen Sie die SPN- und Keytab-Format-Textdatei, um sicherzustellen, dass keine Fehler vorhanden sind.
- ❑ Erstellen Sie die Dienstprinzipalnamen und Keytab-Dateien.

Verwandte Themen:

- "Vorbereiten der Einrichtung der Kerberos-Authentifizierung" auf Seite 73

Vor der Installation der Dienste unter Windows

Führen Sie vor der Installation der Dienste unter Windows die folgenden Aufgaben durch:

- ❑ Lesen Sie die Informatica-Versionshinweise, um mehr über Aktualisierungen der Installation und den Upgradeprozess zu erfahren.

- ❑ Überprüfen Sie die Patch-Anforderungen, um sicherzustellen, dass der Computer über die erforderlichen Betriebssystem-Patches und -Bibliotheken verfügt.
- ❑ Sichern Sie die Data Transformation-Dateien, die in einer früheren Version erstellt wurden.
- ❑ Überprüfen Sie die Umgebungsvariablen, die Sie zum Arbeiten mit der Installation von Informatica konfigurieren müssen.
- ❑ Erstellen Sie ein Systembenutzerkonto, um die Installation durchzuführen und den Informatica-Dienst auszuführen.
- ❑ Richten Sie die Schlüsselspeicher- und Truststore-Dateien ein, wenn Sie die sichere Kommunikation für die Domäne konfigurieren möchten, und richten Sie eine sichere Verbindung zu Webclientanwendungen ein.
- ❑ Extrahieren der Dateien des Installationsprogramms.
- ❑ Überprüfen Sie den Lizenzschlüssel.
- ❑ Führen Sie das Vorinstallations-Systemprüfungstool (i10Pi) aus, um sicherzustellen, dass der Computer die Systemanforderungen für die Installation erfüllt.

Verwandte Themen:

- "Vor der Installation der Dienste unter Windows" auf Seite 86

Vor der Installation von Diensten unter UNIX

Führen Sie vor der Installation der Dienste unter UNIX die folgenden Aufgaben durch:

- ❑ Lesen Sie die Informatica-Versionshinweise, um mehr über Aktualisierungen der Installation und den Upgradeprozess zu erfahren.
- ❑ Überprüfen Sie die Patch-Anforderungen, um sicherzustellen, dass der Computer über die erforderlichen Betriebssystem-Patches und -Bibliotheken verfügt.
- ❑ Installieren Sie die Java-Laufzeitumgebung, wenn Sie Informatica unter AIX installieren.
- ❑ Sichern Sie die Data Transformation-Dateien, die in einer früheren Version erstellt wurden.
- ❑ Überprüfen Sie die Umgebungsvariablen, die Sie zum Arbeiten mit der Installation von Informatica konfigurieren müssen.
- ❑ Erstellen Sie ein Systembenutzerkonto, um die Installation durchzuführen und den Informatica-Dienst auszuführen.
- ❑ Richten Sie die Schlüsselspeicher- und Truststore-Dateien ein, wenn Sie die sichere Kommunikation für die Domäne konfigurieren möchten, und richten Sie eine sichere Verbindung zu Webclientanwendungen ein.
- ❑ Stellen Sie sicher, dass das Betriebssystem die Anforderung des Dateideskriptors erfüllt.
- ❑ Konfigurieren Sie POSIX Asynchronous I/O bei der Installation von Informatica auf IBM AIX auf allen Knoten, auf denen Sie einen PowerCenter-Integrationsdienst ausführen möchten.
- ❑ Extrahieren Sie die Dateien des Installationsprogramms.

- ❑ Überprüfen Sie den Lizenzschlüssel.
- ❑ Führen Sie das Vorinstallations-Systemprüfungstool (i10Pi) aus, um sicherzustellen, dass der Computer die Systemanforderungen für die Installation erfüllt.

Verwandte Themen:

- "Vor der Installation von Diensten unter UNIX" auf Seite 94

Installation von Informatica-Diensten

Verwenden Sie zum Installieren der Informatica-Dienste auf einem Windows- oder UNIX-Computer den Informatica Server Installer. Um mehrere Knoten zu erstellen, können Sie die Informatica-Dienste auf mehreren Computern installieren.

Verwandte Themen:

- "Installation von Informatica-Diensten" auf Seite 106

Durchführen der Domänenkonfiguration

Um die Domänenkonfiguration nach dem Installieren der Informatica-Dienste abzuschließen, führen Sie folgende Aufgaben aus:

- ❑ Führen Sie die folgenden Aufgaben durch, um sicherzustellen, dass die Gebietsschemaeinstellungen und die Codepage kompatibel sind:
  - Stellen Sie sicher, dass die Domänen-Konfigurationsdatenbank mit den Codeseiten der Anwendungsdienste, die Sie in der Domäne erstellen, kompatibel ist.
  - Stellen Sie sicher, dass die Gebietsschemaeinstellungen auf Computern mit Zugriff auf das Administrator-Tool und die Informatica-Client-Tools mit den Codepages der Repositorys in der Domäne kompatibel sind.
  - Konfigurieren Sie die Gebietsschema-Umgebungsvariablen unter UNIX.
- ❑ Konfigurieren Sie die folgenden Umgebungsvariablen:
  - Informatica-Umgebungsvariablen zum Speichern der Einstellungen für Speicherplatz, Domänen und Speicherort.
  - Bibliothekspfad-Umgebungsvariablen unter UNIX auf den Computern, auf denen die Datenintegrationsdienst-, PowerCenter-Integrationsdienst- und PowerCenter-Repository-Dienst-Prozesse ausgeführt werden.
  - Kerberos-Umgebungsvariablen, wenn Sie die Informatica-Domäne so konfigurieren, dass sie auf einem Netzwerk mit Kerberos-Authentifizierung ausgeführt wird.
- ❑ Konfigurieren Sie die Windows-Firewall auf dem Computer, auf dem Sie die Informatica-Domäne erstellt haben.

Verwandte Themen:

- "Durchführen der Domänenkonfiguration" auf Seite 175

Vorbereiten zum Erstellen der Anwendungsdienste

Führen Sie vor dem Erstellen der Anwendungsdienste folgende Aufgaben durch:

- ❑ Überprüfen Sie das Setup für 64-Bit-Windows.
- ❑ Erstellen Sie Verzeichnisse für den Analyst-Dienst zum Speichern von temporären Dateien.
- ❑ Erstellen Sie die Dienstprinzipalnamen und Keytab-Dateien für die Anwendungsdienste.
- ❑ Melden Sie sich bei Informatica Administrator an.
- ❑ Erstellen Sie Verbindungen zu den folgenden Datenbanken, auf die die Anwendungsdienste über die native Konnektivität zugreifen:
  - Datenobjekt-Cache-Datenbank
  - Profiling-Warehouse-Datenbank
  - Referenzdaten-Warehouse
  - Arbeitsablauf-Datenbank

Verwandte Themen:

- "Vorbereiten zum Erstellen der Anwendungsdienste" auf Seite 182

Erstellen der Anwendungsdienste

Zum Erstellen der Anwendungsdienste führen Sie die folgenden Aufgaben durch:

- ❑ Erstellen des Modellrepository-Dienstes
  - Erstellen des Modellrepository-Benutzers, wenn die Domäne keine Kerberos-Authentifizierung verwendet

  Hinweis: Wenn Sie planen, Objekte zu überwachen, die in der Domäne ausgeführt werden, erstellen Sie einen zusätzlichen Modellrepository-Dienst, der speziell für das Speichern von Überwachungsdaten eingerichtet ist.
- ❑ Erstellen des Datenintegrationsdienstes
  - Überprüfen der Hostdateikonfiguration unter UNIX
- ❑ Erstellen des Analyst-Diensts
- ❑ Erstellen des Content-Managementdiensts
- ❑ Erstellen des Suchdienstes
- ❑ Erstellen des PowerCenter-Repository-Dienstes
  - Konfigurieren des PowerCenter-Repository-Dienstes zur Ausführung im normalen Modus

- Erstellen des PowerCenter-Repository-Benutzers, wenn die Domäne keine Kerberos-Authentifizierung verwendet

❑ Erstellen des PowerCenter-Integrationsdiensts

❑ Erstellen des Metadata Manager-Diensts

- Erstellen der Inhalte für das Metadata Manager-Repository

❑ Erstellen des Webdienst-Hub-Dienstes

Verwandte Themen:

- "Erstellen der Anwendungsdienste" auf Seite 191

Vor dem Installieren der Clients

Führen Sie vor der Installation der Clients die folgenden Aufgaben durch:

❑ Überprüfen Sie den Speicherplatz für temporäre Dateien.

❑ Stellen Sie sicher, dass das Benutzerkonto, das Sie zum Installieren der Informatica-Clients verwenden, keine Schreibberechtigung für das Installationsverzeichnis und die Windows-Registrierung hat.

❑ Überprüfen Sie die Mindestsystemanforderungen für das Ausführen der Informatica-Client-Tools.

❑ Stellen Sie sicher, dass Sie die Software von Drittanbietern installiert haben, die für den PowerCenter Client erforderlich ist:

Verwandte Themen:

- "Vor dem Installieren der Clients" auf Seite 226

Installieren der Clients

Verwenden Sie zum Installieren der Informatica-Clients unter Windows den Informatica Client Installer.

Sie können die folgenden Informatica-Client-Anwendungen installieren:

❑ Informatica Developer

❑ PowerCenter-Client

Verwandte Themen:

- “Installieren der Clients” auf Seite 228

Nach dem Installieren der Informatica-Clients

Führen Sie nach der Installation der Clients die folgenden Aufgaben durch:

- ❑ Installieren Sie unter Windows weitere Sprachen zum Anzeigen von anderen Sprachen als denen, die dem System-Gebietsschema entsprechen, und zum Arbeiten mit Repositorys, die eine UTF-8-Codepage verwenden.
- ❑ Wenn Sie die sichere Kommunikation für die Domäne konfiguriert haben, konfigurieren Sie die Informatica-Truststore-Umgebungsvariablen auf den Computern, auf denen die Informatica-Clients gehostet werden.
- ❑ Konfigurieren Sie das Developer-Tool so, dass die Workspace-Metadaten in den Computer geschrieben werden, auf dem der Benutzer angemeldet ist.

Verwandte Themen:

- “Nach dem Installieren der Informatica-Clients” auf Seite 232

INDEX

A

abhängige Dienste
  Übersicht 194
AddLicense (infacmd)
  Fehlersuche 173
Administrator-Tool
  Übersicht 24
Analyst-Dienst
  abhängiger Dienst 194
  erstellen 204
  konfigurieren 204
  nach dem Erstellen 206
  Temporäre Verzeichnisse 183
  Voraussetzungen 183
  zugeordnete Dienste 29
Anforderungen an Software von Drittanbietern
  PowerCenter Client 227
Anmeldung
  Fehlerbehebung 186
Anwendungsdienste
  Abhängigkeiten 194
  Analyst-Dienst 28
  Benennungskonventionen 40
  Content-Managementdienst 29
  Datenintegrationsdienst 30
  Dienstprinzipalnamen 184
  Installationsanforderungen 38
  Keytab-Dateien 184
  Metadata Manager-Dienst 31
  Modellrepository-Dienst 32
  Ports 35
  PowerCenter-Integrationsdienst 32
  PowerCenter-Repository-Dienst 33
  Produkte 27
  Suchdienst 33
  Übersicht 21
  Voraussetzungen 192
  Vorbereitung zum Erstellen 182
  Webdienst-Hub 34
Arbeitsablauf
  IBM DB2-Datenbankanforderungen 67
  Microsoft SQL Server-Datenbankanforderungen 67
  Oracle-Datenbankanforderungen 68
Arbeitsabläufe
  Datenbankanforderungen 67
Audit-Datenbank der Ausnahmeverwaltung
  IBM DB2-Datenbankanforderungen 55
  Microsoft SQL Server-Datenbankanforderungen 56
  Oracle-Datenbankanforderungen 56
Authentifizierung
  Kerberos 22
  LDAP 22
  Nativ 22
automatischer Modus
  Installieren der Informatica-Clients 230
automatischer Modus *(Fortsetzung)*
  Installieren von Informatica-Diensten 154

B

Beispiele
  odbc.ini, Datei 278
Benutzer von Prinzipalnamen
  Formatierung 82
Benutzer-Authentifizierung
  Übersicht 22
Benutzerkonten
  Modellrepository 198
  PowerCenter-Repository 213
  UNIX 97
  Windows 88
Berechnungsrolle
  Knoten 20
Berichterstellungs- und Dashboard-Dienst
  abhängiger Dienst 194
Berichterstellungsdienst
  abhängiger Dienst 194
Betriebsmodus
  PowerCenter-Repository-Dienst 212
Bibliotheksanforderungen
  UNIX 95
  Windows 87
Bibliothekspfade
  Umgebungsvariablen 97

C

catalina.out
  Fehler bei der Installation beheben 170
clients
  Fehlerbehebung bei Installationen 236
Clients
  Konfigurieren für sichere Domänen 232
  Übersicht 23
Content-Management-Dienst
  erforderliche Datenbanken 30
  Master-Content-Management-Dienst 29
  zugeordnete Dienste 29
Content-Managementdienst
  abhängiger Dienst 194
  erstellen 207
  konfigurieren 207

D

Data Analyzer Repository
  Oracle-Datenbankanforderungen 62

Data Transformation
Anforderungen an Software von Drittanbietern 227
Datenbank
mit Microsoft SQL Server verbinden 253
Verbinden zu Sybase ASE 271
Verbindungen testen 70
zu Informix verbinden 263
zu Netezza verbinden (UNIX) 266
zu Netezza verbinden (Windows) 254
zu Oracle verbinden 269
zu Sybase ASE verbinden 257
zu Teradata verbinden (Windows) 258
Datenbank-Clients
IBM DB2 client application enabler 70
konfigurieren 70
Microsoft SQL Server, native Clients 70
Oracle-Clients 70
Sybase open clients 70
Umgebungsvariablen 70
Datenbankanforderungen
Arbeitsablauf-Datenbank 67
Audit-Datenbank der Ausnahmeverwaltung 55
Datenobjekt-Cache 54
Installationsanforderungen 37
Metadata Manager-Repository 56
Modellrepository 60
PowerCenter-Repository 62
Profiling-Warehouse 64
Referenzdaten-Warehouse 65
Datenbankbenutzerkonten
Richtlinien für das Einrichten 50
Datenbanken
Data Analyzer Repository 50
Metadata Manager-Repository 50
mit IBM DB2 verbinden 251, 261
mit Informix verbinden 252, 263
mit Microsoft Access verbinden 252
PowerCenter-Repository 50
verbinden zu (Windows) 250
Verbindung herstellen (UNIX) 260
zu Oracle verbinden 255
zu Teradata verbinden (UNIX) 273
Datenbankverbindungen
erstellen 186
Datenintegrationsdienst
abhängiger Dienst 194
erforderliche Datenbanken 31
erstellen 200
Konfiguration der Hostdatei 203
konfigurieren 200
nach dem Erstellen 203
zugeordnete Dienste 30
Datenobjekt-Cache
Datenbankanforderungen 54
IBM DB2-Datenbankanforderungen 54
Microsoft SQL Server-Datenbankanforderungen 54
Oracle-Datenbankanforderungen 55
dbs2-Verbindung
Testen von Datenbankverbindungen 70
Debug-Protokolle
Beheben von Fehlern bei der Installation 169
Deinstallation
Regeln und Richtlinien 239
Dienste
Anwendungsdienste 21
Aufgaben vor der Installation unter UNIX 94
Aufgaben vor der Installation unter Windows 86
Dienstmanager 21
Dienstmanager
Übersicht 21
Dienstprinzipalnamen
Anwendungsdienste 184
erstellen 82
Kerberos-Authentifizierung 75
Dienstrolle
Knoten 20
DISPLAY
Umgebungsvariablen 87
Domänen
Anwendungsdienste 21
Benennungskonventionen 40
Benutzer-Authentifizierung 22
Dienstmanager 21
Knoten 20
konfigurieren 175
planen 25
Ports 35
Sicherheit 23
Übersicht 19
Domänen-Konfigurations-Repository
Fehlerbehebung 171
Microsoft SQL Server-Datenbankanforderungen 52, 61
Sybase ASE-Datenbankanforderungen 53
Vorbereiten der Datenbanken 50
Domänenkonfigurations-Repository
Anforderungen 37
IBM DB2-Datenbankanforderungen 51, 60
Oracle-Datenbankanforderungen 52
Domänenobjekte
Benennungskonventionen 40
Domänensicherheit
Übersicht 23

E

Einzelknoten
Installation 19
Erstellung von Repository-Inhalten
Metadata Manager-Dienst 222

F

Fehlerbehebung
anmelden 186
Client-Installationen 236
Domänen-Konfigurations-Repository 171
Informatica-Dienste 172
Kerberos-Authentifizierung 186
Fehlersuche
Anfügen von Domänen 172
Erstellen von Domänen 172
Lizenzen 173
Pingen von Domänen 173
firewalls
Konfigurierenn unter Windows 180

G

Gateway-Knoten
Erstellen während der Installation 20
Gebietsschema-Umgebungsvariablen
konfigurieren 176

Geteilte Domäne für Metadata Manager
Aufgaben vor der Installation 290
Beispiel 288
Definition 25
Installationsvoraussetzungen 289
Konfiguration der Anwendungsdienste 289
Richtlinien für Einzelcomputer 290
Überlegungen 26
Übersicht 287
Grafikmodus
Installieren der Informatica-Clients 229
Installieren von Informatica-Diensten 108

H

Hostdatei
Datenintegrationsdienst 203
HTTPS
Installationsanforderungen 88, 98

I

i10Pi
UNIX 101
Windows 91
IATEMPDIR
Umgebungsvariablen 87, 97
IBM DB2
DB2CODEPAGE einrichten 251
DB2INSTANCE einrichten 251
Einzelknoten-Tabellenbereich 62
mit Integration Service verbinden (Windows) 251
Verbinden zu Integration Service (Windows) 261
IBM DB2-Datenbankanforderungen
Arbeitsablauf-Repository 67
Audit-Datenbank der Ausnahmeverwaltung 55
Datenobjekt-Cache 54
Domänen-Repository 51, 60
Metadata Manager-Repository 57
Modellrepository-Datenbank 51, 60
PowerCenter-Repository 62
Profiling-Warehouse 64
Referenzdaten-Warehouse 66
infacmd
Hinzufügen von Knoten zu Domänen 172
Pingen von Objekten 173
infasetup
Definieren von Domänen 172
Definieren von Worker-Knoten 172
Informatica Administrator
anmelden 185
Übersicht 24
Informatica Developer
Konfigurieren von lokalem Workspace-Verzeichnis 233
lokale Computer 233
Remote-Computer 233
Sprachen installieren 232
Informatica server
deinstallieren 238, 239
Informatica-Clients
automatische Installation 230
deinstallieren 238, 242
Installation im Grafikmodus 229
Informatica-Dienste
automatische Installation 154
Fehlerbehebung 172
Informatica-Dienste *(Fortsetzung)*
Installation im Grafikmodus 108
Installation im Konsolenmodus 131
konfigurieren 247
Starten und Anhalten unter Windows 246
unter UNIX starten und beenden 246
Informix
mit Integration Service verbinden (UNIX) 263
mit Integration Service verbinden (Windows) 252
verbinden mit Integrationsdienst (UNIX) 263
installation
Sichern der Dateien vor 87, 96
Installationsanforderungen
Anwendungsdienst-Anforderungen 38
Datenbankanforderungen 37
Festplattenspeicher 35
Mindestsystemanforderungen 35
Port-Anforderungen 35
Schlüsselspeicherdateien 88, 98
Truststore-Dateien 88, 98
Umgebungsvariablen 87, 97
Installationsprotokolle
Beschreibungen 170
isql
Testen von Datenbankverbindungen 70

J

JDBC
verbinden zu (Windows) 250
JRE_HOME
Umgebungsvariablen 87, 97

K

Kerberos SPN-Formatgenerator
Windows 77
Kerberos-Authentifizierung
Erstellen von Dienstprinzipalnamen 82
Erstellen von Keytab-Dateien 82
Fehlerbehebung 186
Generieren der SPN-Formate 75
Generieren von Namensformaten für Keytab-Dateien 75
Konfigurationsdateien 74
planen 22, 48
Keytab-Dateien
Anwendungsdienste 184
Kerberos-Authentifizierung 75, 82
Knoten
Anwendungsdienste 21
Benennungskonventionen 40
Berechnungsrolle 20
Dienstmanager 21
Dienstrolle 20
Fehlersuche 172
gateways 20
Rollen 20
Übersicht 20
worker 20
Kompatibilität der Codeseite
Anwendungsdienste 175
Gebietsschema 175
Konfiguration
Domänen 175
Kerberos-Dateien 74
Umgebungsvariablen 177

Konfiguration *(Fortsetzung)*
Umgebungsvariablen unter UNIX 178
Windows-Firewalls 180
Konsolenmodus
Installieren von Informatica-Diensten 131

L

LANG
Gebietsschema-Umgebungsvariablen 87, 97
Umgebungsvariablen 176
LC_ALL
Gebietsschema-Umgebungsvariablen 87, 97
Umgebungsvariablen 176
LC_CTYPE
Umgebungsvariablen 176
LDAP-Authentifizierung
planen 22
Linux
Datenbank-Client-Umgebungsvariablen 70
Lizenzen
hinzufügen 173
Übersicht 22
Lizenzschlüssel
überprüfen 91, 101
Übersicht 22
localhost
Datenintegrationsdienst 203

M

Mehrere Knoten
Installation 19
Metadata Manager-Dienst
abhängiger Dienst 194
erforderliche Datenbanken 32
erstellen 216, 217
Geteilte Domäne 25
Konfiguration einer geteilten Domäne 287
konfigurieren 216
nach dem Erstellen 222
Repository-Inhalte erstellen 222
Überlegungen zu geteilten Domänen 26
zugeordnete Dienste 31
Metadata Manager-Repository
Datenbankanforderungen 56
Heapgrößen 57
IBM DB2-Datenbankanforderungen 57
Microsoft SQL Server-Datenbankanforderungen 58
Optimieren der IBM DB2-Datenbanken 57
Oracle-Datenbankanforderungen 59
temporäre System-Tabellenbereiche 57
Microsoft Access
mit Integration Service verbinden 252
Microsoft Excel
mit Integration Service verbinden 252
Verwenden von PmNullPasswd 252
Verwenden von PmNullUser 252
Microsoft SQL Server
mit Integration Service verbinden 253
Verbinden von UNIX 264
Microsoft SQL Server-Datenbankanforderungen
Arbeitsablauf-Repository 67
Audit-Datenbank der Ausnahmeverwaltung 56
Datenobjekt-Cache 54
Domänen-Konfigurations-Repository 52, 61
Microsoft SQL Server-Datenbankanforderungen *(Fortsetzung)*
Metadata Manager-Repository 58
PowerCenter-Repository 62
Profiling-Warehouse 64
Referenzdaten-Warehouse 66
Mindestsystemanforderungen
Knoten 38
Modellrepository
Benutzer 198
Datenbankanforderungen 60
IBM DB2-Datenbankanforderungen 51, 60
Oracle-Datenbankanforderungen 61
Modellrepository-Dienst
erforderliche Datenbanken 32
Erstellen 195
konfigurieren 195
nach dem Erstellen 198

N

native Authentifizierung
planen 22
Netezza
verbinden mit Informatica-Clients (UNIX) 266
verbinden mit Integrationsdienst (UNIX) 266
verbinden über Integrationsdienst (Windows) 254
von Informatica-Clients aus verbinden (Windows) 254
node.log
Fehler bei der Installation beheben 170
Normalmodus
PowerCenter-Repository-Dienst 212

O

ODBC-Datenquellen
verbinden zu (Windows) 250
Verbindung herstellen zu (UNIX) 276
odbc.ini, Datei
Beispiel 278
Optimierung
PowerCenter-Repository 62
Oracle
zu Integration Service verbinden (UNIX) 269
zu Integration Service verbinden (Windows) 255
Oracle Net Services
zum Verbinden von Integration Service mit Oracle verwenden (UNIX) 269
zum Verbinden von Integration Service mit Oracle verwenden (Windows) 255
Oracle-Datenbankanforderungen
Arbeitsablauf-Repository 68
Audit-Datenbank der Ausnahmeverwaltung 56
Data Analyzer Repository 62
Datenobjekt-Cache 55
Domänenkonfigurations-Repository 52
Metadata Manager-Repository 59
Modellrepository 61
Profiling-Warehouse 65
Referenzdaten-Warehouse 66

P

Patch-Anforderungen
UNIX 95
Windows 87

PATH
Umgebungsvariablen 97
Ping (infacmd)
Fehlersuche 173
Plattenspeicheranforderungen
Installationsanforderungen 35
Port-Anforderungen
Installationsanforderungen 35
Ports
Anforderungen 35
Anwendungsdienste 35
Domänen 35
PowerCenter Client
Anforderungen an Software von Drittanbietern 227
Sprachen installieren 232
PowerCenter-Domänen
Fehlersuche 172
pingen 173
PowerCenter-Integrationsdienst
abhängiger Dienst 194
erstellen 214
konfigurieren 214
nach dem Erstellen 216
zugeordnete Dienste 33
PowerCenter-Repository
Benutzer 213
Datenbankanforderungen 62
IBM DB2-Datenbankanforderungen 62
Microsoft SQL Server-Datenbankanforderungen 62
Optimieren der IBM DB2-Datenbanken 62
Sybase ASE-Datenbankanforderungen 63
PowerCenter-Repository-Dienst
erforderliche Datenbanken 33
erstellen 210
konfigurieren 210
nach dem Erstellen 212
Normalmodus 212
Profiling Warehouse
IBM DB2-Datenbankanforderungen 64
Microsoft SQL Server-Datenbankanforderungen 64
Profiling-Warehouse
Datenbankanforderungen 64
Oracle-Datenbankanforderungen 65
Protokolldateien
catalina.out 170
Debug-Protokolle 169
Installation 169
Installationsprotokolle 170
node.log 170
Typen 169

Q

Quelldatenbanken
durch ODBC (UNIX) Verbindung herstellen 276

R

Referenzdaten-Warehouse
Datenbankanforderungen 65
IBM DB2-Datenbankanforderungen 66
Microsoft SQL Server-Datenbankanforderungen 66
Oracle-Datenbankanforderungen 66
Repositorys
Installieren der Datenbank-Clients 70
Konfigurieren der nativen Konnektivität 68
Repositorys *(Fortsetzung)*
Vorbereiten der Datenbanken 49

S

Schlüsselspeicherdateien
Installationsanforderungen 88, 98
Service Manager
Protokolldateien 170
sichere Domänen
Konfigurieren von Clients 232
Sicherheit
Datenspeicher 22
Domänen 23
Sichern der Dateien
vor dem Installieren 87, 96
vor dem Upgrade 87, 96
SPN 75
Sprachen
Client-Tools 232
unter Windows installieren 232
sqlplus
Testen von Datenbankverbindungen 70
Suchdienst
abhängiger Dienst 194
erstellen 208, 209
konfigurieren 208
zugeordnete Dienste 34
Sybase ASE
Verbinden zu Integration Service (UNIX) 271
zu Integration Service verbinden (Windows) 257
Sybase ASE-Datenbankanforderungen
Domänen-Konfigurations-Repository 53
PowerCenter-Repository 63
Systemanforderungen
Anwendungsdienste 38
Minimal 35
Systemdienste
Übersicht 21
Systemvoraussetzungen
Mindestinstallationsanforderungen 35

T

Tabellenbereichs
Einzelknoten 62
Teradata
verbinden mit Informatica-Clients (UNIX) 273
verbinden mit Informatica-Clients (Windows) 258
verbinden mit Integrationsdienst (UNIX) 273
verbinden mit Integrationsdienst (Windows) 258
Truststore-Dateien
Installationsanforderungen 88, 98

U

Übersicht
vor dem Installieren der Clients 226
Umgebungsvariablen
Bibliothekspfade unter UNIX 178
Datenbank-Clients 70
Gebietsschema 176
INFA_TRUSTSTORE 232
INFA_TRUSTSTORE_PASSWORD 232
Installation 87, 97

Umgebungsvariablen *(Fortsetzung)*
konfigurieren 177
Konfigurieren unter UNIX 178
Konfigurieren von Clients 232
LANG 176
LANG_C 176
LC_ALL 176
LC_CTYPE 176
UNIX 177
UNIX-Datenbank-Clients 70
UNIX
Benutzerkonten 97
Bibliotheksanforderungen 95
Bibliothekspfade 178
Datenbank-Client-Umgebungsvariablen 70
Datenbank-Client-Variablen 70
i10Pi 101
Installieren von Informatica-Diensten im Konsolenmodus 131
Kerberos SPN-Formatgenerator 79
Patch-Anforderungen 95
Starten und Anhalten der Informatica-Dienste 246
Umgebungsvariablen 177
Verbindung zu ODBC-Datenquellen herstellen 276
vor der Installation 101
upgrades
Sichern der Dateien vor 87, 96

V

verbinden
Integration Service mit IBM DB2 (Windows) 251, 261
Integration Service mit Informix (UNIX) 263
Integration Service mit Informix ASE (Windows) 252
Integration Service mit Microsoft Access 252
Integration Service mit Microsoft SQL Server 253
Integration Service mit Oracle (UNIX) 269
Integration Service mit Oracle (Windows) 255
Integration Service mit Sybase ASE (UNIX) 271
Integration Service mit Sybase ASE (Windows) 257
Microsoft Excel mit Integration Service 252
UNIX-Datenbanken 260
Windows über JDBC 250
Windows-Datenbanken 250
Verbinden
Integrationsdienste zu ODBC-Datenquellen (UNIX) 276
Verbindungen
Eigenschaften für Oracle 189
Erstellen von Datenbankverbindungen 186, 190
IBM DB2-Eigenschaften 187
Verbindungen *(Fortsetzung)*
Microsoft SQL Server-Eigenschaften 188
Verschlüsselungsschlüssel
sicherer Datenspeicher 22
Übersicht 22
64-Bit-Plattformen
Richtlinien 182
unterstützte Plattformen 182
vor dem Installieren der Clients
Überprüfen der Anforderungen an Drittanbietersoftware 227
Überprüfen der Installationsanforderungen 226
Überprüfen der Mindestsystemanforderungen 226
Übersicht 226
vor der Installation
Dienste unter UNIX 94
i10Pi unter UNIX 101
i10Pi unter Windows 91
Services unter Windows 86
Voraussetzungen
Anwendungsdienste 192
Vorbereitungen für Datenbanken
Repositorys 49

W

Webdienst-Hub-Dienst
abhängiger Dienst 194
erstellen 222
konfigurieren 222
zugeordnete Dienste 34
Windows
Benutzerkonten 88
Bibliotheksanforderungen 87
i10Pi 91
Installieren der Informatica-Clients im Grafikmodus 229
Installieren von Informatica-Diensten im Grafikmodus 108
Kerberos SPN-Formatgenerator 77
Konfigurieren von Firewalls 180
Patch-Anforderungen 87
Starten und Anhalten der Informatica-Dienste 246
vor der Installation 91
Worker-Knoten
Erstellen während der Installation 20

Z

Zieldatenbanken
durch ODBC (UNIX) Verbindung herstellen 276