



Informatica®

10.2 .2

Installations- und Konfigurationshandbuch zu Informatica Enterprise Data Catalog

© Copyright Informatica LLC 2015, 2019

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 und das Informatica-Logo 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.

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 GARANTIE ODER KUNDENKONDITIONEN IRGENDNEINER 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/hsqLicense.html>, <http://httpunit.sourceforge.net/doc/license.html>, <http://jung.sourceforge.net/license.txt>, http://www.gzip.org/zlib/zlib_license.html, <http://www.opendap.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/license.html>, <http://www.sqlite.org/copyright.html>, <http://www.tcl.tk/software/tcltk/license.html>, <http://www.jaxen.org/faq.html>, <http://www.jdom.org/docs/faq.html>, <http://www.slf4j.org/license.html>, <http://www.iodbc.org/dataspace/iodbc/wiki/iODBC/License>, <http://www.keplerproject.org/md5/license.html>, <http://www.toedter.com/en/jcalendar/license.html>, <http://www.edankert.com/bounce/index.html>, <http://www.net-snmp.org/about/license.html>, <http://www.openmdx.org/#FAQ>, http://www.php.net/license/3_01.txt, <http://srp.stanford.edu/license.txt>, <http://www.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>.

HAFTUNGS AUSSCHLUSS: 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, melden Sie sie uns unter infa_documentation@Informatica.com.

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

Publikationsdatum: 2019-05-17

Inhalt

Einleitung	10
Informatica-Ressourcen.	10
Informatica-Netzwerk.	10
Informatica-Wissensdatenbank.	10
Informatica-Dokumentation.	11
Informatica-Produktverfügbarkeitsmatrizen.	11
Informatica Velocity.	11
Informatica Marketplace.	11
Globaler Kundensupport von Informatica.	11
Teil I: Installation – Übersicht	12
Kapitel 1: Enterprise Data Catalog	13
Übersicht über die Installation von Enterprise Data Catalog.	13
Installation Prozess.	14
Enterprise Data Catalog-Dienste.	15
Enterprise Data Catalog-Repositorys.	16
Installations- und Konfigurationsprüfliste.	16
Teil II: Vor dem Installieren Enterprise Data Catalog	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.	24
Planungsprozess für die Domäne.	24
Planen der Anwendungsdienste.	25
Datenintegrationsdienst.	25
Modellrepository-Dienst.	26
Katalogdienst.	26
Informatica-Cluster-Dienst.	27
Content-Management-Dienst.	27
Überprüfen der Systemvoraussetzungen.	28

Überprüfen der Installationsanforderungen für Dienste.	28
Überprüfen der Anforderungen an temporären Festplattenspeicher.	29
Überprüfen der Portanforderungen.	29
Überprüfen der Datenbankanforderungen.	31
Überprüfen der Hardwarevoraussetzungen für Anwendungsdienste.	32
Aufzeichnen der Informatica-Domänen- und -Knoteninformationen.	32
Benennungskonventionen für Datenobjekte.	33
Domäne.	34
Knoten.	35
Anwendungsdienste.	35
Sicherer Datenspeicher.	36
Domänensicherheit.	36
Kapitel 3: Vorbereiten von Datenbanken für die Informatica-Domäne	38
Vorbereiten von Datenbanken für die Informatica-Domäne – Übersicht.	38
Einrichten von Datenbankbenutzerkonten.	39
Datenbankanforderungen des Domänen-Konfigurations-Repositorys.	39
IBM DB2-Datenbankanforderungen.	39
Microsoft SQL Server-Datenbankanforderungen.	41
Oracle-Datenbankanforderungen.	41
Sybase ASE-Datenbankanforderungen.	42
Anforderungen für Datenobjekt-Cache-Datenbank.	42
IBM DB2-Datenbankanforderungen.	43
Microsoft SQL Server-Datenbankanforderungen.	43
Oracle-Datenbankanforderungen.	43
Modellrepository-Datenbankanforderungen.	43
IBM DB2-Datenbankanforderungen.	44
Microsoft SQL Server-Datenbankanforderungen.	45
Oracle-Datenbankanforderungen.	45
Anforderungen an das Profiling-Warehouse.	46
IBM DB2-Datenbankanforderungen.	46
Microsoft SQL Server-Datenbankanforderungen.	46
Oracle-Datenbankanforderungen.	47
Anforderungen des Referenzdaten-Warehouse.	47
IBM DB2-Datenbankanforderungen.	48
Microsoft SQL Server-Datenbankanforderungen.	48
Oracle-Datenbankanforderungen.	48
Kapitel 4: Bereitstellungsmethoden.	49
Bereitstellungsmethoden (Übersicht).	49
Bereitstellung auf einem eingebetteten Hadoop-Cluster Voraussetzungen.	49
Voraussetzungen – Eingebetteter Cluster	50
Betriebssystemvoraussetzungen.	50

Voraussetzungen für Hostknoten.	53
Voraussetzungen für die Bereitstellung von Enterprise Data Catalog auf mehreren Knoten.	53
Voraussetzungen für Cluster-Knoten.	54
Voraussetzungen für Apache Ambari.	54
Voraussetzungen für Apache Ranger.	54
Grenzwert für den Dateideskriptor.	54
Voraussetzungen für SSL.	54
Voraussetzungen für Kerberos.	55
Informatica-Cluster-Dienst.	55
Vorbereiten der eingebetteten Hadoop-Clusterumgebung.	60
Verwaltung von eingebetteten Clusterknoten.	60
Voraussetzungen – Vorhandener Cluster.	61
Voraussetzungen für Hostknoten.	61
Voraussetzungen für Clusterknoten.	61
Voraussetzungen für Apache Ranger.	61
Grenzwert für den Dateideskriptor.	61
Voraussetzungen für SSL.	62
Voraussetzungen für Kerberos.	62
Voraussetzungen für die Informatica-Domäne.	63
Benutzerberechtigungen.	63
Vorhandene Hadoop-Cluster-Bereitstellung.	63
Vorbereiten der vorhandenen Hadoop-Clusterumgebung.	64
Kerberos- und SSL-Setup für einen vorhandenen Cluster.	64
Teil III: Installation von Enterprise Data Catalog.	67
Kapitel 5: Installation von Enterprise Data Catalog-Diensten.	68
Übersicht über die Installation von Enterprise Data Catalog-Diensten.	68
Fortsetzen der Installation.	69
Erstellen oder Anfügen einer Domäne.	69
Installieren der Enterprise Data Catalog-Dienste im Konsolenmodus.	70
Sicheres Verzeichnis für den Verschlüsselungsschlüssel und die Konfigurationsdateien.	70
Installieren durch Beitreten zu einer Domäne.	86
Installieren von Enterprise Data Catalog auf einem Domänenknoten.	96
Erstellen der Anwendungsdienste für Enterprise Data Catalog.	97
Installieren von Enterprise Data Catalog im automatischen Modus.	108
Konfigurieren der Eigenschaftendatei.	109
Ausführen des automatischen Installationsprogramms.	127
Installieren der Anwendungsdienste für Enterprise Data Catalog im automatischen Modus.	128
Konfigurieren der Eigenschaftendatei.	128
Ausführen des automatischen Installationsprogramms zum Installieren der Dienste.	128
Sichern der Passwörter in der Eigenschaftendatei.	129

Teil IV: Nach der Installation von Enterprise Data Catalog.....	130
Kapitel 6: Durchführen der Domänenkonfiguration.	131
Durchführen der Domänenkonfiguration - Übersicht.	131
Überprüfen der Kompatibilität der Codepage.	131
Konfigurieren von Gebietsschema-Umgebungsvariablen unter Linux.	132
Konfigurieren der Umgebungsvariablen.	132
Konfigurieren von Umgebungsvariablen für Enterprise Data Catalog.	133
Konfigurieren der Bibliothekspfad-Umgebungsvariablen unter Linux.	134
Berechtigungen des Katalogdiensts.	134
Kapitel 7: Vorbereiten zum Erstellen der Anwendungsdienste.....	137
Vorbereitung zum Erstellen der Anwendungsdienste – Übersicht.	137
Anmelden beim Informatica Administrator.	137
Erstellen von Verbindungen.	138
Eigenschaften von IBM DB2-Verbindungen.	139
Eigenschaften von Microsoft SQL Server-Verbindungen.	140
Eigenschaften für Oracle-Verbindungen.	141
Erstellen einer Verbindung.	142
Kapitel 8: Erstellen der Anwendungsdienste.	143
Erstellen der Anwendungsdienste – Übersicht.	143
Überprüfen der Voraussetzungen für Anwendungsdienste.	143
Abhängigkeiten von Anwendungsdiensten.	145
Erstellen und Konfigurieren des Modellrepository-Dienstes.	145
Erstellen des Modellrepository-Dienstes.	146
Nach dem Erstellen des Modellrepository-Dienstes.	148
Erstellen und Konfigurieren des Datenintegrationsdienstes.	150
Erstellen des Datenintegrationsdienstes.	150
Nach dem Erstellen des Datenintegrationsdienstes.	153
Erstellen eines Katalogdiensts.	153
Konfigurieren des Katalogdiensts für Azure HDInsight.	158
Erstellen und Konfigurieren des Content-Management-Dienstes.	160
Erstellen des Content-Management-Dienstes.	160
Kapitel 9: Konfigurieren von Single Sign-On mithilfe der SAML-Authentifizierung.	162
Übersicht über Single Sign-On mithilfe der SAML-Authentifizierung.	162
Konfigurieren des standardmäßigen RelayState-URL-Parameters in OKTA.	162
Konfigurieren von Anwendungs-URL-Endpunkten für Enterprise Data Catalog in den Active Directory-Verbunddiensten.	163

Teil V: Deinstallation.....	164
Kapitel 10: Deinstallation.....	165
Deinstallation - Übersicht.....	165
Regeln und Richtlinien für die Deinstallation.....	165
Deinstallation von Enterprise Data Catalog.....	166
Deinstallieren von Enterprise Data Catalog im automatischen Modus.....	166
Teil VI: Fehlerbehebung.....	167
Kapitel 11: Fehlerbehebung.....	168
Fehlerbehebung – Übersicht.....	168
Fehlerbehebung bei Installationsprotokolldateien.....	168
Debug-Protokolldateien.....	169
Dateiinstallations-Protokolldatei.....	169
Service Manager-Protokolldateien.....	169
Fehlerbehebung von Domänen und Knoten.....	170
Erstellen des Domänenkonfigurations-Repository.....	170
Erstellen einer Domäne oder Beitreten zu einer Domäne.....	171
Ausführen einer Ressource.....	171
Starten von Enterprise Data Catalog.....	171
Pingen der Domäne.....	172
Hinzufügen einer Lizenz.....	172
Fehlerbehebung bei häufig auftretenden Problemen bei der Cluster-Bereitstellung.....	172
Fehlerbehebung bei der Bereitstellung auf einem vorhandenen Cluster.....	179
Fehlerbehebung bei der Bereitstellung auf einem eingebetteten Cluster.....	180
Fehlerbehebung bei Problemen mit Anwendungsdiensten.....	184
Anhang A: Starten und Beenden von Enterprise Data Catalog-Diensten.....	185
Starten und Beenden von Enterprise Data Catalog-Diensten unter Linux.....	185
Beenden der Enterprise Data Catalog-Dienste im Administrator Tool.....	185
Regeln und Richtlinien zum Starten oder Beenden von Enterprise Data Catalog.....	186
Anhang B: Entfernen des sudo-Zugriffs, nachdem ein eingebetteter Cluster erstellt wurde.....	187
Entfernen des sudo-Zugriffs, nachdem ein eingebetteter Cluster erstellt wurde.....	187
Anhang C: Konfigurieren eines benutzerdefinierten Protokollverzeichnisses für Ambari.....	189
Konfigurieren eines benutzerdefinierten Protokollverzeichnisses für Ambari.....	189

Anhang D: Konfigurieren von Enterprise Data Catalog für WANdisco Fusion-fähigen Cluster.....	190
Konfigurieren von Enterprise Data Catalog für WANdisco Fusion-fähigen Cluster.	190
Anhang E: Konfigurieren des Informatica Custom Service-Deskriptors.....	192
Übersicht.	192
Voraussetzungen.	193
Erstellen des Informatica Custom Service-Deskriptordiensts.	193
Häufig gestellte Fragen (FAQ).	195
Anhang F: Erstellen von benutzerdefinierten Benutzern und Benutzergruppen für Dienste, die in einem eingebetteten Cluster bereitgestellt werden.....	197
Übersicht.	197
Voraussetzungen.	198
Erstellen von benutzerdefinierten Benutzern und Benutzergruppen für Dienste, die in einem eingebetteten Cluster bereitgestellt werden.	198
Anhang G: Konfigurieren benutzerdefinierter Ports für Hadoop-Anwendungen.....	200
Übersicht.	200
Konfigurieren benutzerdefinierter Ports für Hadoop-Anwendungen.	202
Index.	203

Einleitung

Das *Informatica Installations- und Konfigurationshandbuch* wendet sich an Systemadministratoren, die für die Installation des Informatica-Produkts zuständig sind. In diesem Handbuch wird davon ausgegangen, dass Sie sich mit Betriebssystemen, Konzepten von relationalen Datenbanken sowie den Datenbank-Engines, Einfachdateien oder Mainframe-Systemen in Ihrer Umgebung auskennen. Des Weiteren wird vorausgesetzt, dass Sie mit den Schnittstellenanforderungen für die unterstützenden Anwendungen vertraut sind.

Informatica-Ressourcen

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

Informatica-Netzwerk

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

Als Mitglied des Informatica-Netzwerks haben Sie die folgenden Optionen:

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

Informatica-Wissensdatenbank

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

Zum Durchsuchen der Wissensdatenbank besuchen Sie <https://search.informatica.com>. Wenn Sie Fragen, Kommentare oder Ideen zur Wissensdatenbank haben, wenden Sie sich per E-Mail an das Team der Informatica-Wissensdatenbank unter KB_Feedback@informatica.com.

Informatica-Dokumentation

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

Zusätzlich zum Dokumentationsportal bietet Informatica in der Informatica-Wissensdatenbank Dokumentationen für viele Produkte an. Wenn Sie im Dokumentationsportal keine Dokumentation zu Ihrem Produkt oder Ihrer Produktversion finden, durchsuchen Sie die Wissensdatenbank unter <https://search.informatica.com>

Wenn Sie Fragen, Kommentare oder Ideen zur Produktdokumentation haben, wenden Sie sich an das Informatica-Dokumentationsteam unter infa_documentation@informatica.com

Informatica-Produktverfügbarkeitsmatrizen

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

Informatica Velocity

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

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

Informatica Marketplace

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

Globaler Kundensupport von Informatica

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

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

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

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

Teil I: Installation – Übersicht

- [Enterprise Data Catalog, 13](#)

KAPITEL 1

Enterprise Data Catalog

Dieses Kapitel umfasst die folgenden Themen:

- [Übersicht über die Installation von Enterprise Data Catalog, 13](#)
- [Installation Prozess, 14](#)
- [Enterprise Data Catalog-Dienste, 15](#)
- [Enterprise Data Catalog-Repositorys, 16](#)
- [Installations- und Konfigurationsprüfliste, 16](#)

Übersicht über die Installation von Enterprise Data Catalog

Informatica bietet ein Installationsprogramm an, das sowohl Enterprise Data Catalog als auch die zugehörigen Dienste installiert. Enterprise Data Catalog wird innerhalb der Informatica-Domäne installiert. Enterprise Data Catalog verwendet den Katalogdienst und andere Anwendungsdienste, um konfigurierte Datenobjekte in einem Unternehmen zusammenzuführen und eine umfassende Ansicht der Datenobjekte und der Datenobjektbeziehungen darzustellen.

Sie können Enterprise Data Catalog und seine Dienste entweder auf einem eingebetteten oder auf einem vorhandenen Hadoop-Cluster bereitstellen.

Eingebetteter Cluster

Bezieht sich auf die Hadoop-Distribution, die im Installationsprogramm von Enterprise Data Catalog enthalten ist. Sie können den Cluster bei der Installation von Enterprise Data Catalog konfigurieren.

Vorhandener Cluster

Bezieht sich auf einen Hadoop-Cluster in Ihrer Unternehmensumgebung, wenn Sie Enterprise Data Catalog bereitstellen möchten. Vergewissern Sie sich, dass der Hadoop-Cluster, den Sie verwenden, in den [Product Availability Matrices \(PAM\) for Enterprise Data Catalog](#) aufgeführt wird. Konfigurieren Sie den Cluster, bevor Sie Enterprise Data Catalog bereitstellen.

Um Enterprise Data Catalog verwenden zu können, müssen Sie die Enterprise Data Catalog-Dienste installieren und eine Domäne erstellen. Installieren Sie die Dienste mithilfe des Installationsprogramms für Enterprise Data Catalog. Bei der Installation von Enterprise Data Catalog müssen Sie die Domäne und die Anwendungsdienste konfigurieren, die Enterprise Data Catalog verwendet. Enterprise Data Catalog erfordert eine dedizierte Domäne, bevor Sie es verwenden können.

Die Enterprise Data Catalog-Dienste bestehen aus Diensten zur Unterstützung der Domäne und Anwendungsdiensten, um Aufgaben auszuführen und Datenbanken zu verwalten. Bei der Informatica-Domäne handelt es sich um die Verwaltungseinheit für die Enterprise Data Catalog-Umgebung. Die Domäne

ist eine Sammlung von Knoten, die die Computer darstellen, auf denen die Anwendungsdienste ausgeführt werden. Wenn Sie die Enterprise Data Catalog-Dienste auf einem Computer installieren, installieren Sie alle Dateien für alle Dienste.

Bei der Installation von Enterprise Data Catalog auf einem einzigen Computer erstellen Sie auf demselben Computer die Informatica-Domäne und einen Knoten. Wenn Sie auf mehreren Computern eine Installation ausführen, erstellen Sie einen Gateway-Knoten und die Informatica-Domäne für die erste Installation. Während der Installation auf zusätzlichen Computern erstellen Sie Worker-Knoten, die Sie mit der Domäne verknüpfen.

Enterprise Data Catalog enthält die folgenden Client-Anwendungen:

- Informatica Administrator
- Informatica Catalog Administrator
- Suchwerkzeug für Enterprise Data Catalog

Sie verwenden die Clients für den Zugriff auf die Dienste in der Domäne.

Installation Prozess

Die Installation von Enterprise Data Catalog besteht aus mehreren Phasen.

Der Installationsprozess besteht aus den folgenden Phasen:

1. Führen Sie vor der Installation der Enterprise Data Catalog-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 von der Domäne verwendeten Benutzerauthentifizierungstyp.
 - b. Bereiten Sie die Datenbanken für die Domäne vor. Überprüfen Sie die Datenbankanforderungen und richten Sie dann die für Enterprise Data Catalog erforderlichen Datenbanken ein.
 - c. Richten Sie die Computer so ein, dass sie die Linux-Anforderungen erfüllen, damit Sie die Enterprise Data Catalog-Dienste erfolgreich installieren und ausführen können.
 - d. Bestimmen Sie, ob die Standard-Datensatzgröße für die Installation von Enterprise Data Catalog geändert werden muss. Enterprise Data Catalog verfügt über die Datensatzgrößen "Klein", "Mittel", "Groß", "Standard" und "Demo". Diese Größen können Sie mit benutzerdefinierten Eigenschaften in Informatica Administrator konfigurieren. Datensätze werden basierend auf der Menge der zu verarbeitenden Metadaten und der Anzahl der zum Verarbeiten von Metadaten verwendeten Knoten klassifiziert.

Hinweis:

- Nach der Installation können Sie die Datensatzgröße von einer niedrigeren Datensatzgröße auf eine höhere Datensatzgröße umschalten. Wenn Sie z. B. während der Installation eine kleine Datensatzgröße ausgewählt haben, können Sie die Datensatzgröße nach der Installation zu Mittel oder Groß ändern. Wenn Sie jedoch während der Installation einen höheren Datensatzwert ausgewählt haben, z. B. Groß, können Sie die Datensatzgröße nach der Installation nicht in eine niedrigere Datensatzgröße ändern, z. B. Mittel, Klein oder Standard.
- Sie können die Datensatzgröße nicht ändern, wenn Sie während der Installation eine Demo-Datensatzgröße ausgewählt haben.

- Sie müssen den Katalogdienst neu starten und indizieren, wenn Sie die Datensatzgröße nach der Installation von Enterprise Data Catalog ändern.

Weitere Informationen zu den Datensatzgrößen und zur Leistungsoptimierung finden Sie in folgendem Artikel in der Informatica-Ratgeber-Bibliothek: *Optimieren der Leistung von Enterprise Data Catalog*.

2. Installieren Sie Enterprise Data Catalog.

Verwenden Sie das Installationsprogramm, um die Enterprise Data Catalog-Dienste auf einem oder mehreren Linux-Computern zu installieren. 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 Enterprise Data Catalog-Dienste die folgenden Aufgaben aus, um die Installation der Dienste abzuschließen:

- 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.
- Optional können Sie das Erstellen der Anwendungsdienste vorbereiten. Überprüfen Sie Betriebssystemanforderungen für Anwendungsdienste und erstellen Sie dann die Benutzer und Verbindungen, die für die Anwendungsdienste erforderlich sind.

Sie können die Anwendungsdienste anhand einer der folgenden Möglichkeiten erstellen:

- Automatisch, wenn Sie Enterprise Data Catalog installieren.
- Manuell in Informatica Administrator nach der Installation von Enterprise Data Catalog
- Manuell unter Verwendung des Installationsprogramms zu einem späteren Zeitpunkt, nachdem Sie Enterprise Data Catalog installiert und das Installationsprogramm beendet haben.

Wenn die Installation aufgrund eines Fehlers, einer Unterbrechung oder eines unbeabsichtigten Beendens des Installationsprogramms nicht abgeschlossen wurde, können Sie mit dem Installationsprogramm die Installation an der Stelle fortsetzen, an der sie gestoppt wurde.

Enterprise Data Catalog-Dienste

Anwendungsdienste von Enterprise Data Catalog stellen serverbasierte Funktionen dar. Nach Abschluss der Installation können Sie optional Anwendungsdienste basierend auf dem Lizenzschlüssel erstellen, der für Ihr Unternehmen generiert wurde.

Beim Erstellen eines Anwendungsdiensts benennen Sie einen Knoten, 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 Dienstyp.

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 benötigen 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.

Enterprise Data Catalog verwendet die folgenden Anwendungsdienste:

- Datenintegrationsdienst

- Modellrepository-Dienst
- Katalogdienst
- Informatica-Cluster-Dienst
- Content-Management-Dienst

Enterprise Data Catalog-Repositorys

Enterprise Data Catalog verwendet unterschiedliche Arten von Repositorys, je nachdem, welche Daten- und Metadatentypen es speichert.

Für Enterprise Data Catalog sind folgende Repositorys erforderlich:

Domänenkonfigurations-Repository

Eine relationale Datenbank, in der Domänenkonfiguration und Benutzerinformationen gespeichert werden.

Modellrepository

Eine relationale Datenbank, in der Metadaten gespeichert werden, die von Enterprise Data Catalog und von Anwendungsdiensten erstellt wurden, um die Zusammenarbeit zwischen den Clients und Diensten zu ermöglichen. Im Modellrepository werden auch die Ressourcenkonfiguration und die Datendomäneninformationen gespeichert.

Profiling-Warehouse

Eine relationale Datenbank zum Speichern der Profilergebnisse. Profilstatistiken sind Bestandteil der umfassenden Metadatenansicht, die Enterprise Data Catalog bietet.

Referenzdaten-Warehouse

Eine relationale Datenbank, in der Datenwerte für die Referenztabellenobjekte gespeichert werden, 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.

Installations- und Konfigurationsprüfliste

Die Installations- und Konfigurationsprüfliste fasst die Aufgaben zusammen, die Sie ausführen müssen, um die Installation von Enterprise Data Catalog abzuschließen.

Führen Sie die folgenden Aufgaben aus, um den Vorgang abzuschließen:

1. Planen Sie die Domäne.
2. Bereiten Sie die Datenbanken für die Domäne vor.
3. Stellen Sie sicher, dass die Computer die Linux-Anforderungen erfüllen. Überprüfen Sie, ob TAR- und ZIP-Dienstprogramme in der Linux-Umgebung verfügbar sind, um die Installationsdateien zu extrahieren und die Dienste bereitzustellen.
4. Wählen Sie die Datensatzgröße oder den Arbeitslasttyp für die Installation aus. Wenn Sie die Standard-Datensatzgröße ändern möchten, müssen Sie eine der folgenden Datensatzgrößen in Informatica Administrator wählen: Klein, Mittel, Groß oder Demo. Sie können die entsprechende Datengröße

basierend auf den Mengen-Metadaten, die Enterprise Data Catalog verarbeiten muss, und der Anzahl der Knoten bestimmen, die zur Verarbeitung von Metadaten verwendet werden. Weitere Informationen

Hinweis:

- Nach der Installation können Sie die Datensatzgröße von einer niedrigeren Datensatzgröße auf eine höhere Datensatzgröße umschalten. Wenn Sie z. B. während der Installation eine kleine Datensatzgröße ausgewählt haben, können Sie die Datensatzgröße nach der Installation zu Mittel oder Groß ändern. Wenn Sie jedoch während der Installation einen höheren Datensatzwert ausgewählt haben, z. B. Groß, können Sie die Datensatzgröße nach der Installation nicht in eine niedrigere Datensatzgröße ändern, z. B. Mittel, Klein oder Standard.
- Sie können die Datensatzgröße nicht ändern, wenn Sie während der Installation eine Demo-Datensatzgröße ausgewählt haben.

Weitere Informationen zu den Datensatzgrößen und zur Leistungsoptimierung finden Sie in folgendem Artikel in der Informatica-Ratgeber-Bibliothek: *Optimieren der Leistung von Enterprise Data Catalog..*

5. Installieren Sie Enterprise Data Catalog.
6. Melden Sie sich bei Informatica Administrator an.
7. Wenn Sie während der Installation keine Anwendungsdienste erstellt haben, müssen Sie die Anwendungsdienste jetzt erstellen und aktivieren. Die Anwendungsdienste umfassen den Modellrepository-Dienst, den Datenintegrationsdienst, den Katalogdienst, den Informatica-Cluster Dienst und den Content-Management-Dienst.
8. Erstellen Sie die Domänenbenutzer.
9. Weisen Sie den Benutzern und Gruppen die erforderlichen Berechtigungen zu.
10. Installieren Sie Informatica Developer, wenn Sie die Datendomänenerkennung für Metadaten-Quellen mit Datendomänen ausführen möchten, die Referenztabellen verwenden.
11. Wenn Sie vordefinierte Datendomänen in Profiling-Statistiken verwenden möchten, müssen Sie die erforderlichen Datendomänen mit Informatica Developer importieren.
12. Starten Sie Catalog Administrator und das Suchwerkzeug für Enterprise Data Catalog von Informatica Administrator aus.

Teil II: Vor dem Installieren Enterprise Data Catalog

Dieser Teil enthält die folgenden Kapitel:

- [Planen der Domäne, 19](#)
- [Vorbereiten von Datenbanken für die Informatica-Domäne , 38](#)
- [Bereitstellungsmethoden, 49](#)

KAPITEL 2

Planen der Domäne

Dieses Kapitel umfasst die folgenden Themen:

- [Einführung in die Informatica-Domäne, 19](#)
- [Planungsprozess für die Domäne, 24](#)
- [Planen der Anwendungsdienste, 25](#)
- [Überprüfen der Systemvoraussetzungen, 28](#)
- [Aufzeichnen der Informatica-Domänen- und -Knoteninformationen, 32](#)

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 Enterprise Data Catalog-Dienste muss das Domänenkonfigurations-Repository in einer relationalen Datenbank erstellt werden.

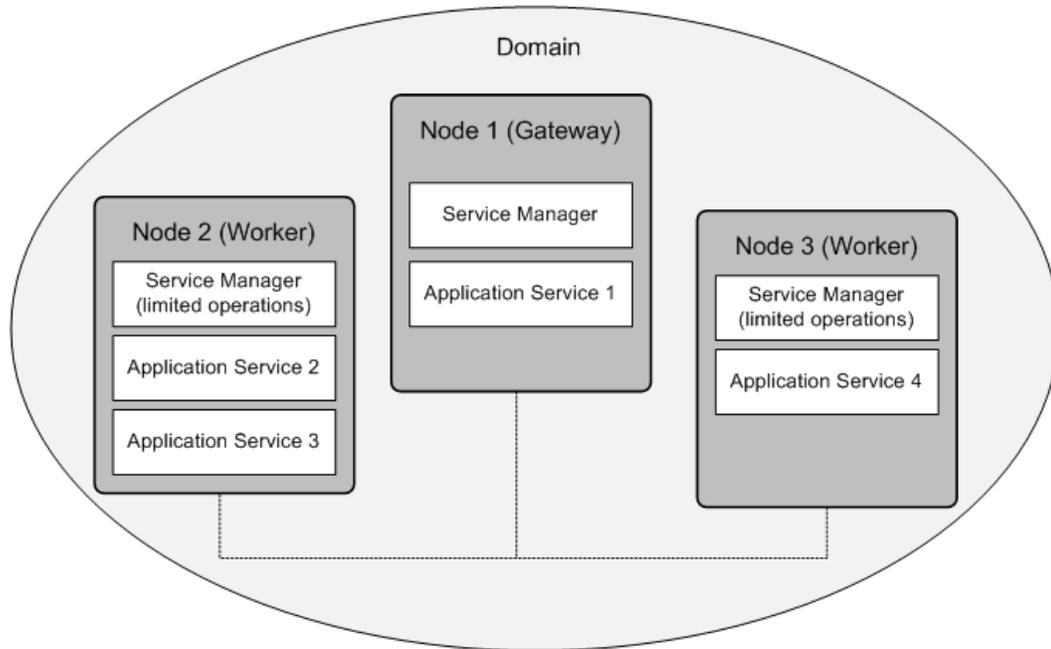
Domäne mit einem oder mehreren Knoten

Wenn Sie die Enterprise Data Catalog-Dienste auf einem Computer installieren, erstellen Sie einen Knoten und eine Domäne. Sie können die Enterprise Data Catalog-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.

Welche Domänenfunktionen und Dienste ein Knoten ausführt, hängt von den folgenden Knotenkonfigurationen ab:

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 Enterprise Data Catalog-Dienste erstellen Sie einen Gateway-Knoten und die Informatica-Domäne. Beim Installieren der Enterprise Data Catalog-Dienste auf weiteren Computern erstellen Sie zusätzliche Gateway-Knoten oder Worker-Knoten, die Sie mit der Domäne verknüpfen.

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 *Handbuch für Informatica Administrator*.

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

Voraussetzungen für die Bereitstellung von Enterprise Data Catalog auf mehreren Knoten

Für die Bereitstellung von Enterprise Data Catalog auf mehreren Knoten müssen die folgenden Voraussetzungen erfüllt sein:

- Stellen Sie sicher, dass Sie zum Starten aller Knoten dieselben Benutzeranmeldedaten verwenden.
- Bevor Sie Enterprise Data Catalog auf einem eingebetteten Cluster bereitstellen, müssen Sie für alle Hostknoten die SSH-Anmeldung ohne Passwortschutz beim Clusterknoten aktivieren.
- Stellen Sie sicher, dass auf allen Knoten die gleiche Version der Apache Ambari-Binärdateien vorhanden ist, bevor Sie Enterprise Data Catalog in einem eingebetteten Cluster bereitstellen.
- Stellen Sie sicher, dass Sie auf allen Knoten die gleiche Kopie der binären Ressourcendateien verwenden.
- Wenn Sie Enterprise Data Catalog auf mehreren Knoten bereitstellen möchten, stellen Sie sicher, dass Sie den Informatica-Cluster-Dienst und den Katalogdienst auf separaten Knoten konfigurieren.

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 beinhalten Dienste, die über mehrere Instanzen in der Domäne verfügen können, und Systemdienste, die über eine einzelne Instanz in der Domäne verfügen können. 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 Dienstyp.

Wenn Sie die Hochverfügbarkeitsoption wählen, können Sie einen Anwendungsdienst auf mehreren Knoten ausführen. Falls Sie die Hochverfügbarkeitsoption nicht wählen, konfigurieren Sie die einzelnen Anwendungsdienste für die Ausführung auf jeweils einem Knoten.

Einige Anwendungsdienste benötigen 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.

Bei der Installation der Enterprise Data Catalog-Dienste 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

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

Das Installationsprogramm konfiguriert 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 zur Benutzerauthentifizierung finden Sie im *Informatica-Sicherheitshandbuch*.

Verschlüsselungsschlüssel für sicheren Datenspeicher

Informatica verschlüsselt vertrauliche Daten wie Passwörter und sichere Verbindungsparameter, bevor die Daten in den Enterprise Data Catalog-Repositorys gespeichert werden. Informatica verwendet ein

Schlüsselwort zum Erstellen eines Verschlüsselungsschlüssels, mit dem vertrauliche Daten verschlüsselt werden.

Wenn Sie die Enterprise Data Catalog-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: `<Enterprise Data Catalog-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 ein Schlüsselwort angeben, auch wenn Sie keine sichere Kommunikation für die Domäne aktivieren.

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 Enterprise Data Catalog-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 Enterprise Data Catalog-Dienste installieren und eine Domäne erstellen, können Sie das Domänenkonfigurations-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 bzw. 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.

Hinweis: Enterprise Data Catalog unterstützt keine Informatica-Domäne, die für die Kerberos-Authentifizierung aktiviert ist.

Informatica-Clients

Informatica-Clients sind eine Gruppe von Clients, die Sie für den Zugriff auf zugrunde liegende Funktionen von Enterprise Data Catalog verwenden. Die Clients senden Anfragen an den Dienstmanager oder an Anwendungsdienste.

Die Informatica-Clients bestehen aus mehreren Thin- oder Web-Client-Anwendungen. Sie verwenden die Clients für den Zugriff auf die Dienste in der Domäne. Wenn Sie die Informatica-Client-Installation ausführen, können Sie Informatica Developer installieren. Dabei handelt es sich um eine Thick-Client-Anwendung zum Importieren von Datendomänen. Wenn Sie die Datendomäneninformationen in Enterprise Data Catalog anzeigen müssen, müssen Sie Informatica Developer installieren. Das Developer Tool ist eine Clientanwendung, mit der Sie Datendomänen erstellen, exportieren und importieren können. Die im Developer Tool erstellten Objekte werden in einem Modellrepository gespeichert, und der Datenintegrationsdienst führt die Objekte aus. Wenn Sie in der Profilkonfiguration vordefinierte Datendomänen verwenden, führt der Content-Management-Dienst die Datendomänenobjekte aus.

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

Sie können die folgenden Thin-Client-Anwendungen installieren:

Informatica Administrator

Informatica Administrator ist das Verwaltungstool für die Verwaltung der Informatica-Domäne und -Sicherheit. Das Administrator Tool ist eine Thin- oder Web-Client-Anwendung. Im Administrator Tool können Sie Domänenverwaltungsaufgaben (z. B. die Verwaltung von Protokollen und Domänenobjekten) sowie Sicherheitsverwaltungsaufgaben (z. B. die Verwaltung von Benutzern, Gruppen und Rollen) ausführen. Außerdem können Sie mit Informatica Administrator die erforderlichen Anwendungsdienste, z. B. Datenintegrationsdienst, Modellrepository-Dienst und Katalogdienst, erstellen.

Enterprise Data Catalog

Enterprise Data Catalog ist ein Webclient, der eine umfassende Ansicht der Metadaten aus konfigurierten Datenobjekten anzeigt. Scanner extrahieren die Metadaten aus den externen Datenquellen. Sie können Metadaten durchsuchen und Informationen anzeigen, z. B. Datenobjektbeziehungen und Herkunftsinformationen.

Informatica Catalog Administrator

Informatica Catalog Administrator ist das Verwaltungstool, mit dem Sie Ressourcen, Scanner, Zeitpläne, Attribute und Verbindungen verwalten können.

Planungsprozess für die Domäne

Bevor Sie die Enterprise Data Catalog-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 für die Datenbanken bestimmen, die von den einzelnen Anwendungsdiensten benötigt werden.

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 die Sicherheit für die Domäne konfigurieren, müssen Sie den Speicherort und das Passwort für die Schlüsselspeicher- und Truststore-Dateien kennen. Im Rahmen der Planung müssen Sie außerdem

überprüfen, ob jeder Computer und jeder Datenbankserver in der Domäne die Mindestsystemanforderungen erfüllt.

Hinweis: Außerdem müssen Sie das Dienstprogramm *ktutil* für die Befehlszeilenschnittstelle auf dem Informatica-Domänencomputer installieren.

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.

Das Installationsprogramm fragt Sie, ob Sie während des Installationsvorgangs optional einige Dienste erstellen möchten.

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

Datenintegrationsdienst

Der Datenintegrationsdienst ist ein Anwendungsdienst, der Profile in der Informatica-Domäne ausführt. Der Datenintegrationsdienst generiert Profilergebnisse für Ressourcen, die Sie zum Abrufen von Profilmetadaten eingerichtet haben, und schreibt die Profilergebnisse dann in das Profiling-Warehouse.

Zugeordnete 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 her, um Jobs auszuführen, wie zum Beispiel das Ausführen von Profilen. Beim Erstellen des Datenintegrationsdiensts geben Sie den Namen des Modellrepository-Diensts an.

Erforderliche 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 das Unternehmen generiert wurde. Wenn Sie den Datenintegrationsdienst erstellen, geben Sie Verbindungsdaten 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 vordefinierte logische

Datenobjekte und virtuelle Tabellen. Sie benötigen eine Datenobjekt-Cache-Datenbank, um die Leistung für SQL-Datendienstabfragen und Webdienst-Anfragen zu erhöhen.

Profiling-Warehouse

Speichert Profiling-Informationen, z. B. Profilergebnisse. Sie benötigen ein Profiling-Warehouse zum Speichern von Profiling-Statistiken, die von einem Ressourcen-Scan generiert werden.

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 von Catalog Administrator oder vom Datenintegrationsdienst auf ein Modellrepository-Objekt zugreifen, sendet der Client oder der Dienst eine Anfrage an den Modellrepository-Dienst. Der Modellrepository-Dienst ruft Metadaten aus den Modellrepository-Datenbanktabellen ab, fügt sie dort ein und aktualisiert sie.

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.

Katalogdienst

Der Katalogdienst ist ein Anwendungsdienst, der Enterprise Data Catalog in der Informatica-Domäne ausführt. Der Katalogdienst verwaltet die Verbindungen zwischen den Dienstkomponenten und den Benutzern, die Zugriff auf die Suchoberfläche von Enterprise Data Catalog und Catalog Administrator haben.

Der Katalog stellt eine indizierte Bestandsliste aller konfigurierten Datenobjekte in einem Unternehmen dar. Im Katalog finden Sie Metadaten und statistische Informationen, wie z. B. Profilstatistiken, Datenobjektbewertungen, Datendomänen und Datenbeziehungen.

Hinweis: Sie müssen die Hadoop-Clusterzertifikate in den Domänen-Truststore importieren, bevor Sie einen Katalogdienst für einen Hadoop-Cluster erstellen können, der das SSL-Protokoll verwendet.

Zugeordnete Dienste

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

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

Modellrepository-Dienst

Der Katalogdienst stellt eine Verbindung mit dem Modellrepository-Dienst her, um auf Informationen zur Ressourcenkonfiguration und zu Datendomänen aus dem Modellrepository zuzugreifen. Beim Erstellen des Katalogdiensts geben Sie den Namen des Modellrepository-Diensts an.

Datenintegrationsdienst

Der Katalogdienst stellt eine Verbindung mit dem Datenintegrationsdienst her, um Jobs auszuführen, z. B. zum Generieren von Profilstatistiken für die Ressourcen. Beim Erstellen des Katalogdiensts geben Sie den Namen des Datenintegrationsdiensts an.

Informatica-Cluster-Dienst

Wenn Sie Enterprise Data Catalog auf dem eingebetteten Cluster installiert haben, stellt der Katalogdienst eine Verbindung mit dem Informatica-Cluster-Dienst her, um alle eingebetteten Hadoop-Clusterdienste, Apache Ambari-Server und Apache Ambari-Agenten zu verwalten. Wenn Sie den Katalogdienst für eine Bereitstellung auf einem eingebetteten Cluster erstellen, müssen Sie den Namen des Informatica-Cluster-Diensts angeben.

Content-Management-Dienst

Der Katalogdienst verwendet den Content-Management-Dienst, um Referenzdaten für Datendomänen abzurufen, die Referenztabelle verwenden. Wenn Sie den Katalogdienst erstellen, können Sie optional den Namen des Content-Management-Diensts angeben.

Informatica-Cluster-Dienst

Der Informatica-Cluster-Dienst ist ein Anwendungsdienst, der alle Hadoop-Dienste, Apache Ambari-Server und Apache Ambari-Agenten auf einem eingebetteten Hadoop-Cluster ausführt und verwaltet. Wenn Sie bei der Installation von Enterprise Data Catalog den Bereitstellungsmodus für eingebettete Cluster auswählen, müssen Sie erst den Informatica-Cluster-Dienst erstellen, bevor Sie den Katalogdienst erstellen. Anschließend können Sie den Wert für den Informatica-Cluster-Dienst angeben, wenn Sie den Katalogdienst erstellen.

Content-Management-Dienst

Der Content-Managementdienst ist ein Anwendungsdienst für die Verwaltung von Referenzdaten. Ein Referenzdatenobjekt enthält einen Satz von Datenwerten, die Enterprise Data Catalog beim Ausführen der Datendomänenerkennung für Quelldaten sucht. Die Datendomänenerkennung ermittelt abgeleitete Geschäftssemantiken auf der Basis von Spaltendaten. Beispiele hierfür sind Sozialversicherungsnummer, Telefonnummer und Kreditkartennummer.

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

Zugeordnete 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 Übertragen von Daten zwischen Referenztabelle und externen Datenquellen. Beim Erstellen des Content-Management-Diensts

geben Sie den Namen des Datenintegrationsdiensts an. Sie müssen den Datenintegrationsdienst und den 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. Beim Erstellen des Content-Management-Diensts geben Sie den Namen des Modellrepository-Diensts an.

Erforderliche Datenbanken

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

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

Referenzdaten-Warehouse

Speichern Sie 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. Für die Verwaltung von Referenztabellendaten in Enterprise Data Catalog benötigen Sie ein Referenzdaten-Warehouse.

Überprüfen der Systemvoraussetzungen

Stellen Sie sicher, dass Ihre Umgebung 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>

Überprüfen der Installationsanforderungen für Dienste

Überprüfen Sie, ob Ihr Computer die Mindestsystemanforderungen für die Installation der Enterprise Data Catalog-Dienste erfüllt.

Die Systemanforderungen unterscheiden sich je nach den folgenden Bedingungen:

Wenn sich die Informatica-Domäne und der Hadoop-Cluster auf dem gleichen Computer befinden

Die Mindest-Arbeitsspeicheranforderung für das Linux-Betriebssystem beträgt 32 GB RAM. Der erforderliche Mindest-Festplattenspeicher beträgt 135 GB. Die Anzahl der benötigten CPU-Kerne beträgt 24.

Wenn sich die Informatica-Domäne und der Hadoop-Cluster auf verschiedenen Computern befinden

Die Mindest-Arbeitsspeicheranforderung für das Linux-Betriebssystem beträgt 24 GB für einen Cluster-Knoten und 32 GB für den Computer, auf dem die Informatica-Domäne ausgeführt wird. Der erforderliche Mindest-Festplattenspeicher beträgt 75 GB. Die Anzahl der benötigten CPU-Kerne beträgt 8 Kerne für einen Cluster-Knoten und 16 Kerne für den Computer, auf dem die Informatica-Domäne ausgeführt wird.

Überprüfen der Anforderungen an temporären Festplattenspeicher

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

Das Installationsprogramm benötigt 8 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 Enterprise Data Catalog-Dienste installieren.

In der folgenden Tabelle werden die von Enterprise Data Catalog verwendeten Ports beschrieben:

Porttyp	Beschreibung
Knotenport	Portnummer des während der Installation erstellten Knotens. Standardwert ist 6005.
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. Der JDBC/ODBC-Treiber für den SQL-Datendienst verwendet diesen Port ebenfalls. 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. Der HTTPS-Standardport ist 8443.
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.
Bereich von dynamischen Portnummern für Anwendungsdienste	Portnummernbereich, der Anwendungsdienstprozessen dynamisch zugewiesen werden kann, wenn diese gestartet werden. Wenn Sie einen Anwendungsdienst starten, der einen dynamischen Port verwendet, weist der Dienstmanager dem Dienstprozess dynamisch den ersten verfügbaren Port in diesem Bereich zu. Die Zahl der Ports in diesem Bereich muss mindestens doppelt so groß sein wie die Zahl der Anwendungsdienstprozesse, die auf dem Knoten laufen werden. Standardwerte sind 6014 bis 6114. Der Dienstmanager weist dem Modellrepository-Dienst dynamisch Portnummern aus diesem Bereich zu.

Porttyp	Beschreibung
HTTPS-Port für Hadoop-Verteilungen	Wenn Sie Enterprise Data Catalog in einer HTTPS-aktivierten Hadoop-Verteilung bereitstellen, gelten die folgenden Standardportnummern: - Cloudera. 7183 - Hortonworks. 8443 - Azure HDInsight. 8443
Statische Ports für Anwendungsdienste	Statischen Ports sind dedizierte Portnummern zugewiesen, die sich nicht ändern. Beim Erstellen des Anwendungsdiensts können Sie die Standardportnummer übernehmen oder die Portnummer manuell zuweisen. Die folgenden Dienste verwenden statische Portnummern: - Content-Management-Dienst. Der Standardwert ist 8105 für HTTP. - Datenintegrationsdienst. Der Standardwert ist 8095 für HTTP.

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	<p>Das Domänenkonfigurations-Repository unterstützt die folgenden Datenbanktypen:</p> <ul style="list-style-type: none"> - IBM DB2 UDB - Microsoft SQL Server - Microsoft Azure SQL-Datenbank - Oracle - Sybase ASE <p>Zulassen von 200 MB Speicherplatz für die Datenbank.</p>
Datenobjekt-Cache-Datenbank	<p>Die Datenobjekt-Cache-Datenbank unterstützt die folgenden Datenbanktypen:</p> <ul style="list-style-type: none"> - IBM DB2 UDB - Microsoft SQL Server - Microsoft Azure SQL-Datenbank - Oracle <p>Zulassen von 200 MB Speicherplatz für die Datenbank.</p> <p>Weisen Sie basierend auf der Menge der Daten, die Sie zwischenspeichern möchten, mehr Speicherplatz zu.</p>
Modellrepository	<p>Das Modellrepository unterstützt die folgenden Datenbanktypen:</p> <ul style="list-style-type: none"> - IBM DB2 UDB - Microsoft SQL Server - Microsoft Azure SQL-Datenbank - Oracle <p>Zulassen von 3 GB Speicherplatz für DB2. Lassen Sie 200 MB Festplattenspeicher für alle anderen Datenbanktypen zu.</p> <p>Weisen Sie basierend auf der Menge der Metadaten, die Sie speichern möchten, mehr Speicherplatz zu.</p>
Profiling-Warehouse	<p>Das Profiling-Warehouse unterstützt die folgenden Datenbanktypen:</p> <ul style="list-style-type: none"> - IBM DB2 UDB - Microsoft SQL Server - Microsoft Azure SQL-Datenbank - Oracle <p>Zulassen von 10 GB Speicherplatz für die Datenbank.</p>
Referenzdaten-Warehouse	<p>Das Referenzdaten-Warehouse unterstützt die folgenden Datenbanktypen:</p> <ul style="list-style-type: none"> - IBM DB2 UDB - Microsoft SQL Server - Microsoft Azure SQL-Datenbank - Oracle <p>Zulassen von 200 MB Speicherplatz für die Datenbank.</p>

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 einer Informatica-Domäne mit mehreren Knoten 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: <ul style="list-style-type: none"> - Datenintegrationsdienst - Modellrepository-Dienst - Katalogdienst - Content-Management-Dienst - Informatica-Cluster-Dienst Hinweis: Gilt für die eingebettete Hadoop-Bereitstellung auf HortonWorks.	2 CPUs mit mindestens 4 Kernen	16 GB	60 GB
Ein Knoten führt die folgenden Dienste aus: <ul style="list-style-type: none"> - Datenintegrationsdienst - Modellrepository-Dienst - Katalogdienst - Content-Management-Dienst Hinweis: Wenn Sie Enterprise Data Catalog auf einem Kerberos-fähigen vorhandenen Cluster unter Cloudera, HortonWorks oder Azure HDInsight installieren, wären die Mindestanforderungen 4 CPUs mit mindestens 4 Kernen, 32 GB Arbeitsspeicher und 60 GB Festplattenspeicher.	2 CPUs mit mindestens 4 Kernen	16 GB	60 GB

Aufzeichnen der Informatica-Domänen- und -Knoteninformationen

Wenn Sie die Enterprise Data Catalog-Dienste installieren, benötigen Sie Informationen über die Domäne, Knoten, Anwendungsdienste und Datenbanken, die Sie erstellen möchten.

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.

Die Namen von Domänen, Knoten und Anwendungsdiensten können Sie 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 außerdem Namen, die die Nutzung des Domänenobjekts in Enterprise Data Catalog vermitteln.

Weitere Informationen zu Benennungskonventionen für Datenobjekte finden Sie in folgendem Artikel über die schnelle Anwendung von optimalen Vorgehensweisen in Informatica auf dem Mein Support-Portal: [Informatica Platform Naming Conventions](#).

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
Content-Management-Dienst	CMS_<ORG>_<ENV>	CMS_FIN_DEV
Datenintegrationsdienst	DIS_<ORG>_<ENV>	DIS_ICC_DEV
Modellrepository-Dienst	MRS_<ORG>_<ENV>	MRS_FIN_DEV
Katalogdienst	CS_<ORG>_<ENV>	CS_HR_DEV
Informatica-Cluster-Dienst	ICS_<ORG>_<ENV>	ICS_FIN_DEV

Domäne

Bei der ersten Installation der Enterprise Data Catalog-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 maximal 128 Zeichen umfassen und muss im 7-Bit-ASCII-Format vorliegen. 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 Computer nur einen Netzwerknamen aufweist, verwenden Sie den Standardhostnamen. Der Hostname des Knotens darf keine Unterstriche (_) enthalten. Wenn der Computer mehrere Netzwerknamen aufweist, können Sie den Standardhostnamen ändern und einen alternativen Netzwerknamen verwenden. Wenn der Computer nur einen Netzwerknamen aufweist, verwenden Sie den Standardhostnamen. 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 mit dem Hostnamen des Computers identisch.	

Knoten

Wenn Sie die Enterprise Data Catalog-Dienste installieren, fügen Sie den Installationscomputer 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 werden soll. Wenn der Computer nur einen Netzwerknamen aufweist, verwenden Sie den Standardhostnamen. Der Hostname des Knotens darf keine Unterstriche (_) enthalten. Wenn der Computer mehrere Netzwerknamen aufweist, können Sie den Standardhostnamen ändern und einen alternativen Netzwerknamen verwenden. Wenn der Computer nur einen Netzwerknamen aufweist, verwenden Sie den Standardhostnamen. 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 mit dem Hostnamen des Computers identisch.			

Anwendungsdienste

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

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
Katalogdienst		
Content-Management-Dienst		
Datenintegrationsdienst		
Modellrepository-Dienst		
Informatica-Cluster-Dienst		

Sicherer Datenspeicher

Bei der Installation der Enterprise Data Catalog-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: <ul style="list-style-type: none"> - 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 ist das folgende Verzeichnis: <Enterprise Data Catalog-Installationsverzeichnis>/isp/config/keys	

Domänensicherheit

Wenn Sie die Informatica-Anwendungsdienste 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	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".	

Sicherheitsinformationen	Beschreibung	Wert
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.	

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	Pfad und Dateiname der Truststore-Datei für die sichere Datenbank.	
Datenbank-Truststore-Passwort	Passwort für die TrustStore-Datei.	

Sichere Verbindung für Informatica Administrator

Sie können optional eine sichere HTTPS-Verbindung für Informatica Administrator 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
Schlüsselspeicherpasswort	Ein Volltext-Passwort für die Schlüsselspeicherdatei.	
Schlüsselspeicherdatei-Verzeichnis	Der Speicherort der Schlüsselspeicherdatei.	

KAPITEL 3

Vorbereiten von Datenbanken für die Informatica-Domäne

Dieses Kapitel umfasst die folgenden Themen:

- [Vorbereiten von Datenbanken für die Informatica-Domäne – Übersicht, 38](#)
- [Einrichten von Datenbankbenutzerkonten, 39](#)
- [Datenbankanforderungen des Domänen-Konfigurations-Repositorys, 39](#)
- [Anforderungen für Datenobjekt-Cache-Datenbank, 42](#)
- [Modellrepository-Datenbankanforderungen, 43](#)
- [Anforderungen an das Profiling-Warehouse, 46](#)
- [Anforderungen des Referenzdaten-Warehouse, 47](#)

Vorbereiten von Datenbanken für die Informatica-Domäne – Übersicht

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
- Modellrepository
- Profiling-Warehouse
- Referenzdaten-Warehouse

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 Domänenkonfigurations-Repository und für die den Anwendungsdiensten zugeordneten Repository-Datenbanken ein.

Beachten Sie beim Einrichten der Benutzerkonten die folgenden Richtlinien:

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

Datenbankanforderungen des Domänenkonfigurations-Repositorys

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

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

Wenn Sie Enterprise Data Catalog installieren, geben Sie die Datenbank- und Benutzerkontoinformationen für das Domänenkonfigurations-Repository an. Das Installationsprogramm für Enterprise Data Catalog verwendet JDBC für die Kommunikation mit dem Domänenkonfigurations-Repository.

Das Domänenkonfigurations-Repository unterstützt die folgenden Datenbanktypen:

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

Lassen Sie 200 MB Speicherplatz.

IBM DB2-Datenbankanforderungen

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

- Wenn sich das Repository in einer IBM DB2-Datenbank befindet, überprüfen Sie, ob IBM DB2 Version 10.5 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

Parameter	Wert
applheapsz	8192
appl_ctl_heap_sz	8192
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-Tabellenalias für Repository-Tabellen. Stellen Sie sicher, dass für keine Tabellen in der Datenbank Tabellenalias erstellt wurden.

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

Der Standardwert für DynamicSections ist für die Repositories von Enterprise Data Catalog zu niedrig. Für Enterprise Data Catalog ist ein größeres DB2-Paket als der Standard erforderlich. Beim Einrichten der DB2-Datenbank für das Domänenkonfigurations-Repository oder ein Modellrepository müssen Sie den Parameter DynamicSections auf einen Wert von mindestens 3000 festlegen. Wenn der Parameter DynamicSections auf einen niedrigeren Wert festgelegt ist, kann es beim Installieren oder Ausführen von Enterprise Data Catalog-Diensten zu Problemen kommen.

Microsoft SQL Server-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository die folgenden Anleitungen:

- Geben Sie den Namen des Datenbankschemas an, wenn Sie Microsoft SQL Server als Modellrepository-Datenbank verwenden.
- Um Sperrkonflikte zu minimieren, legen Sie die Isolationsstufe „Momentaufnahmeisolation zulassen“ und „Lesen mit Commit“ auf ALLOW_SNAPSHOT_ISOLATION und READ_COMMITTED_SNAPSHOT fest. Führen Sie zum Festlegen der Isolationsstufe 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 Isolationsstufe für die Datenbank korrekt ist:

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

```
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 mindestens 8 K ein. Diese Konfiguration wird nur einmal vorgenommen und kann später nicht mehr geändert werden.

Die Datenbank für das Data Analyzer-Repository benötigt eine Seitengröße von mindestens 8 KB. Wenn Sie eine Data Analyzer-Datenbank in einer Sybase ASE-Instanz einrichten, deren Seitengröße kleiner als 8 KB ist, generiert Data Analyzer beim Ausführen von Berichten möglicherweise Fehler. Wenn die Seitengröße erhöht wird, lockert Sybase ASE die Zeilengrößenbeschränkung.

Data Analyzer enthält eine Klausel GROUP BY in der SQL-Abfrage für den Bericht. Beim Ausführen des Berichts speichert Sybase ASE alle GROUP BY- und Aggregatspalten in einer temporären Arbeitstabelle. Die maximale Größe für Indexzeilen in der Arbeitstabelle wird durch die Seitengröße der Datenbank beschränkt. Beispiel: Wenn Sybase ASE mit der Standard-Seitengröße von 2 KB installiert wird, darf die Indexzeilengröße 600 Byte nicht überschreiten. Die Klausel GROUP BY in der SQL-Abfrage der meisten Data Analyzer-Berichte generiert jedoch eine Indexzeilengröße von über 600 Byte.

- Stellen Sie sicher, dass der Datenbankbenutzer über die Berechtigungen CREATE TABLE und CREATE VIEW verfügt.
- Legen Sie „allow nulls by default“ auf TRUE fest.
- Aktivieren Sie die Option „Distributed Transaction Management (DTM)“ auf dem Datenbankserver.
- Erstellen Sie ein DTM-Benutzerkonto und weisen Sie dem Benutzer die Berechtigung dtm_tm_role zu. In der folgenden Tabelle sind die DTM-Konfigurationseinstellungen für den Wert dtm_tm_role aufgeführt:

DTM-Konfiguration	Sybase-Systemprozedur	Wert
Distributed Transaction Management-Berechtigung	sp_role "grant"	dtm_tm_role, <i>Benutzername</i>

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
- Microsoft Azure SQL-Datenbank
- 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-Tabellenalias für Repository-Tabellen. Stellen Sie sicher, dass für keine Tabellen in der Datenbank Tabellenalias 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 die folgenden Anleitungen:

- 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.

Modellrepository-Datenbankanforderungen

Enterprise Data Catalog-Dienste und Informatica-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
- Microsoft Azure SQL-Datenbank

- 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-Datenbank befindet, überprüfen Sie, ob IBM DB2 Version 10.5 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

Parameter	Wert
applheapsz	8192
appl_ctl_heap_sz	8192
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-Tabellenalias für Repository-Tabellen. Stellen Sie sicher, dass für keine Tabellen in der Datenbank Tabellenalias erstellt wurden.
- Aktualisieren Sie im Dienstprogramm DataDirect Connect for JDBC den Parameter DynamicSections auf 3000.

Der Standardwert für DynamicSections ist für die Repositories von Enterprise Data Catalog zu niedrig. Für Enterprise Data Catalog ist ein größeres DB2-Paket als der Standard erforderlich. Beim Einrichten der DB2-Datenbank für das Domänenkonfigurations-Repository oder ein Modellrepository müssen Sie den Parameter DynamicSections auf einen Wert von mindestens 3000 festlegen. Wenn der Parameter DynamicSections auf einen niedrigeren Wert festgelegt ist, kann es beim Installieren oder Ausführen von Enterprise Data Catalog-Diensten zu Problemen kommen.

Microsoft SQL Server-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository die folgenden Anleitungen:

- 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]
```

```
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. 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.

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
- Microsoft Azure SQL-Datenbank
- 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-Tabellenalias für Repository-Tabellen. Stellen Sie sicher, dass für keine Tabellen in der Datenbank Tabellenalias 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 die folgenden Anleitungen:

- 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.
- 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
- Microsoft Azure SQL-Datenbank
- 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-Tabellenalias für Repository-Tabellen. Stellen Sie sicher, dass für keine Tabellen in der Datenbank Tabellenalias 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 die folgenden Anleitungen:

- 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.

KAPITEL 4

Bereitstellungsmethoden

Dieses Kapitel umfasst die folgenden Themen:

- [Bereitstellungsmethoden \(Übersicht\), 49](#)
- [Bereitstellung auf einem eingebetteten Hadoop-Cluster Voraussetzungen, 49](#)
- [Voraussetzungen – Eingebetteter Cluster , 50](#)
- [Voraussetzungen – Vorhandener Cluster, 61](#)
- [Vorhandene Hadoop-Cluster-Bereitstellung, 63](#)
- [Vorbereiten der vorhandenen Hadoop-Clusterumgebung, 64](#)
- [Kerberos- und SSL-Setup für einen vorhandenen Cluster, 64](#)

Bereitstellungsmethoden (Übersicht)

Sie können Enterprise Data Catalog entweder in einer eingebetteten Hadoop-Distribution auf Hortonworks oder in einer vorhandenen Hadoop-Distribution auf Cloudera, Hortonworks oder Azure HDInsight bereitstellen. Bevor Sie die Option mit dem vorhandenen Hadoop-Cluster für die Bereitstellung von Enterprise Data Catalog auswählen, müssen Sie vor der Installation von Enterprise Data Catalog die Cluster-Umgebung von Cloudera, Hortonworks oder Azure HDInsight in Ihrem Unternehmen einrichten. Wenn Sie die Option mit dem eingebetteten Hadoop-Cluster auswählen, konfigurieren Sie den Hortonworks-Cluster beim Installieren von Enterprise Data Catalog.

Bereitstellung auf einem eingebetteten Hadoop-Cluster Voraussetzungen

Wenn Sie Enterprise Data Catalog auf einem eingebetteten Hadoop-Cluster installieren, können Sie Anwendungsdienste erstellen, z. B. den Modellrepository-Dienst, den Datenintegrationsdienst und den Katalogdienst.

Wenn Sie die eingebettete Hadoop-Verteilung auswählen, erstellt das Installationsprogramm für Enterprise Data Catalog den **Informatica-Cluster-Dienst**, einen Anwendungsdienst. Enterprise Data Catalog verwendet Apache Ambari, um den eingebetteten Hadoop-Cluster zu verwalten und zu überwachen. Der eingebettete Hadoop-Cluster für Enterprise Data Catalog unterstützt die Option für hohe Verfügbarkeit.

Die folgenden Komponenten der eingebetteten Hadoop-Clusterumgebungen von Enterprise Data Catalog unterstützen die Option für hohe Verfügbarkeit:

- HDFS
- HBase
- YARN
- Solr

Voraussetzungen – Eingebetteter Cluster

Bevor Sie Enterprise Data Catalog in einem eingebetteten Hadoop-Cluster installieren, müssen Sie sicherstellen, dass die Systemumgebung die Voraussetzungen für die Bereitstellung von Enterprise Data Catalog erfüllt.

Betriebssystemvoraussetzungen

In den folgenden Abschnitten finden Sie die Betriebssystemvoraussetzungen für Cluster-Knoten, bevor Sie Enterprise Data Catalog auf einem eingebetteten Cluster installieren:

- ["Allgemeine Betriebssystemvoraussetzungen für Red Hat Enterprise Linux und SUSE Linux Enterprise Server" auf Seite 50](#)
- ["Betriebssystemvoraussetzungen für Red Hat Enterprise Linux" auf Seite 52](#)
- ["Betriebssystemvoraussetzungen für SUSE Linux Enterprise Server" auf Seite 53](#)

Allgemeine Betriebssystemvoraussetzungen für Red Hat Enterprise Linux und SUSE Linux Enterprise Server

Sie können Enterprise Data Catalog auf einem Computer installieren, auf dem Red Hat Enterprise Linux Server oder SUSE Linux Enterprise Server ausgeführt werden.

Überprüfen Sie die folgenden allgemeinen Voraussetzungen sowohl für SUSE Linux Enterprise Server als auch für Red Hat Enterprise Linux Server:

- Stellen Sie sicher, dass es sich um ein 64-Bit-Betriebssystem handelt.
- Stellen Sie sicher, dass Sie `file` installiert haben.
- Stellen Sie sicher, dass `Bash` als Standard-Shell festgelegt ist.
- Wenn Sie ein Benutzerkonto ohne Root-Berechtigungen verwenden und den `sudo`-Zugriff entfernen möchten, stellen Sie sicher, dass `defaults requiretty` in `/etc/sudoers` auskommentiert ist.
- Wenn Sie ein Benutzerkonto ohne Root-Berechtigungen verwenden, stellen Sie sicher, dass der Hadoop-Benutzer über `sudo`-Berechtigungen verfügt.
- Stellen Sie sicher, dass Sie die Passwortabfrage für den Hadoop-Benutzer deaktivieren.
- Stellen Sie sicher, dass Sie `python-devel` installieren.
- Stellen Sie sicher, dass Sie `UMASK` auf `022` (`0022`) oder `027` (`0027`) festlegen.
- Stellen Sie sicher, dass Sie den vollqualifizierten Domännennamen (FQDN) für „hostname -f“ festlegen.
- Stellen Sie sicher, dass der Speicherort `/var` nicht über Schreibberechtigungen für alle verfügt.
- Stellen Sie sicher, dass Sie die Linux-Basis-Repositorys konfigurieren.

- Stellen Sie sicher, dass Sie das Befehlszeilen-Netzwerkdienstprogramm „netstat“ installieren.
- Überprüfen Sie, ob das Root-Verzeichnis (/) über mindestens 10 GB freien Festplattenspeicher verfügt.
- Wenn Sie Enterprise Data Catalog auf einem eingebetteten Cluster installieren und den Informatica-Clusterdienst an einem separaten Mount-Speicherort mounten möchten, vergewissern Sie sich, dass der Mount-Speicherort über mindestens 50 GB an freiem Festplattenspeicher verfügt.
- Stellen Sie sicher, dass das Flag NOEXEC nicht für das Dateisystem festgelegt ist, das auf dem Verzeichnis/`tmp` gemountet ist.
- Sie sollten sicherstellen, dass das /`tmp`-Verzeichnis über mindestens 20 GB an freiem Festplattenspeicher verfügt, um die Leistung zu verbessern.
- Stellen Sie sicher, dass Sie die Dienstprogramme `scp`, `curl`, `unzip`, `wget` und `tar` installieren.
- Stellen Sie sicher, dass das `home`-Verzeichnis mit Schreibberechtigungen versehen ist.
- Stellen Sie sicher, dass die konfigurierte Datei /`etc/hosts` Datei auf allen Computern den vollqualifizierten Domännennamen (FQDN) für die Computer enthält.
- Stellen Sie sicher, dass der NTP-Daemon (Network Time Protocol) synchronisiert ist und ausgeführt wird.
- Stellen Sie sicher, dass für das /`tmp`-Verzeichnis die Berechtigung „`chmod 777`“ konfiguriert ist.
- Stellen Sie sicher, dass für die Verzeichnisse / und /`var` nicht die Berechtigung `chmod 777` konfiguriert ist.
- Stellen Sie sicher, dass das /`var`-Verzeichnis über mindestens 2 GB freien Festplattenspeicher verfügt.
- Stellen Sie sicher, dass das /`usr`-Verzeichnis über mindestens 2 GB freien Festplattenspeicher verfügt.
- Stellen Sie sicher, dass Sie Selinux deaktiviert oder Selinux auf den uneingeschränkten Modus festgelegt haben.
- Stellen Sie sicher, dass /`etc/hosts` über einen Eintrag für die Loopback-Adresse `127.0.0.1 localhost localhost.domain.com` verfügt.
- Stellen Sie sicher, dass Sie für einen Benutzer ohne Root-Berechtigungen die Kernbegrenzung auf /`unlimited` festlegen.
- Wenn Sie als `workingDir /` konfigurieren, vergewissern Sie sich, dass für das unter den Verzeichnissen /`tmp` und /`var` gemountete Dateisystem das EXEC-Flag festgelegt ist.
- Wenn / nicht als `workingDir` konfiguriert ist, vergewissern Sie sich, dass das `workingDir`-Verzeichnis über die Lese-, Schreib- und Ausführungsberechtigung verfügt. Vergewissern Sie sich, dass außerdem das EXEC-Flag für das Verzeichnis festgelegt ist.
- Überprüfen Sie, ob Sie über die Schreibberechtigung für das Verzeichnis /`home` verfügen. Sie können die Berechtigung in der Datei /`etc/default/useradd` konfigurieren.
- Stellen Sie sicher, dass jeder Computer im Cluster den Eintrag `127.0.0.1 localhost localhost.localdomain` in der Datei /`etc/hosts` enthält.
- Überprüfen Sie, ob die Datei /`etc/hosts` die vollqualifizierten Hostnamen für alle Clusterknoten enthält. Stellen Sie alternativ sicher, dass Reverse-DNS-Lookup die vollqualifizierten Hostnamen für alle Clusterknoten zurückgibt.
- Überprüfen Sie, ob das Linux-Repository `postgresql` Version 8.14.18, Release 1.el6_4 oder spätere Versionen enthält.
- Stellen Sie sicher, dass Sie das Soft-Limit für maximale Benutzerprozesse auf 32000 oder mehr festlegen.
- Stellen Sie sicher, dass Sie das Hard-Limit für maximale Benutzerprozesse auf 32000 oder mehr festlegen.
- Sie müssen das Soft-Limit für maximale Benutzerprozesse auf 10000 oder mehr für die Clusterknoten festlegen.

- Sie müssen das Hard-Limit für maximale Benutzerprozesse auf 10000 oder mehr für die Clusterknoten festlegen.
- Überprüfen Sie auf jedem Hostcomputer, ob die folgenden Tools und Anwendungen verfügbar sind:
 - YUM und RPM (RHEL/CentOS/Oracle Linux)
 - Zypper
 - scp, curl, unzip, tar und wget
 - awk
 - OpenSSL Version 1.0.1e-30.el6_6.5.x86_64 oder höher.
Hinweis: Stellen Sie sicher, dass die \$PATH-Variable auf das Verzeichnis /usr/bin verweist, um die richtige Version von Linux OpenSSL zu verwenden.
- Wenn Enterprise Data Catalog auf einem eingebetteten Cluster installiert ist und Sie das Linux-Basis-Repository nicht konfiguriert haben oder über keine Internetverbindung verfügen, installieren Sie die folgenden Pakete:
 - Folgende RPMs auf dem Ambari-Server-Host:
 - postgresql-libs
 - postgresql-server
 - postgresql
 - Die folgenden RPMs auf allen Clusterknoten:
 - nc
 - redhat-lsb
 - psmisc
 - python-devel

Betriebssystemvoraussetzungen für Red Hat Enterprise Linux

Überprüfen Sie die folgenden Voraussetzungen für einen Red Hat Linux Enterprise Server, wenn Sie Enterprise Data Catalog auf einem Red Hat Enterprise Linux Server installieren möchten:

Betriebssystem	Voraussetzungen:
Red Hat Enterprise Linux Versionen 6 und 7	<ul style="list-style-type: none"> - Stellen Sie für Red Hat Enterprise Linux Version 7.0 sicher, dass Sie Sudo Version 1.8.16 oder höher verwenden. - Installieren Sie kernel-headers und kernel-devel. - Installieren Sie libtirpc-devel. - Installieren Sie openssl Version v1.0.1 Build 16 oder höher oder v1.0.2k. - Installieren Sie YUM. - Stellen Sie sicher, dass das Verzeichnis /etc/sysconfig/network vorhanden ist, und konfigurieren Sie die Leseberechtigung für das Verzeichnis. - /etc/sysconfig/network enthält denselben Eintrag wie der für „hostname -f“ konfigurierte Eintrag. - Installieren Sie Python Version 2.6.x oder 2.7.x. Gilt für Red Hat Enterprise Linux Version 6. - Installieren Sie Python Version 2.7.x. Gilt für Red Hat Enterprise Linux Version 7. - Deaktivieren Sie die SSL-Zertifikatsvalidierung.

Betriebssystemvoraussetzungen für SUSE Linux Enterprise Server

Überprüfen Sie die folgenden Voraussetzungen für einen SUSE Linux Enterprise Server, wenn Sie beabsichtigen, Enterprise Data Catalog auf einem SUSE Linux Enterprise Server zu installieren:

Betriebssystem	Voraussetzungen:
SUSE Linux Enterprise Server Versionen 11 und 12	<ul style="list-style-type: none">- Installieren Sie netcat-openbsd.- Installieren Sie kernel-default-devel.- Stellen Sie sicher, dass das Verzeichnis <code>/etc/HOSTNAME</code> vorhanden ist, und konfigurieren Sie die Leseberechtigung für das Verzeichnis.- Stellen Sie sicher, dass das Verzeichnis <code>/etc/HOSTNAME</code> denselben Eintrag enthält wie der für „hostname -f“ konfigurierte Eintrag.- Installieren Sie Zypper.- Installieren Sie die folgenden Versionen von Python:<ul style="list-style-type: none">- 2.6.8/2.6.9/2.7.x für SUSE Linux Version 11.- 2.7.x für SUSE Linux Version 12.- Aktualisieren Sie für SUSE Enterprise Linux Server 11 alle Hosts auf Python Version 2.6.8-0.15.1.- Wenn Sie die Installation von Enterprise Data Catalog unter SUSE Linux Enterprise Server 12 durchführen, müssen Sie die folgenden RPM-Paket-Manager (RPMs) auf allen Cluster-Knoten installieren:<ul style="list-style-type: none">- openssl-1.0.1c-2.1.3.x86_64.rpm- libopenssl1_0_0-1.0.1c-2.1.3.x86_64.rpm- libopenssl1_0_0-32bit-1.0.1c-2.1.3.x86_64.rpm- python-devel-2.6.8-0.15.1.x86_64- Installieren Sie libsappy nicht, wenn Sie Enterprise Data Catalog auf SUSE Linux Enterprise Server installieren.

Voraussetzungen für Hostknoten

Überprüfen Sie die folgenden Voraussetzungen für Hostknoten:

- Stellen Sie sicher, dass die passwortlose SSH vom Domänencomputer für den Apache Ambari-Server aktiviert ist.
- Stellen Sie sicher, dass die passwortlose SSH vom Apache Ambari-Server für alle Apache Ambari-Agents aktiviert ist.
- Stellen Sie sicher, dass die Anzahl der konfigurierten Apache Ambari-Agents eins oder mehr als zwei beträgt.

Voraussetzungen für die Bereitstellung von Enterprise Data Catalog auf mehreren Knoten

Überprüfen Sie die folgenden Voraussetzungen, um den Enterprise Data Catalog auf mehreren Knoten bereitzustellen:

- Stellen Sie sicher, dass Sie zum Starten aller Knoten dieselben Benutzeranmeldedaten verwenden.
- Aktivieren Sie die passwortlose SSH-Anmeldung für alle Hostknoten beim Clusterknoten.
- Stellen Sie sicher, dass Sie auf allen Knoten die gleiche Version der Apache Ambari-Binärdateien verwenden.
- Stellen Sie sicher, dass Sie auf allen Knoten die gleichen binären Ressourcendateien verwenden.
- Stellen Sie sicher, dass Sie den Informatica-Cluster-Dienst und den Katalogdienst auf separaten Knoten konfigurieren.

Voraussetzungen für Cluster-Knoten

Die Clusterknoten müssen die folgenden Anforderungen erfüllen:

Knotentyp	Mindestanforderungen
Masterknoten	<ul style="list-style-type: none">- 4 CPUs.- Ungenutzter verfügbarer Arbeitsspeicher: 12 GB.- Verfügbarer Gesamtarbeitsspeicher: 16 GB.- 60 GB Festplattenspeicher.
Slave-Knoten	<ul style="list-style-type: none">- 4 CPUs.- Ungenutzter verfügbarer Arbeitsspeicher: 12 GB.- Verfügbarer Gesamtarbeitsspeicher: 16 GB.- Festplattenspeicher: 60 GB.

Voraussetzungen für Apache Ambari

Überprüfen Sie die folgenden Voraussetzungen für Apache Ambari:

- Apache Ambari erfordert bestimmte Ports, die während der Installation geöffnet und verfügbar sind, um mit den von Apache Ambari bereitgestellten und verwalteten Hosts zu kommunizieren. Sie müssen die iptables vorübergehend deaktivieren, um diese Anforderung zu erfüllen.
- Überprüfen Sie, ob die Arbeitsspeicher- und Paketanforderungen für Apache Ambari erfüllt sind. Weitere Informationen erhalten Sie in der HortonWorks-Dokumentation.

Voraussetzungen für Apache Ranger

Vor der Bereitstellung von Enterprise Data Catalog auf Clustern, auf denen Apache Ranger aktiviert ist, müssen Sie die folgenden Berechtigungen für den Informatica-Domänenbenutzer konfigurieren:

- Schreibberechtigung für den HDFS-Ordner.
- Berechtigung zum Senden von Anwendungen an die YARN-Warteschlange.

Grenzwert für den Dateideskriptor

Überprüfen Sie, ob die maximale Anzahl geöffneter Dateideskriptoren mindestens 10.000 beträgt. Verwenden Sie den Befehl `ulimit`, um den aktuellen Wert zu überprüfen und ihn bei Bedarf zu ändern.

Voraussetzungen für SSL

Wenn Sie das SSL-Protokoll für den Cluster aktivieren möchten, überprüfen Sie die folgenden Voraussetzungen:

- Wenn für den Cluster SSL aktiviert ist, müssen Sie das Ambari-Serverzertifikat in den Truststore der Informatica-Domäne importieren.
- Bei einem SSL-fähigen Cluster wird empfohlen, SSL für die Informatica-Domäne und die Anwendungsdienste zu aktivieren.
- Sie müssen die Hadoop-Clusterzertifikate in den Domänen-Truststore importieren, bevor Sie einen Katalogdienst für einen Hadoop-Cluster erstellen können, der das SSL-Protokoll verwendet.

- Wenn Sie für eine Enterprise Data Catalog-Bereitstellung in einer Informatica-Domäne mit mehreren Knoten SSL-Authentifizierung aktivieren möchten, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:
 - Exportieren Sie die Datei Default.keystore jedes Knotens in die Datei infa_truststore.jks auf allen Knoten.
 - Stellen Sie sicher, dass Default.keystore für jeden Hostknoten eindeutig ist.
 - Kopieren Sie Default.keystore an einen eindeutigen Speicherort für jeden Knoten.
 - Wenn sich der Informatica-Clusterdienst und der Katalogdienst auf verschiedenen Knoten befinden, exportieren Sie das Apache Ambari Server-Zertifikat auf allen Knoten nach infa_truststore.jks.

Voraussetzungen für Kerberos

Wenn Sie die Kerberos-Authentifizierung für den Cluster aktivieren möchten, überprüfen Sie die folgenden Voraussetzungen:

- Bevor Sie Kerberos-Authentifizierung für den Katalogdienst aktivieren können, müssen Sie die Keytab-Dateien des Benutzers und des Hosts zusammenführen.
- Legen Sie den Wert `udp_preference_limit` auf **1** fest (in `$INFA_HOME/services/shared/security/krb5.conf`).
- Stellen Sie sicher, dass das KDC-Zertifikat im Domänenknoten vorhanden ist.
- Wenn Sie für eine Enterprise Data Catalog-Bereitstellung in einer Informatica-Domäne mit mehreren Knoten Kerberos-Authentifizierung aktivieren möchten, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:
 - Stellen Sie sicher, dass alle Domänenknoten in den folgenden Verzeichnissen die Datei `krb5.conf` enthalten:
 - `$INFA_HOME/services/shared/security/`
 - `/etc/` in allen Clusterknoten.
 - Stellen Sie sicher, dass dieselbe `krb5.conf`-Datei in der Informatica-Domäne und auf den Clusterknoten verwendet wird.
 - Stellen Sie sicher, dass die Datei `/etc/hosts` aller Cluster- und Domänenknoten den `krb`-Hosteintrag und einen Hosteintrag für andere Knoten enthält.
 - Installieren Sie `krb5-workstation` in allen Domänenknoten.
 - Stellen Sie sicher, dass die Keytab-Datei an einem gemeinsamen Speicherort auf allen Domänenknoten vorhanden ist.
- Stellen Sie sicher, dass Sie die folgenden erforderlichen Pakete installieren, bevor Sie Kerberos für Enterprise Data Catalog unter Red Hat Enterprise Linux aktivieren:
 - `krb5-workstation`
 - `krb5-libs`
- Stellen Sie für Enterprise Data Catalog auf SUSE Linux Enterprise Server sicher, dass Sie die folgenden erforderlichen Pakete installieren:
 - `krb5-server`
 - `krb5-client`

Informatica-Cluster-Dienst

Der Informatica-Cluster-Dienst ist ein Anwendungsdienst, der alle Hadoop-Dienste, Apache Ambari-Server und Apache Ambari-Agenten in einem eingebetteten Hadoop-Cluster ausführt und verwaltet. Wenn Sie die

Bereitstellung in einem eingebetteten Cluster auswählen, müssen Sie zuerst den Informatica-Cluster-Dienst erstellen, bevor Sie den Katalogdienst erstellen. Anschließend können Sie den Wert des Informatica-Cluster-Diensts an den Katalogdienst übergeben.

Der Informatica-Cluster-Dienst verteilt die Hortonworks-Binärdateien und startet die erforderlichen Hadoop-Dienste auf den Hosts, auf denen der eingebettete Cluster ausgeführt wird.

Sie können den Informatica-Cluster-Dienst auf Hosts bereitstellen, auf denen Centrify aktiviert ist. Centrify wird in eine vorhandene Active Directory-Infrastruktur integriert, um die Benutzerauthentifizierung auf Remote-Hosts unter Linux zu verwalten.

Hinweis: Informatica lässt sich nicht zur Verwaltung oder Generierung von Schlüsseltabellen mit Centrify integrieren.

Sie können den Informatica-Cluster-Dienst auf Hosts bereitstellen, die den Zugriff mit den folgenden JSch SSH-Verschlüsselungsalgorithmen ermöglichen:

In der folgenden Tabelle sind die unterstützten Methoden und Algorithmen aufgeführt:

Methoden	Algorithmen
Schlüsselaustausch	<ul style="list-style-type: none"> - diffie-hellman-group-exchange-sha1 - diffie-hellman-group1-sha1 - diffie-hellman-group14-sha1 - diffie-hellman-group-exchange-sha256 - ecdh-sha2-nistp256 - ecdh-sha2-nistp384 - ecdh-sha2-nistp521
Chiffrieren	<ul style="list-style-type: none"> - blowfish-cbc - 3des-cbc - aes128-cbc - aes192-cbc - aes256-cbc - aes128-ctr - aes192-ctr - aes256-ctr - 3des-ctr - arcfour - arcfour128 - arcfour256
MAC	<ul style="list-style-type: none"> - hmac-md5 - hmac-sha1 - hmac-md5-96 - hmac-sha1-96
Host-Schlüsseltyp	<ul style="list-style-type: none"> - ssh-dss - ssh-rsa - ecdsa-sha2-nistp256 - ecdsa-sha2-nistp384 - ecdsa-sha2-nistp521

Informatica-Cluster-Dienstablauf

Der Informatica-Cluster-Dienst ist ein ISP-Dienst, der den eingebetteten Hadoop-Cluster in Enterprise Data Catalog verwaltet.

Nachdem der Informatica-Cluster-Dienst erstellt wurde, führt er die folgenden Aktionen aus:

1. Starten des Apache Ambari-Servers und zugehöriger Agenten.

- Erstellen der Hadoop-Dienste und Überwachungssysteme auf Apache Ambari einschließlich HDFS, Apache Zookeeper, Yarn und zugehöriger Überwachungsdienste.
- Starten der Hadoop-Dienste.
- Wenn Sie Enterprise Data Catalog herunterfahren, beendet der Informatica-Cluster-Dienst alle Hadoop-Dienste und den Apache Ambari-Server und seine Agenten.

Erstellen eines Informatica-Clusterdiensts

Sie können den Informatica-Clusterdienst generieren, wenn Sie Enterprise Data Catalog installieren oder den Anwendungsdienst manuell mit Informatica Administrator erstellen.

Wenn Sie Enterprise Data Catalog auf mehreren Knoten bereitstellen möchten, stellen Sie sicher, dass Sie den Informatica-Clusterdienst und den Katalogdienst auf separaten Knoten konfigurieren.

- Wählen Sie im Administrator Tool eine Domäne aus, und klicken Sie auf die Registerkarte **Dienste und Knoten**.

- Klicken Sie im Menü "Aktionen" auf **Neu > Informatica-Clusterdienst**.

Das Dialogfeld **Neuer Informatica-Clusterdienst – Schritt 1 von 4** wird geöffnet.

- Konfigurieren Sie die allgemeinen Eigenschaften im Dialogfeld.

In der folgenden Tabelle werden die Eigenschaften beschrieben:

Eigenschaft	Beschreibung
Name	Name des Diensts. Der Name unterliegt nicht der Groß- und Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf maximal 128 Zeichen umfassen und nicht mit @ beginnen. Der Name darf keine Leerzeichen enthalten. Die Zeichen im Namen müssen mit der Codepage des Modellrepositorys kompatibel sein, das Sie mit dem Katalogdienst verknüpfen. Der Name darf folgende Zeichen nicht enthalten: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () []
Beschreibung	Beschreibung des Diensts. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Domäne, in der der Anwendungsdienst ausgeführt wird.
Lizenz	Dem Informatica-Clusterdienst zuzuweisende Lizenz. Wählen Sie die Lizenz aus, die Sie mit Enterprise Data Catalog installiert haben.
Knoten	Knoten in der Informatica-Domäne, auf dem der Informatica-Clusterdienst ausgeführt wird. Wenn Sie den Knoten ändern, müssen Sie den Informatica-Clusterdienst deaktivieren und erneut aktivieren.
Sicherungsknoten	Wenn die Lizenz hohe Verfügbarkeit einschließt, sind dies die Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist.

- Klicken Sie auf **Weiter**.

Das Dialogfeld **Neuer Informatica-Clusterdienst – Schritt 2 von 4** wird geöffnet.

- Konfigurieren Sie die Sicherheitseigenschaften im Dialogfeld.

In der folgenden Tabelle werden die Eigenschaften beschrieben:

Eigenschaft	Beschreibung
HTTP-Port	Eine eindeutige HTTP-Portnummer, die für jeden Datenintegrationsdienst-Prozess verwendet wird. Die Standardeinstellung ist 9075.
TLS (Transport Layer Security) aktivieren	Wählen Sie die Option zum Aktivieren von TLS für den Informatica-Clusterdienst.
HTTPS-Port	Portnummer für die HTTPS-Verbindung. Erforderlich, wenn Sie die Option TLS (Transport Layer Security) aktivieren auswählen.
Schlüsselspeicherdatei	Pfad und Dateiname der Schlüsselspeicherdatei. Die Schlüsselspeicherdatei enthält die Schlüssel und Zertifikate, die bei Verwendung des SSL-Sicherheitsprotokolls mit Catalog Administrator erforderlich sind. Erforderlich, wenn Sie die Option TLS (Transport Layer Security) aktivieren auswählen.
Schlüsselspeicherpasswort	Passwort für die Schlüsselspeicherdatei. Erforderlich, wenn Sie die Option TLS (Transport Layer Security) aktivieren auswählen.
SSL-Protokoll	Zu verwendendes Secure Sockets Layer-Protokoll.

6. Klicken Sie auf **Weiter**.

Das Dialogfeld **Neuer Informatica-Clusterdienst – Schritt 3 von 4** wird geöffnet.

7. Konfigurieren Sie im Dialogfeld die Eigenschaften des Hadoop-Clusters.

In der folgenden Tabelle werden die Eigenschaften beschrieben:

Eigenschaft	Beschreibung
Hadoop-Gateway-Host	Host, auf dem der Apache Ambari-Server läuft.
Hadoop-Gateway-Port	Web-Port für den Apache Ambari-Server.
Gateway-Benutzer	Benutzername für den Apache Ambari-Server.
Hadoop-Knoten	Hosts, auf denen die Apache Ambari-Agenten laufen.
Standardpasswort überschreiben	Wählen Sie diese Option aus, wenn Sie das Standardpasswort für den Cluster ändern möchten. Geben Sie das neue Passwort im Textfeld Admin-Passwort für Ambari-Server ein.

Eigenschaft	Beschreibung
Aktivieren der Kerberos-Authentifizierung	Wählen Sie diese Option, um die Kerberos-Authentifizierung für den Cluster zu aktivieren.
KDC-Typ	Wählen Sie einen der folgenden Kerberos KDC-Typen (Key Distribution Center) aus, wenn Sie die Option Kerberos-Authentifizierung aktivieren ausgewählt hatten: - Active Directory. Wählen Sie diese Option aus, wenn Sie das Active Directory-KDC verwenden möchten. - MIT KDC. Wählen Sie diese Option, wenn Sie MIT KDC verwenden möchten. Geben Sie nach Auswahl des KDC-Typs die folgenden Optionen an. - KDC-Host. Name des KDC-Hostcomputers. - Host des Administratorservers. Der Name des Administratorservers, auf dem der KDC-Server gehostet wird. - Bereich. Name des Kerberos-Bereichs auf dem Computer, auf dem der KDC-Server gehostet wird. - Administratorprinzipal. Der Kerberos-Administratorprinzipal. - Administratorpasswort. Das Kerberos-Administratorpasswort. - LDAP-URL. Diese Eigenschaft gilt für Microsoft Active Directory und stellt die URL zum LDAP-Serververzeichnis dar. - Container-DN. Diese Eigenschaft gilt für Microsoft Active Directory und stellt den Distinguished Name des Containers dar, zu dem der Benutzer gehört. - KDC-Zertifikatspfad. Stellen Sie bei Verwendung von KDC mit Active Directory den Pfad des KDC-Zertifikats auf dem Computer in der Informatica-Domäne bereit.

8. Klicken Sie auf **Weiter**.

Das Dialogfeld **Neuer Informatica-Clusterdienst – Schritt 4 von 4** wird geöffnet.

9. Konfigurieren Sie die Domänensicherheitsoptionen für den Informatica-Clusterdienst.

In der folgenden Tabelle werden die Eigenschaften beschrieben:

Eigenschaft	Beschreibung
Domäne ist SSL-aktiviert	Geben Sie an, ob die Informatica-Domäne für SSL aktiviert ist.
Domänen-Truststore-Dateispeicherort	Speicherort der Domänen-Truststore-Datei.
Domänen-Truststore-Passwort	Passwort für die Domänen-Truststore-Datei.
Dienst aktivieren	Wählen Sie diese Option aus, um den Informatica-Clusterdienst unmittelbar nach dem Erstellen des Diensts zu aktivieren.

10. Klicken Sie auf **Fertig stellen**.

Hinweis: Nachdem Sie die Sicherheitsoptionen des Informatica-Clusterdiensts in Informatica Administrator aktualisiert haben, starten Sie den Informatica-Clusterdienst neu.

Überprüfen Sie vor dem Aktivieren des Informatica-Clusterdiensts die folgenden Voraussetzungen, die auf den für den Cluster konfigurierten Sicherheitsoptionen basieren:

- Kerberos-fähiger Cluster:
 - Sie müssen den KDC-Hostnamen (Key Distribution Center) und die IP-Adresse auf allen Clusterknoten und Domänencomputern im Verzeichnis `/etc/hosts` konfigurieren
 - Vergewissern Sie sich, dass sich die Datei "krb5.conf" auf allen Clusterknoten und Domänencomputern im Verzeichnis `/etc` befindet.

- SSL-fähiger Cluster:
 - Stellen Sie bei einem SSL-fähigen Cluster sicher, dass die Datei des Domänen-Truststores konfiguriert und an einen gemeinsamen Speicherort kopiert wird, auf den alle Clusterknoten zugreifen können.
 - Wenn sich der Solr-Schlüsselspeicher und das Passwort vom Schlüsselspeicher und Passwort des Informatica-Clusterdiensts unterscheiden, müssen Sie das öffentliche Zertifikat von Solr auf alle Clusterknoten exportieren und das Zertifikat in den YARN-Truststore und den Domänen-Truststore importieren.

Vorbereiten der eingebetteten Hadoop-Clusterumgebung

Vor der Installation von Enterprise Data Catalog auf einem eingebetteten Hadoop-Cluster müssen Sie mehrere Validierungsprüfungen durchführen.

Führen Sie die folgenden Schritte aus, bevor Sie Enterprise Data Catalog in einer eingebetteten Hadoop-Clusterumgebung installieren:

- Konfigurieren Sie die Datei `/etc/hosts` auf jedem Computer, sodass Sie vollqualifizierte Domännennamen haben. Informatica empfiehlt für den Hostnamen folgendes Format in Kleinbuchstaben: `<ip-adresse des computers> <vollqualifizierter name> <alias>`.

Hinweis: Führen Sie den Befehl `#hostname -f` aus, um den konfigurierten Hostnamen zu überprüfen.
- Richten Sie SSH-Verbindungen (Secure Shell) ohne Passwortschutz zwischen den folgenden Komponenten ein:
 - Vom Informatica-Cluster-Dienst zum Hadoop-Gateway.
 - Vom Hadoop-Gateway zu den Apache-Hadoop-Knoten.
- Stellen Sie sicher, dass die Datei `/etc/hosts` auf dem Computer, der die Informatica-Domäne hostet, Einträge für alle Hadoop-Hosts enthält.

Verwaltung von eingebetteten Clusterknoten

Ein Hadoop-Cluster verfügt über eine Reihe von Computern, die für die Ausführung von Hadoop-Anwendungen und -Diensten konfiguriert sind. Ein typischer Hadoop-Cluster enthält einen Masterknoten und mehrere Slave- oder Worker-Knoten. Der Masterknoten führt die Master-Daemons JobTracker und NameNode aus. Ein Slave-Knoten führt die DataNode- und TaskTracker-Daemons aus. In kleinen Clustern kann der Masterknoten auch die Slave-Daemons ausführen.

Cluster mit hoher Verfügbarkeit

Sie können die Hochverfügbarkeitsoption für die HDFS-, HBase-, YARN- und Solr-Komponenten der eingebetteten Hadoop-Clusterumgebung verwenden. Wenn Sie den Informatica-Cluster-Dienst auf einem hochverfügbaren Cluster mit mehreren Knoten einrichten, benötigen Sie mindestens drei Knoten, damit Enterprise Data Catalog korrekt funktioniert. Wenn Sie den Informatica-Cluster-Dienst bereits auf einem einzelnen Knoten eingerichtet haben, können Sie den Cluster nicht durch Hinzufügen weiterer Knoten zum Cluster hochverfügbar machen.

Wenn der eingebettete Cluster nur drei Knoten enthält, verteilt Enterprise Data Catalog alle Master- und Slave-Dienste auf allen drei Knoten. Wenn der eingebettete Cluster mehr als drei Knoten enthält, wählt Enterprise Data Catalog automatisch die obersten drei Knoten mit der höchsten Systemkonfiguration als Masterknoten aus. Die restlichen Knoten dienen als Slave-Knoten. Wenn Sie dem eingebetteten Cluster Knoten hinzufügen, dienen die neu hinzugefügten Knoten als Slave-Knoten. Die Knoten, die Sie dem Cluster hinzufügen, müssen die Mindest-Konfigurationsanforderungen für Slave-Knoten erfüllen.

Cluster ohne hohe Verfügbarkeit

Sie können den Informatica-Cluster-Dienst auf einem einzelnen Knoten einrichten, der nicht hochverfügbar ist. In solchen Fällen verbleiben die Master- und Worker-Knoten auf demselben Knoten. Sie können den Informatica-Cluster-Dienst nicht aufschalten, wenn Sie einen einzelnen Knoten zu einem bestehenden Cluster mit einem Knoten hinzufügen oder den Informatica-Cluster-Dienst mit zwei Knoten einrichten.

Knoten löschen

Sie können Knoten aus dem eingebetteten Cluster löschen, sofern sie die folgenden Bedingungen erfüllen:

- Ein Masterknoten kann nicht gelöscht werden.
- Sie können einen Knoten nicht löschen, wenn die Anzahl der Live-Datenknoten im Cluster beim Löschen des Knotens kleiner als drei ist.

Voraussetzungen – Vorhandener Cluster

Bevor Sie Enterprise Data Catalog in einem vorhandenen Hadoop-Cluster installieren, müssen Sie sicherstellen, dass die Systemumgebung die Voraussetzungen für die Bereitstellung von Enterprise Data Catalog erfüllt.

Voraussetzungen für Hostknoten

Überprüfen Sie auf jedem Hostcomputer, ob die zip- und unzip-Dienstprogramme verfügbar sind.

Voraussetzungen für Clusterknoten

Überprüfen Sie die folgenden Voraussetzungen auf allen Clusterknoten:

- Die OpenSSL-Version auf den Clusterknoten ist openssl-1.0.1e-30.el6_6.5.x86_64 oder höher oder v1.0.2k.
- Sie müssen Java Development Kit (JDK) 1.8 auf allen Clusterknoten installieren.
- Stellen Sie sicher, dass der Grenzwert für maximale Benutzerprozesse auf 32000 oder größer festgelegt ist.

Voraussetzungen für Apache Ranger

Bevor Sie Enterprise Data Catalog auf Clustern bereitstellen, auf denen Apache Ranger aktiviert ist, stellen Sie sicher, dass der Informatica-Domänenbenutzer über die erforderliche Berechtigung zum Einreichen von Anwendungen in der YARN-Warteschlange verfügt.

Grenzwert für den Dateideskriptor

Überprüfen Sie, ob die maximale Anzahl geöffneter Dateideskriptoren mindestens 10.000 beträgt. Verwenden Sie den Befehl `ulimit`, um den aktuellen Wert zu überprüfen und ihn bei Bedarf zu ändern.

Voraussetzungen für SSL

Wenn Sie das SSL-Protokoll für den Cluster aktivieren möchten, überprüfen Sie die folgenden Voraussetzungen:

- Wenn Sie den Katalogdienst erstellen, der eine Verbindung mit einem SSL-fähigen vorhandenen Cluster herstellt, müssen Sie die folgenden Eigenschaften konfigurieren:
 - Pfad zu Solr-Schlüsselspeicherdatei und Passwort.
 - Importieren Sie die Hadoop-Cluster-Zertifikate in den Truststore der Informatica-Domäne.
- Wenn für den Cluster SSL aktiviert ist, stellen Sie sicher, dass Sie SSL für die Informatica-Domäne und den Katalogdienst aktivieren.
- Wenn Sie einen neuen Solr-Schlüsselspeicher erstellen, stellen Sie sicher, dass Sie das öffentliche Solr-Zertifikat auf alle Cluster-Knoten exportieren.
- Stellen Sie sicher, dass Sie die öffentlichen Zertifikate der Informatica-Domäne in alle YARN-Truststores importieren.
- Wenn Sie für eine Enterprise Data Catalog-Bereitstellung in einer Informatica-Domäne mit mehreren Knoten SSL-Authentifizierung aktivieren möchten, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:
 - Exportieren Sie die Datei `Default.keystore` jedes Knotens in die Datei `infa_truststore.jks` auf allen Knoten.
 - Stellen Sie sicher, dass `Default.keystore` für jeden Hostknoten eindeutig ist.
 - Kopieren Sie `Default.keystore` an einen eindeutigen Speicherort für jeden Knoten.

Voraussetzungen für Kerberos

Wenn Sie Kerberos für den Cluster aktivieren möchten, überprüfen Sie die folgenden Voraussetzungen:

- Bevor Sie Kerberos aktivieren, müssen Sie die folgenden erforderlichen Pakete installieren:
 - `krb5-workstation`
 - `krb5-libs`
- Denken Sie daran, die folgenden Voraussetzungen zu konfigurieren:
 - Eine Keytab-Datei, die alle Benutzer in LDAP enthält.
 - Name der Kerberos-Domäne.
 - HDFS-NameNode und YARN-Ressourcenmanager-Dienstprinzipale..
- Stellen Sie sicher, dass Sie die HTTP-Keytab-Datei mit den Keytab-Dateien des Benutzers und Hosts zusammenführen.
- Wenn Sie die Protokolldateien an einem gemeinsamen Speicherort zusammenfassen möchten, erstellen Sie das Verzeichnis `service-logs` unter `/Informatica/LDM/<service cluster name>/` und legen Sie den Benutzer des Dienstclusters als Besitzer des Verzeichnisses fest, wenn der Cluster für Kerberos aktiviert ist.

Hinweis: Falls der Cluster nicht für Kerberos aktiviert ist, erstellen Sie das Verzeichnis `service-logs` unter `/informatica/ldm/<Dienst-Clustername>/` und legen Sie den Domänenbenutzer als Besitzer des Verzeichnisses fest.
- Wenn der Cluster nicht für Kerberos aktiviert ist, erstellen Sie das Verzeichnis `<Domänenbenutzername>` unter `/user` und legen Sie den Domänenbenutzer als Besitzer des Verzeichnisses fest.

Hinweis: Wenn der Cluster für Kerberos aktiviert ist, erstellen Sie das Verzeichnis `<Dienst-Clustername>` unter `/user` und legen Sie den Benutzer des Dienst-Clusters als Besitzer des Verzeichnisses fest. Wenn

der Cluster nicht für Kerberos aktiviert ist, legen Sie den Domänenbenutzer als Besitzer des Verzeichnisses fest.

- Wenn Sie für eine Enterprise Data Catalog-Bereitstellung in einer Informatica-Domäne mit mehreren Knoten Kerberos-Authentifizierung aktivieren möchten, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:
 - Stellen Sie sicher, dass alle Domänenknoten in den folgenden Verzeichnissen die Datei `krb5.conf` enthalten:
 - `$INFA_HOME/services/shared/security/`
 - `/etc/`
 - Stellen Sie sicher, dass die Datei `/etc/hosts` aller Cluster- und Domänenknoten den krb-Hosteintrag und einen Hosteintrag für andere Knoten enthält.
 - Installieren Sie `krb5-workstation` in allen Domänenknoten.
 - Stellen Sie sicher, dass die Keytab-Datei an einem gemeinsamen Speicherort auf allen Domänenknoten vorhanden ist.
 - Stellen Sie sicher, dass der Benutzer des Dienstclusters auf allen Clusterknoten konfiguriert ist.

Voraussetzungen für die Informatica-Domäne

Achten Sie darauf, dass Sie die Informatica-Domäne nicht auf einem Knoten im vorhandenen Hadoop-Cluster erstellen.

Benutzerberechtigungen

Konfigurieren Sie die folgenden Berechtigungen für Benutzerkonten, wenn Sie einen Enterprise Data Catalog auf einem vorhandenen Cluster bereitstellen möchten:

- Stellen Sie sicher, dass Sie für Eigentümer, Gruppen und andere Lese-, Schreib- und Ausführungsberechtigungen auf HDFS-Verzeichnisse vergeben.
- Wenn Sie Enterprise Data Catalog auf einer Cloudera Hadoop-Distribution bereitstellen möchten, müssen Sie dem Cloudera-Benutzerkonto, das Sie zum Starten des Katalogdiensts verwenden, in Cloudera Manager eine der folgenden Rollen zuordnen:
 - Operator
 - Configurator
 - Cluster Administrator
 - Navigator Administrator
 - Full Administrator

Vorhandene Hadoop-Cluster-Bereitstellung

Sie können Enterprise Data Catalog auf einem Hadoop-Cluster bereitstellen, den Sie auf Cloudera, HortonWorks oder Azure HDInsight eingerichtet haben. Wenn Sie die Kerberos-Authentifizierung in Ihrem Unternehmen zur Authentifizierung von Benutzern und Diensten in einem Netzwerk aktiviert haben, können Sie die Informatica-Domäne für die Verwendung der Kerberos-Netzwerkauthentifizierung konfigurieren.

Sie müssen Zookeeper-, HDFS- und Yarn-Spezifikationen konfigurieren, wenn Sie Enterprise Data Catalog auf einem vorhandenen Hadoop-Cluster in Ihrem Unternehmen installieren. Der Katalogdienst verwendet die

folgenden Spezifikationen und startet die folgenden Dienste und Komponenten auf dem Hadoop-Cluster als YARN-Anwendung:

- Solr Version 5.2.1
- HBase Version 0.98
- Scanner-Komponenten

Vorbereiten der vorhandenen Hadoop-Clusterumgebung

Vor der Installation von Enterprise Data Catalog auf einem vorhandenen Hadoop-Cluster müssen Sie mehrere Validierungsprüfungen durchführen.

Führen Sie die folgenden Schritte aus, bevor Sie Enterprise Data Catalog für die Verwendung eines vorhandenen Clusters installieren:

- Erstellen Sie vor dem Erstellen des Katalogdiensts erst die folgenden Verzeichnisse in HDFS:

```
- /Informatica/LDM/<Dienst-Clustername>  
- /user/<Benutzername>
```

Dabei ist `<Dienst-Clustername>` der Name des Dienst-Clusters, den Sie beim Erstellen des Katalogdiensts eingeben müssen, und `<Benutzername>` der Benutzername des Informatica-Domänenbenutzers.

- Ersetzen Sie `<Benutzername>` durch den Informatica-Domänenbenutzer, der Besitzer der Verzeichnisse / `Informatica/LDM/<Dienst-Clustername>` und `/user/<Benutzername>` ist.

Kerberos- und SSL-Setup für einen vorhandenen Cluster

Sie können Enterprise Data Catalog auf einem vorhandenen Cluster installieren, der die Kerberos-Netzwerkauthentifizierung verwendet, um Benutzer und Dienste in einem Netzwerk zu authentifizieren. Enterprise Data Catalog unterstützt auch die SSL-Authentifizierung für die sichere Kommunikation im Cluster.

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.

Informatica unterstützt weder bereichsübergreifende Kerberos-Authentifizierung noch Kerberos-Authentifizierung mit mehreren Bereichen. Der Serverhost, die Client-Computer und der Kerberos-Authentifizierungsserver müssen sich im selben Bereich befinden.

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.

Voraussetzungen für die SSL-Authentifizierung

Stellen Sie sicher, dass der vorhandene Cluster die folgenden Anforderungen erfüllt, bevor Sie die SSL-Authentifizierung im Cluster aktivieren können:

- Informatica-Domäne ist im SSL-Modus konfiguriert.
- Die Cluster- und YARN-REST-Endpunkte sind Kerberos-aktiviert.
- Erstellen Sie eine Schlüsselspeicherdatei für die Apache Solr-Anwendung auf allen Knoten im Cluster. Importieren Sie öffentliche Zertifikate von Apache Solr-Schlüsselspeicherdateien auf allen Hosts in alle Truststore-Dateien, die für HDFS und YARN konfiguriert sind. Dieser Schritt ist für Apache Spark- und Scanner-Jobs erforderlich, um eine Verbindung zur Apache Solr-Anwendung herzustellen.
- Importieren Sie die öffentlichen Zertifikate von Apache Solr- und YARN-Anwendungen in die Truststore-Datei der Informatica-Domäne. Dieser Schritt ist erforderlich, damit der Katalogdienst eine Verbindung zu YARN- und Solr-Anwendungen herstellen kann.
- Importieren Sie die öffentlichen Zertifikate der Informatica-Domäne und des Katalogdiensts in den YARN-Truststore.
- Importieren Sie das öffentliche Zertifikat des Katalogdiensts in den Truststore der Informatica-Domäne.
- Führen Sie die folgenden Schritte aus, wenn Sie Enterprise Data Catalog auf einem vorhandenen Hortonworks Version 2.5-Cluster bereitstellen möchten, der keine SSL-Authentifizierung unterstützt:
 1. Konfigurieren Sie die folgenden Eigenschaften in der Datei `/etc/hadoop/conf/ssl-client.xml`:
`ssl.client.truststore.location` und `ssl.client.truststore.password`.
 2. Vergewissern Sie sich, dass der Wert für `ssl.client.truststore.location` auf das Verzeichnis `/opt` und nicht auf das Verzeichnis `/etc` festgelegt ist. Sie müssen den vollständigen Pfad zur Truststore-Datei für die Eigenschaft `ssl.client.truststore.location` konfigurieren. Sie können den Wert beispielsweise in ähnlicher Form festlegen wie `/opt/truststore/infa_truststore.jks`.
 3. Exportieren Sie das in der Informatica-Domäne verwendete Schlüsselspeicherzertifikat.
 4. Importieren Sie das Schlüsselspeicherzertifikat in die Truststore-Datei der Informatica-Domäne.
 5. Platzieren Sie die Domain-Truststore-Datei in allen Hadoop-Knoten im Verzeichnis `/opt`.
Beispiel: `/opt/truststore/infa_truststore.jks`.
 6. Öffnen Sie die Datei `/etc/hadoop/conf/ssl-client.xml`.
 7. Ändern Sie die Eigenschaften `ssl.client.truststore.location` und `ssl.client.truststore.password`.

Voraussetzungen für die Kerberos-Authentifizierung

Führen Sie die folgenden Schritte aus, bevor Sie die Kerberos-Authentifizierung für den vorhandenen Cluster aktivieren:

- Erstellen Sie die folgenden Benutzer in der LDAP-Sicherheitsdomäne, in der `<Benutzername>` der Dienst-Clustername ist.
 - `<Benutzername>@KERBEROSDOMAIN.COM`
 - `<Benutzername>/<Hostname>@KERBEROSDOMAIN.COM`

Hinweis: Erstellen Sie die Benutzer-ID für alle Hosts im Cluster.

 - `HTTP/<Hostname>@KERBEROSDOMAIN.COM`

Hinweis: Erstellen Sie die Benutzer-ID für alle Hosts im Cluster.

- Erstellen Sie eine Keytab-Datei mit Anmeldeinformationen für alle in LDAP erstellten Benutzer. Sie können Keytab-Dateien für jeden Benutzer im KDC-Server erstellen und sie dann mit dem Befehl `ktutil` zusammenführen, um eine einzige Keytab-Datei zu erstellen.
- Erstellen Sie in HDFS die folgenden Ordner, die Enterprise Data Catalog als Datenverzeichnisse für den Katalogdienst verwendet: `/Informatica/LDM/<Benutzername>` und `/user/<Benutzername>`.
- Ändern Sie den Besitzer dieser beiden Ordner in `<Benutzername>`.
- Erstellen Sie einen lokalen Benutzer mit dem Benutzernamen `<Benutzername>` auf allen Hosts im Cluster. Dieser Schritt ist erforderlich, um die Anwendung auf YARN als Benutzer zu starten, der für den Katalogdienst konfiguriert ist.
- Richten Sie den Parameter `udp_preference_limit` in der Kerberos-Konfigurationsdatei `krb5.conf` ein und legen Sie ihn auf 1 fest. Dieser Parameter legt das Protokoll fest, das Kerberos beim Senden einer Meldung an das KDC verwendet. Legen Sie `udp_preference_limit = 1` fest, damit TCP immer verwendet wird. Die Informatica-Domäne unterstützt nur das TCP-Protokoll. Wenn der Parameter `udp_preference_limit` auf einen anderen Wert festgelegt wurde, wird die Informatica-Domäne eventuell unerwartet heruntergefahren.

Teil III: Installation von Enterprise Data Catalog

- [Installation von Enterprise Data Catalog-Diensten, 68](#)

KAPITEL 5

Installation von Enterprise Data Catalog-Diensten

Dieses Kapitel umfasst die folgenden Themen:

- [Übersicht über die Installation von Enterprise Data Catalog-Diensten, 68](#)
- [Installieren der Enterprise Data Catalog-Dienste im Konsolenmodus, 70](#)
- [Installieren von Enterprise Data Catalog im automatischen Modus, 108](#)
- [Installieren der Anwendungsdienste für Enterprise Data Catalog im automatischen Modus, 128](#)
- [Sichern der Passwörter in der Eigenschaftendatei, 129](#)

Übersicht über die Installation von Enterprise Data Catalog-Diensten

Sie können die Enterprise Data Catalog-Dienste auf einem Linux-Computer installieren. Sie können das Installationsprogramm im Konsolen- oder im unbeaufsichtigten Modus ausführen.

Führen Sie die Vorinstallationsaufgaben zur Vorbereitung auf die Installation durch. Sie können die Enterprise Data Catalog-Dienste auf mehreren Computern installieren. Der Installationsprozess erstellt einen Dienst namens Informatica, der als Daemon unter Linux ausgeführt wird. Beim Starten des Informatica-Diensts wird der Dienstmanager gestartet; dieser verwaltet alle Domänenvorgänge.

Nach der Installation können Sie sich mit Informatica Administrator bei der Domäne anmelden und die Anwendungsdienste konfigurieren.

Fortsetzen einer unvollständigen Installation

Wenn die Installation aufgrund eines Fehlers, einer Unterbrechung oder eines unbeabsichtigten Beendens des Installationsprogramms nicht abgeschlossen wurde, können Sie die Installation an der Stelle fortsetzen, an der sie gestoppt wurde. Stellen Sie sicher, dass die Informatica-Domäne ausgeführt wird, bevor Sie die Installation fortsetzen. Um die Installation fortzusetzen, führen Sie den Befehl `./install.sh` aus.

Wenn die Installation beim Erstellen eines der Anwendungsdienste angehalten wird, behält das Installationsprogramm die von Ihnen angegebenen Werte bei. Wenn Sie die Installation fortsetzen, fordert Sie das Installationsprogramm auf, die beibehaltenen Werte zu bestätigen, und fährt dann mit der Bereitstellung der Lizenz fort. Wenn Sie einen Anwendungsdienst erstellt und aktiviert haben, fährt das Installationsprogramm mit dem nächsten Schritt fort.

Fortsetzen der Installation

Wenn der Installationsvorgang mittendrin angehalten wird, können Sie die Installation ab dem Fehler fortsetzen oder beenden.

Bevor Sie das Installationsprogramm fortsetzen können, müssen Sie die folgenden Voraussetzungen erfüllen:

- Überprüfen Sie in der im Verzeichnis `<INFA_HOME>` befindlichen Installationsprotokolldatei, ob die Informatica-Domäne und ein Anwendungsdienst erstellt wurden. Der Name der Installationsprotokolldatei hat folgende Syntax: `Informatica_<Version>_Services_.log<Zeitstempel>`
- Stellen Sie sicher, dass Sie die Datei `installInst.obj` nicht löschen, die sich im Verzeichnis `tools` unter dem Installationsverzeichnis befindet.
- Wenn Sie die automatische Installation verwendet haben, stellen Sie sicher, dass die Eigenschaft `RESUME_INSTALLATION` in der Datei `SilentInput.properties` auf `true` festgelegt ist.

Führen Sie die folgenden Schritte aus, um die Installation fortzusetzen:

1. Öffnen Sie eine Eingabeaufforderung und navigieren Sie zum Speicherort der Installationsdateien.
2. Um die Installation fortzusetzen, führen Sie den Befehl `./install.sh` aus. Wenn Sie den automatischen Modus für die Installation verwendet haben, führen Sie `silentInstall.sh` aus, um die Installation fortzusetzen.
3. Wenn das Installationsprogramm ausgeführt wird, werden Sie möglicherweise gefragt, ob Sie den vorherigen Installationsvorgang fortsetzen möchten.
 - Wenn Sie die Installation fortsetzen möchten, geben Sie **2** ein.
 - Wenn Sie die Installation nicht fortsetzen möchten, geben Sie **1** ein. Der Standardwert ist **1**.

Bevor Sie die Installation fortsetzen, überprüft das Installationsprogramm die Anwendungsdienste, die Sie vor dem Stoppen des Installationsprogramms konfiguriert hatten.

Erstellen oder Anfügen einer Domäne

Bei der Erstinstallation müssen Sie eine Domäne erstellen. Treten Sie einer Domäne bei, wenn Sie die Installation auf mehreren Computern durchführen 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 Computers. Eine Domäne enthält einen oder mehrere Knoten.

Erfolgt die Installation auf mehreren Computern, 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.

Wenn Sie die Enterprise Data Catalog-Dienste installieren, erstellen Sie einen Knoten auf dem Computer. Sie können eine Domäne erstellen und den Knoten dieser neuen Domäne hinzufügen. Wenn Sie keine neue Domäne erstellen möchten, können Sie den Knoten mit einer anderen Domäne verknüpfen.

Wenn Sie einer Domäne beitreten, können Sie den Knoten, den Sie erstellen, als Gateway-Knoten konfigurieren. Beim Erstellen eines Gateway-Knotens können Sie die Option zum Aktivieren einer sicheren HTTPS-Verbindung zu Informatica Administrator auswählen.

Installieren der Enterprise Data Catalog-Dienste im Konsolenmodus

Sie können die Enterprise Data Catalog-Dienste im Konsolenmodus unter Linux installieren.

Beim Ausführen des Installationsprogramms im Konsolenmodus stellen die Wörter "Beenden" und "Zurück" reservierte Wörter dar. Verwenden Sie sie daher nicht als Eingabetext.

Sicheres Verzeichnis für den Verschlüsselungsschlüssel und die Konfigurationsdateien

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 `nodemeta.xml`-Datei. Das Installationsprogramm weist unter Linux 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. 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

Dieses Verzeichnis wird nicht von Enterprise Data Catalog verwendet.

Das Installationsprogramm weist die folgenden Berechtigungen zu den Verzeichnissen und den Dateien in den Verzeichnissen zu:

Verzeichnisberechtigungen

Der Eigentümer des Verzeichnisses verfügt über `-wx`-Berechtigungen zum Verzeichnis, jedoch über keine `r`-Berechtigung. Der Eigentümer des Verzeichnisses ist das Benutzerkonto, das zum Ausführen des Installationsprogramms verwendet wird. Die Gruppe, zu der der Eigentümer gehört, verfügt auch über `-wx`-Berechtigungen zum Verzeichnis, jedoch über keine `r`-Berechtigung.

Beispiel: Das Benutzerkonto `ediga` ist Eigentümer des Verzeichnisses und gehört zur `infaadmin`-Gruppe. Das `ediga`-Benutzerkonto und die `infaadmin`-Gruppe verfügen über die folgenden Berechtigungen: `-wx--wx---`

Das `ediga`-Benutzerkonto und die `infaadmin`-Gruppe kann in Dateien im Verzeichnis schreiben und diese ausführen. Sie können die Liste der Dateien im Verzeichnis nicht anzeigen, allerdings können sie eine bestimmte Datei nach dem Namen auflisten.

Wenn Sie den Namen einer Datei im Verzeichnis kennen, können Sie die Datei aus dem Verzeichnis auf einen anderen Speicherort kopieren. Wenn Sie den Namen der Datei nicht kennen, müssen Sie die Berechtigung für das Verzeichnis ändern, um die Leseberechtigung hinzuzufügen, bevor Sie die Datei kopieren können. Sie können den Befehl `chmod 730` verwenden, um dem Eigentümer des Verzeichnisses und der Unterverzeichnisse eine Leseberechtigung zu gewähren.

Beispiel: Sie müssen die Verschlüsselungsschlüsseldatei mit dem Namen `siteKey` in ein temporäres Verzeichnis kopieren, um sie für einen anderen Knoten in der Domäne zugänglich zu machen. Führen Sie den Befehl `chmod 730` für das Verzeichnis `<Informatica-Installationsverzeichnis>/isp/config` aus, um die folgenden Berechtigungen zuzuweisen: `"rwx-wx---`". Anschließend können Sie die Verschlüsselungsschlüsseldatei aus dem Unterverzeichnis `/keys` in ein anderes Verzeichnis kopieren.

Nachdem Sie die Dateien kopiert haben, ändern Sie die Berechtigungen für das Verzeichnis wieder in Schreib- und Ausführungsberechtigungen. Sie können den Befehl `chmod 330` zum Entfernen der Leseberechtigung verwenden.

Hinweis: Verwenden Sie die Option `-R` nicht, um die Berechtigungen für das Verzeichnis und die Dateien rekursiv zu ändern. Das Verzeichnis und die Dateien im Verzeichnis verfügen über verschiedene Berechtigungen.

Dateiberechtigungen

Der Eigentümer der Dateien im Verzeichnis verfügt über `rwx`-Berechtigungen für die Dateien. Der Eigentümer der Dateien im Verzeichnis ist das Benutzerkonto, das zum Ausführen des Installationsprogramms verwendet wird. Die Gruppe, zu der der Eigentümer gehört, enthält auch `rwx`-Berechtigungen für die Dateien im Verzeichnis.

Der Eigentümer und die Gruppe verfügen über vollen Zugriff auf die Datei und kann die Datei im Verzeichnis anzeigen oder bearbeiten.

Hinweis: Sie müssen den Namen der Datei kennen, um die Datei auflisten oder bearbeiten zu können.

Installieren durch 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 den Befehl `./install.sh` aus, um das Installationsprogramm zu starten.
Im Installationsprogramm wird eine Meldung angezeigt, in der Sie dazu aufgefordert werden, die Informatica-Dokumentation zu lesen, bevor Sie mit der Installation fortfahren.
4. Wählen Sie **J**, um die Installation fortzusetzen.
5. Wählen Sie **1**, um Produkte der Informatica Big Data-Suite zu installieren.
6. Wählen Sie **1**, um das Tool zur Systemüberprüfung vor der Installation auszuführen. Das Tool überprüft, ob Ihr Computer die Mindest-Systemanforderungen für die Installation oder Aktualisierung von Informatica erfüllt.
Hinweis: Wenn Sie sicher sind, dass Ihr Computer die Mindest-Systemanforderungen für die Installation oder Aktualisierung von Informatica erfüllt, können Sie diesen Schritt überspringen.
7. Wählen Sie **3**, um Informatica zu installieren.
8. Wählen Sie **2**, um den Installations- bzw. Aktualisierungsbedingungen zuzustimmen.
9. Drücken Sie **2**, um zu bestätigen, dass Sie wissen, dass Version 10.2.2 für die Big Data-Produktsuite spezifisch ist, und mit der Installation fortzufahren.
10. Wählen Sie **2**, um Informatica-Anwendungsdienste mit Enterprise Data Catalog zu installieren.
Das Installationsprogramm fordert Sie auf, zu bestätigen, dass die aktuelle Version der Informatica-Anwendungsdienste nicht auf dem Knoten installiert ist.
11. Wählen Sie **1**, wenn Sie nicht die aktuelle Version der Informatica-Anwendungsdienste installiert haben. Andernfalls drücken Sie **2**.
12. Wählen Sie den Hadoop-Clustertyp für Enterprise Data Catalog aus. Wählen Sie **2**, um Enterprise Data Catalog in einer eingebetteten Hadoop-Verteilung bereitzustellen. Wählen Sie **1**, um Enterprise Data Catalog in einer vorhandenen Hadoop-Verteilung bereitzustellen.

- Wenn Sie die eingebettete Hadoop-Verteilung ausgewählt haben, geben Sie nach der Konfiguration der Informatica-Domäne, des Modellrepository-Diensts und des Datenintegrationsdiensts folgende Informationen an:

Option	Beschreibung
SSH-Benutzername	Benutzername für die SSH-Verbindung (Secure Shell) ohne Passwortschutz.
Informatica-Cluster-Dienstname	Name des Informatica-Cluster-Diensts für den eingebetteten Cluster.
Informatica-Cluster-Dienstport	Portnummer für den Informatica-Cluster-Dienst.
Ambari-Serverhost.	Hostinformationen für den Ambari-Server. Ambari ist ein webbasiertes Tool für die Bereitstellung, Verwaltung und Überwachung von Apache Hadoop-Clustern, welches die Unterstützung für Hadoop HDFS, Hadoop MapReduce, Hive, HBase und ZooKeeper beinhaltet.
Durch Komma getrennte Ambari-Agent-Hosts	Gilt für die Hochverfügbarkeit. Wenn Sie mehrere Ambari-Agent-Hosts verwenden, geben Sie die kommagetrennten Werte der Namen der Ambari-Agent-Hosts an.
Ambari-Web-Port	Nummer des Ports, auf dem der Ambari-Server ausgeführt werden muss.
Katalogdienstname	Name des Katalogdiensts.
Katalogdienstport	Portnummer des Katalogdiensts.
Schlüsseltabellen-Speicherort	Gilt für einen Kerberos-aktivierten Cluster. Speicherort der zusammengeführten Benutzer- und Host-Keytab-Datei.
Kerberos-Konfigurationsdatei	Gilt für einen Kerberos-aktivierten Cluster. Speicherort der Kerberos-Konfigurationsdatei.

- Geben Sie die folgenden Details an, wenn Sie einen vorhandenen Cluster auswählen:

Eigenschaft	Beschreibung
Hadoop-Verteilung	Wählen Sie eine der folgenden Optionen aus: <ul style="list-style-type: none"> - ClouderaManager - HDInsight - Hortonworks
Cluster-URL	Vollqualifizierter Hostname für den Zugriff auf den Cluster.
Cluster-URL-Benutzername	Benutzername für den Zugriff auf den Cluster.
Cluster-URL-Passwort	Passwort für den Cluster-URL-Benutzernamen.

- Wenn Sie die vorhandene Hadoop-Distribution als `ClouderaManager` oder `Hortonworks` ausgewählt haben, geben Sie die folgenden Informationen an:

Option	Beschreibung
Katalogdienstname	Name des Katalogdiensts.
Katalogdienstport	Portnummer des Katalogdiensts.
URI des Yarn-Ressourcenmanagers	Der Dienst innerhalb von Hadoop, der die MapReduce-Aufgaben an bestimmte Knoten im Cluster sendet. Verwenden Sie das folgende Format: <code><hostname>:<port></code> Wobei <ul style="list-style-type: none"> • <code>hostname</code> der Name bzw. die IP-Adresse des Yarn-Ressourcenmanagers ist. • <code>port</code> ist der Port, den der Yarn-Ressourcenmanager auf Remoteprozeduraufrufe (RPC) abhört.
Yarn-Ressourcenmanager-HTTP-URI	Der HTTP-URI-Wert für den Yarn-Ressourcenmanager.
URI des Yarn-Ressourcenmanager-Schedulers	Der Scheduler-URI-Wert für den Yarn-Ressourcenmanager.
Zookeeper-Cluster-URI	Der URI für die Zookeeper-Dienste, bei dem es sich um einen besonders leistungsfähigen Koordinationsdienst für verteilte Anwendungen handelt.
HDFS-NameNode-URI	Der URI für den Zugriff auf HDFS. Verwenden Sie das folgende Format, um den NameNode-URI in der Cloudera-Verteilung anzugeben: <code>hdfs://<namenode>:<port></code> Wobei <ul style="list-style-type: none"> • <code><namenode></code> der Hostname oder die IP-Adresse von NameNode ist. • <code><Port></code> der Port ist, den der NameNode auf Remoteprozeduraufrufe (RPC) abhört.
Dienst-Clustername	Name des Dienst-Clusters. Stellen Sie vor dem Abschluss der Installation sicher, dass ein Verzeichnis <code>/Informatica/LDM/<ServiceClusterName></code> in HDFS vorhanden ist. Hinweis: Wenn Sie keinen Dienst-Clusternamen angeben, betrachtet Enterprise Data Catalog <code>DomainName_CatalogServiceName</code> als Standardwert. Das Verzeichnis <code>/Informatica/LDM/<DomainName>_<CatalogServiceName></code> muss sich dann in HDFS befinden. Andernfalls kann der Katalogdienst fehlschlagen.
HTTP-URI des Verlaufsservers	HTTP-URI für den Zugriff auf den Verlaufsserver.
Ist der Cluster sicher?	Legen Sie diese Eigenschaft auf einen der folgenden Werte fest, wenn Sie einen vorhandenen Cluster verwenden, der sicher ist: <ul style="list-style-type: none"> • 1: Gibt an, dass der vorhandene Cluster nicht sicher ist. • 2: Gibt an, dass der vorhandene Cluster sicher ist. Der Standardwert ist 1.

Option	Beschreibung
Ist der Cluster SSL-aktiviert?	<p>Nur anwendbar, wenn Sie die Hadoop-Distribution als <code>Hortonworks</code> und <code>ClouderaManager</code> ausgewählt haben.</p> <p>Legen Sie diese Eigenschaft auf einen der folgenden Werte fest, wenn ein vorhandener Cluster für SSL aktiviert ist:</p> <ul style="list-style-type: none"> • 1: Gibt an, dass der vorhandene Cluster nicht für SSL aktiviert ist. • 2: Gibt an, dass der vorhandene Cluster für SSL aktiviert ist. <p>Der Standardwert ist 1.</p>
Aktivieren der Kerberos-Authentifizierung	<p>Nur anwendbar, wenn Sie die Hadoop-Distribution als <code>Hortonworks</code> und <code>ClouderaManager</code> ausgewählt haben.</p> <p>Legen Sie diese Eigenschaft auf einen der folgenden Werte fest, wenn ein vorhandener Cluster für Kerberos aktiviert ist:</p> <ul style="list-style-type: none"> • 1: Gibt an, dass der vorhandene Cluster nicht für Kerberos aktiviert ist. • 2: Gibt an, dass der vorhandene Cluster für Kerberos aktiviert ist.

Je nach den von Ihnen festgelegten Einstellungen erstellt Enterprise Data Catalog einen Informatica-Cluster-Dienst für die eingebettete Hadoop-Distribution.

13. Drücken Sie die **Eingabetaste**, um fortzufahren.
14. Wählen Sie **2**, wenn das Installationsprogramm die Informatica-Anwendungsdienste basierend auf der Größe der Daten, die Sie bereitstellen möchten, optimieren soll.
Im Installationsprogramm werden die folgenden Optionen für verschiedene Datengrößen angezeigt:
 - Sandbox
 - Einfach
 - Standard
 - Hohe Parallelität und hohes Volumen
15. Geben Sie den Pfad und Dateinamen des Informatica-Lizenzschlüssels ein und drücken Sie die **Eingabetaste**.
16. 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.
17. Wählen Sie **2**, um das Dienstprogramm für die Vorabüberprüfung auszuführen. Das Dienstprogramm unterstützt Sie bei der Validierung der Voraussetzungen für die Installation von Enterprise Data Catalog in einem eingebetteten Cluster. Außerdem validiert das Dienstprogramm die Konfiguration der Informatica-Domäne, der Cluster-Hosts und der Hadoop-Clusterdienste.
Das Installationsprogramm fordert Sie auf, zu bestätigen, dass Sie die Kerberos-Authentifizierung für den Cluster aktivieren möchten.
18. Wählen Sie **2**, wenn Sie die Kerberos-Authentifizierung für den Cluster aktivieren möchten, und geben Sie die folgenden Details an:
 - a. **Keytab-Speicherort.** Speicherort der zusammengeführten Benutzer- und Host-Keytab-Datei.
 - b. **Kerberos-Konfigurationsdatei.** Speicherort der Kerberos-Konfigurationsdatei.

19. Geben Sie den Gateway-Benutzernamen ein und drücken Sie die **Eingabetaste**. Der Standardwert ist **root**.
20. Geben Sie den Gateway-Hostnamen für den Informatica-Hadoop-Cluster in folgendem Format ein: `<hostname>.<FQDN>` und drücken Sie die **Eingabetaste**.
21. Geben Sie die durch Kommas getrennte Liste von Informatica-Hadoop-Cluster-Knoten wie gezeigt im folgenden Format ein: `<hostname>.<FQDN>, <Hostname1>.<FQDN>, <Hostname2>.<FQDN>` und drücken Sie die **Eingabetaste**.
22. Geben Sie den Gateway-Port des Informatica-Hadoop-Clusters ein und drücken Sie die **Eingabetaste**. Der Standardwert ist **8080**.
Achten Sie zur Vermeidung eines Portkonflikts darauf, dass Sie Oracle nicht mit Port 8080 auf demselben Computer konfigurieren, auf dem der Informatica-Cluster-Dienst ausgeführt wird.
23. Geben Sie den Pfad zum Arbeitsverzeichnis ein und drücken Sie die **Eingabetaste**. Der Pfad gibt den Speicherort an, in dem Sie den Informatica-Cluster-Dienst bereitstellen möchten.
Das Installationsprogramm startet das Vorabüberprüfungs-Dienstprogramm.
24. Drücken Sie die **Eingabetaste**, um nach der Ausführung des Dienstprogramms für die Vorabüberprüfung fortzufahren.
25. Überprüfen Sie die Installationsinformationen und drücken Sie die **Eingabetaste**, um fortzufahren.
Das Installationsprogramm kopiert die Enterprise Data Catalog-Dateien in das Installationsverzeichnis. Sie werden aufgefordert, eine Domäne zu erstellen oder einer Domäne beizutreten.
26. 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.
27. 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.
28. 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
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 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	<p>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.</p> <p>1 – Von Installationsprogramm generierten Schlüsselspeicher verwenden 2 – Schlüsselspeicherdatei und Passwort eingeben</p> <p>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/</p>

- c. Wenn Sie den Schlüsselspeicher festlegen, geben Sie das Passwort und den Speicherort der Schlüsselspeicherdatei ein.
29. Wählen Sie **2**, wenn Sie Single Sign-On mithilfe der SAML-Authentifizierung für Enterprise Data Catalog-Anwendungen aktivieren möchten.
30. Geben Sie die URL des SAML-Identitätsanbieters (IdP) ein und drücken Sie die **Eingabetaste**.
 Informationen zu den Konfigurationsschritten, die Sie nach der Installation von Enterprise Data Catalog ausführen müssen, finden Sie im Abschnitt *Konfigurieren von Single Sign-On mithilfe der SAML-Authentifizierung*.
 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 **Domänenkonfigurations-Repository** angezeigt.
31. 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
1 – Standardmäßige SSL-Zertifikatsdateien 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.
2 – 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.

32. 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.

33. 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.

34. Geben Sie an, ob ein sicheres Domänenkonfigurations-Repository erstellt werden soll.

In einer mit dem SSL-Protokoll gesicherten Datenbank können Sie ein Domänen-Konfigurations-Repository erstellen. Um ein Domänenkonfigurations-Repository in einer sicheren Datenbank zu erstellen, wählen Sie 1.

Zum Erstellen eines Domänen-Konfigurations-Repositorys in einer ungesicherten Datenbank drücken Sie 2.

35. Wenn Sie kein sicheres Domänenkonfigurations-Repository erstellen möchten, 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	Das Passwort für die Domänen-Konfigurationsdatenbank. Der Dienstname bei Oracle- und IBM DB2-Datenbanken oder Datenbankname bei Microsoft Microsoft SQL Server und Sybase ASE.
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 für die JDBC-Verbindungszeichenfolge für die Datenbanken:

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.

36. 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	Schließen Sie die JDBC-Verbindung für die sichere Datenbank ab, indem Sie den Hostnamen, die Portnummer und die Parameter für die sichere Datenbank eingeben.

Neben dem Hostnamen und der Portnummer für den Datenbankserver müssen Sie die folgenden sicheren Datenbankparameter 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` einstellen.

Sie können folgende Syntax für die Verbindungszeichenfolgen verwenden:

- **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.

37. Wenn die Datenbank ein Domänenkonfigurations-Repository für eine frühere Domäne enthält, überschreiben Sie die Daten oder richten 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.

38. Geben Sie im Abschnitt **Domänensicherheit – Verschlüsselungsschlüssel** das Schlüsselwort und das Verzeichnis des Verschlüsselungsschlüssels für die 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: <ul style="list-style-type: none"> - 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.

Das Installationsprogramm legt verschiedene Berechtigungen für das Verzeichnis und die Dateien im Verzeichnis fest.

39. Drücken Sie die **Eingabetaste**.
Der Abschnitt **Domänen- und Knotenkonfiguration** wird angezeigt.
40. 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	Der Name der zu erstellenden Domäne. Der Standardname der Domäne 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: ` % * + ; " ? , < > \ /
Knoten-Hostname	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. Hinweis: Verwenden Sie nicht localhost. Der Hostname muss den Computer eindeutig kennzeichnen.
Knotenname	Name des auf diesem Computer zu erstellenden Knotens. Der Knotenname ist nicht mit dem Hostnamen des Computers identisch.
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: <ul style="list-style-type: none"> - Beim Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden und er darf nicht länger als 128 Zeichen sein. - 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.
Passwort bestätigen	Geben Sie das Passwort zur Bestätigung erneut ein.

41. 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“	<p>Legen Sie fest, ob die vom Installationsprogramm zugewiesenen Portnummern für die Domänen- und Knotenkomponenten angezeigt werden sollen:</p> <p>1 – Nein 2 – Ja</p> <p>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.</p>

42. 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.

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-Datendienstes. 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-HTTPS-Port	Kein Standardport. Geben Sie die erforderliche Portnummer beim Erstellen des Diensts ein. Durch Setzen dieses Ports auf 0 wird eine HTTPS-Verbindung zum Administrator Tool deaktiviert.
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.

43. Wählen Sie aus, ob Sie den Modellrepository-Dienst, den Datenintegrationsdienst und den Katalogdienst im Zuge der Installation erstellen möchten. Sie können diese Dienste nach der Installation in Informatica Administrator erstellen. Wählen Sie **1**, um die Dienste zu erstellen, oder **2**, um die Installation ohne Erstellung der Dienste abzuschließen.

Wenn Sie 1 gewählt haben, wird der Abschnitt **Datenbank des Modellrepository-Diensts** angezeigt.

44. Wenn Sie 1 gewählt haben, müssen Sie den Datenbanktyp auswählen und die Datenbankparameter für das Modellrepository eingeben.
45. Geben Sie an, ob Sie eine sichere Datenbank konfigurieren möchten. Wählen Sie **1**, um eine sichere Datenbank zu konfigurieren, oder **2**, um den Schritt zu überspringen.
46. Um JDBC-Verbindungsinformationen zu konfigurieren, wählen Sie **1** und geben Sie die JDBC-Parameter ein. Wählen Sie **2**, um die Konfiguration der JDBC-Verbindung zu überspringen.
47. Wählen Sie den Datenbanktyp für das Modellrepository aus, und geben Sie die Anmeldeinformationen einschließlich der Datenbankbenutzer-ID und des Benutzerpassworts ein.
48. Optional können Sie die JDBC-Verbindung und ihre Parameter konfigurieren.
49. Geben Sie die folgenden Informationen ein: Modellrepository-Dienstname, Name des Datenintegrationsdiensts und die Portnummer für den Datenintegrationsdienst, wenn Sie den Standardwert nicht verwenden möchten.

Option	Beschreibung
MRS-Name	Name des Modellrepository-Diensts.
DIS-Name	Name des Datenintegrationsdiensts.
HTTP-Protokolltyp	Sicherheitsprotokoll, das vom Datenintegrationsdienst verwendet wird.
Port	Portnummer.

Es werden Meldungen zum Erstellen des Modellrepository-Diensts und des Datenintegrationsdiensts angezeigt.

50. Geben Sie neben dem Modellrepository-Dienst und dem Datenintegrationsdienst die folgenden erforderlichen Informationen ein, um die Datenbanken für das Profiling-Warehouse und das Referenzdaten-Warehouse zu erstellen:

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, auf dem das Referenzdaten-Warehouse gehostet wird.

Profiling-Warehouse-Datenbanktyp

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, auf dem das Profiling-Warehouse gehostet wird.

In der Installationsübersicht wird nach der Installation angegeben, ob die Installation erfolgreich abgeschlossen wurde. In den Protokolldateien der Installation finden Sie weitere Informationen über die vom Installationsprogramm ausgeführten Aufgaben und die Konfigurationseigenschaften der installierten Komponenten.

Installieren durch Beitreten zu einer Domäne

Sie können einer Domäne beitreten, 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 den Befehl `./install.sh` aus, um das Installationsprogramm zu starten.
Im Installationsprogramm wird eine Meldung angezeigt, in der Sie dazu aufgefordert werden, die Informatica-Dokumentation zu lesen, bevor Sie mit der Installation fortfahren.
4. Wählen Sie **J**, um die Installation fortzusetzen.
5. Wählen Sie **1**, um Produkte der Informatica Big Data-Suite zu installieren.
6. Wählen Sie **1**, um das Tool zur Systemüberprüfung vor der Installation auszuführen. Das Tool überprüft, ob Ihr Computer die Mindest-Systemanforderungen für die Installation oder Aktualisierung von Informatica erfüllt.
Hinweis: Wenn Sie sicher sind, dass Ihr Computer die Mindest-Systemanforderungen für die Installation oder Aktualisierung von Informatica erfüllt, können Sie diesen Schritt überspringen.
7. Wählen Sie **3**, um Informatica zu installieren.
8. Wählen Sie **2**, um den Installations- bzw. Aktualisierungsbedingungen zuzustimmen.
9. Drücken Sie **2**, um zu bestätigen, dass Sie wissen, dass Version 10.2.2 für die Big Data-Produktsuite spezifisch ist, und mit der Installation fortzufahren.
10. Wählen Sie **2**, um Informatica-Dienste mit Enterprise Data Catalog zu installieren.
Das Installationsprogramm fordert Sie auf, zu bestätigen, dass die aktuelle Version der Informatica-Dienste nicht auf dem Knoten installiert ist.
11. Wählen Sie **1**, wenn Sie nicht die aktuelle Version der Informatica-Dienste installiert haben. Andernfalls drücken Sie **2**.
12. Wählen Sie den Hadoop-Clustertyp für Enterprise Data Catalog aus. Wählen Sie **2**, um Enterprise Data Catalog auf einer internen Hadoop-Verteilung auf Hortonworks mit dem Ambari-Tool bereitzustellen. Drücken Sie **1**, um den Enterprise Data Catalog auf einer vorhandenen Hadoop-Distribution auf Cloudera, HortonWorks oder Azure HDInsight bereitzustellen.
Je nach den von Ihnen festgelegten Einstellungen erstellt Enterprise Data Catalog einen Informatica-Cluster-Dienst für die interne Hadoop-Verteilung.
13. Wenn Sie die eingebettete Hadoop-Distribution ausgewählt haben, geben Sie nach der Konfiguration der Informatica-Domäne, des Modellrepository-Diensts und des Datenintegrationsdiensts folgende Informationen an:

-

Option	Beschreibung
SSH-Benutzername	Benutzername für die SSH-Verbindung (Secure Shell) ohne Passwortschutz.
Informatica-Cluster-Dienstname	Name des Informatica-Cluster-Diensts für den internen Cluster.
Informatica-Cluster-Dienstport	Portnummer für den Informatica-Cluster-Dienst.

Option	Beschreibung
Ambari-Serverhost.	Hostinformationen für den Ambari-Server. Ambari ist ein webbasiertes Tool für die Bereitstellung, Verwaltung und Überwachung von Apache Hadoop-Clustern, welches die Unterstützung für Hadoop HDFS, Hadoop MapReduce, Hive, HBase und ZooKeeper beinhaltet.
Durch Komma getrennte Ambari-Agent-Hosts	Gilt für die Hochverfügbarkeit. Wenn Sie mehrere Ambari-Agent-Hosts verwenden, geben Sie die kommagetrennten Werte der Namen der Ambari-Agent-Hosts an.
Ambari-Web-Port	Nummer des Ports, auf dem der Ambari-Server ausgeführt werden muss.
Katalogdienstname	Name des Katalogdiensts.
Katalogdienstport	Portnummer des Katalogdiensts.
Schlüsseltabellen-Speicherort	Gilt für einen Kerberos-aktivierten Cluster. Speicherort der zusammengeführten Benutzer- und Host-Keytab-Datei.
Kerberos-Konfigurationsdatei	Gilt für einen Kerberos-aktivierten Cluster. Speicherort der Kerberos-Konfigurationsdatei.

- Geben Sie die folgenden Details an, wenn Sie einen vorhandenen Cluster auswählen:

Eigenschaft	Beschreibung
Hadoop-Verteilung	Wählen Sie eine der folgenden Optionen aus: - ClouderaManager - HDInsight - Hortonworks
Cluster-URL	Vollqualifizierter Hostname für den Zugriff auf den Cluster.
Cluster-URL-Benutzername	Benutzername für den Zugriff auf den Cluster.
Cluster-URL-Passwort	Passwort für den Cluster-URL-Benutzernamen.

- Wenn Sie die vorhandene Hadoop-Distribution als `ClouderaManager` oder `Hortonworks` ausgewählt haben, geben Sie die folgenden Informationen an:

Option	Beschreibung
Katalogdienstname	Name des Katalogdiensts.
Katalogdienstport	Portnummer des Katalogdiensts.

Option	Beschreibung
URI des Yarn-Ressourcenmanagers	<p>Der Dienst innerhalb von Hadoop, der die MapReduce-Aufgaben an bestimmte Knoten im Cluster sendet.</p> <p>Verwenden Sie das folgende Format: <code><hostname>:<port></code></p> <p>Wobei</p> <ul style="list-style-type: none"> • <code>hostname</code> der Name bzw. die IP-Adresse des Yarn-Ressourcenmanagers ist. • <code>port</code> ist der Port, den der Yarn-Ressourcenmanager auf Remoteprozeduraufrufe (RPC) abhört.
Yarn-Ressourcenmanager-HTTP-URI	Der HTTP-URI-Wert für den Yarn-Ressourcenmanager.
URI des Yarn-Ressourcenmanager-Schedulers	Der Scheduler-URI-Wert für den Yarn-Ressourcenmanager.
Zookeeper-Cluster-URI	Der URI für die Zookeeper-Dienste, bei dem es sich um einen besonders leistungsfähigen Koordinationsdienst für verteilte Anwendungen handelt.
HDFS-NameNode-URI	<p>Der URI für den Zugriff auf HDFS.</p> <p>Verwenden Sie das folgende Format, um den NameNode-URI in der Cloudera-Verteilung anzugeben: <code>hdfs://<namenode>:<port></code></p> <p>Wobei</p> <ul style="list-style-type: none"> • <code><namenode></code> der Hostname oder die IP-Adresse von NameNode ist. • <code><Port></code> der Port ist, den der NameNode auf Remoteprozeduraufrufe (RPC) abhört.
Dienst-Clustername	<p>Name des Dienst-Clusters. Stellen Sie vor dem Abschluss der Installation sicher, dass ein Verzeichnis <code>/Informatica/LDM/<ServiceClusterName></code> in HDFS vorhanden ist.</p> <p>Hinweis: Wenn Sie keinen Dienst-Clusternamen angeben, betrachtet Enterprise Data Catalog <code>DomainName_CatalogServiceName</code> als Standardwert. Das Verzeichnis <code>/Informatica/LDM/<DomainName>_<CatalogServiceName></code> muss sich dann in HDFS befinden. Andernfalls kann der Katalogdienst fehlschlagen.</p>
HTTP-URI des Verlaufsservers	HTTP-URI für den Zugriff auf den Verlaufsserver.
Ist der Cluster sicher?	<p>Legen Sie diese Eigenschaft auf einen der folgenden Werte fest, wenn Sie einen vorhandenen Cluster verwenden, der sicher ist:</p> <ul style="list-style-type: none"> • 1: Gibt an, dass der vorhandene Cluster nicht sicher ist. • 2: Gibt an, dass der vorhandene Cluster sicher ist. <p>Der Standardwert ist 1.</p>

Option	Beschreibung
Ist der Cluster SSL-aktiviert?	Nur anwendbar, wenn Sie die Hadoop-Distribution als <code>Hortonworks</code> und <code>ClouderaManager</code> ausgewählt haben. Legen Sie diese Eigenschaft auf einen der folgenden Werte fest, wenn ein vorhandener Cluster für SSL aktiviert ist: <ul style="list-style-type: none"> • 1: Gibt an, dass der vorhandene Cluster nicht für SSL aktiviert ist. • 2: Gibt an, dass der vorhandene Cluster für SSL aktiviert ist. Der Standardwert ist 1.
Aktivieren der Kerberos-Authentifizierung	Legen Sie diese Eigenschaft auf einen der folgenden Werte fest, wenn ein vorhandener Cluster für Kerberos aktiviert ist: <ul style="list-style-type: none"> • 1: Gibt an, dass der vorhandene Cluster nicht für Kerberos aktiviert ist. • 2: Gibt an, dass der vorhandene Cluster für Kerberos aktiviert ist.

14. Drücken Sie die **Eingabetaste**, um fortzufahren.
Es wird eine Eingabeaufforderung in Bezug auf die Lizenzschlüsseldatei angezeigt.
15. Wählen Sie **2**, wenn das Installationsprogramm die Informatica-Anwendungsdienste basierend auf der Größe der bereitgestellten Daten optimieren soll.
Im Installationsprogramm werden die folgenden Optionen für verschiedene Datengrößen angezeigt:
 - Sandbox
 - Einfach
 - Standard
 - Hohe Parallelität und hohes Volumen
16. Geben Sie den Pfad und Dateinamen des Informatica-Lizenzschlüssels ein und drücken Sie die **Eingabetaste**.
17. 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.
18. Wählen Sie **2**, um das Dienstprogramm für die Vorabüberprüfung auszuführen. Das Dienstprogramm unterstützt Sie bei der Validierung der Voraussetzungen für die Installation von Enterprise Data Catalog in einem eingebetteten Cluster. Außerdem validiert das Dienstprogramm die Konfiguration der Informatica-Domäne, der Cluster-Hosts und der Hadoop-Clusterdienste.
Das Installationsprogramm fordert Sie auf, zu bestätigen, dass Sie die Kerberos-Authentifizierung für den Cluster aktivieren möchten.
19. Wählen Sie **2**, wenn Sie die Kerberos-Authentifizierung für den Cluster aktivieren möchten, und geben Sie die folgenden Details an:
 - a. **Keytab-Speicherort.** Speicherort der zusammengeführten Benutzer- und Host-Keytab-Datei.
 - b. **Kerberos-Konfigurationsdatei.** Speicherort der Kerberos-Konfigurationsdatei.
20. Geben Sie den Gateway-Benutzernamen an und drücken Sie die **Eingabetaste**. Der Standardwert ist **root**.
21. Geben Sie den Gateway-Hostnamen für den Informatica-Hadoop-Cluster in folgendem Format an: `<hostname>.<FQDN>` und drücken Sie die **Eingabetaste**.

22. Geben Sie die durch Kommas getrennte Liste von Informatica-Hadoop-Cluster-Knoten wie gezeigt im folgenden Format an: <hostname>.<FQDN>, <Hostname1>.<FQDN>, <Hostname2>.<FQDN> und drücken Sie die **Eingabetaste**.
23. Geben Sie den Gateway-Port des Informatica-Hadoop-Clusters an und drücken Sie die **Eingabetaste**. Der Standardwert ist **8080**.
Achten Sie darauf, dass Oracle nicht mit Port 8080 auf demselben Computer konfiguriert wird, auf dem der Informatica-Cluster-Dienst ausgeführt wird.
24. Geben Sie den Pfad zum Arbeitsverzeichnis an und drücken Sie die **Eingabetaste**. Der Pfad gibt den Speicherort an, in dem Sie den Informatica-Cluster-Dienst bereitstellen möchten.
Das Installationsprogramm startet das Vorabüberprüfungs-Dienstprogramm.
25. Drücken Sie die **Eingabetaste**, um nach der Ausführung des Dienstprogramms für die Vorabüberprüfung fortzufahren.
26. Überprüfen Sie die Installationsinformationen und drücken Sie die **Eingabetaste**, um fortzufahren.
Das Installationsprogramm kopiert die Enterprise Data Catalog-Dateien in das Installationsverzeichnis. Sie werden aufgefordert, eine Domäne zu erstellen oder einer Domäne beizutreten.
27. 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.
28. Geben Sie an, ob für die anzufügende Domäne die Option zur sicheren Kommunikation aktiviert wurde.
Wählen Sie 1, um einer ungesicherten Domäne beizutreten, oder 2, um einer sicheren Domäne beizutreten.
29. 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.

30. Geben Sie die Verbindungsdetails zu Informatica Administrator ein.
- a. Geben Sie an, ob eine sichere HTTPS-Verbindung zu 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
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.

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	<p>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.</p> <p>1 – Von Installationsprogramm generierten Schlüsselspeicher verwenden 2 – Schlüsselspeicherdatei und Passwort eingeben</p> <p>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/</p>

- c. Wenn Sie den Schlüsselspeicher festlegen, geben Sie das Passwort und den Speicherort der Schlüsselspeicherdatei ein.

31. Wählen Sie **2**, wenn Sie Single Sign-On mithilfe der SAML-Authentifizierung für Enterprise Data Catalog-Anwendungen aktivieren möchten.

32. Geben Sie die URL des SAML-Identitätsanbieters (IdP) an und drücken Sie die **Eingabetaste**.

Informationen zu den Konfigurationsschritten, die Sie nach der Installation von Enterprise Data Catalog ausführen müssen, finden Sie im Abschnitt *Konfigurieren von Single Sign-On mithilfe der SAML-Authentifizierung*.

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 **Domänenkonfigurations-Repository** angezeigt.

33. 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
1 – Standardmäßige SSL-Zertifikatsdateien 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.
2 – 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.

34. 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.

35. Geben Sie die Daten des Verschlüsselungsschlüssels für die Informatica-Domäne ein, der Sie beitreten möchten.

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.

In der folgenden Tabelle werden die Verschlüsselungsschlüsselparameter beschrieben, die beim Hinzufügen einer Domäne angegeben werden müssen:

Eigenschaft	Beschreibung
Auswählen des Verschlüsselungsschlüssels	<p>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.</p> <p>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.</p>
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.

36. 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	<p>Hostname für den Knoten. Der Hostname des Knotens darf keine Unterstriche (_) enthalten.</p> <p>Hinweis: Verwenden Sie nicht localhost. Der Hostname muss den Computer eindeutig kennzeichnen.</p>
Knotenname	<p>Der Name des auf diesem Computer zu erstellenden Informatica-Knotens. Der Knotenname ist nicht mit dem Hostnamen des Computers identisch.</p>
Knoten-Portnummer	<p>Die Portnummer für den Knoten.</p>
Datenbank-Truststore-Datei	<p>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.</p> <p>Sie ist verfügbar, wenn Sie einen Gateway-Knoten zu einer Domäne mit einer Domänenkonfigurations-Repository-Datenbank hinzufügen, die durch das SSL-Protokoll gesichert ist.</p>
Truststore-Passwort	<p>Passwort für die Datenbank-Truststore-Datei für die sichere Datenbank.</p> <p>Sie ist verfügbar, wenn Sie einen Gateway-Knoten zu einer Domäne mit einer Domänenkonfigurations-Repository-Datenbank hinzufügen, die durch das SSL-Protokoll gesichert ist.</p>

37. 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“	<p>Legen Sie fest, ob die vom Installationsprogramm zugewiesenen Portnummern für die Domänen- und Knotenkomponenten angezeigt werden sollen:</p> <p>1 – Nein 2 – Ja</p> <p>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.</p>

38. 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.

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-Datendienstes. 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-HTTPS-Port	Kein Standardport. Geben Sie die erforderliche Portnummer beim Erstellen des Diensts ein. Durch Setzen dieses Ports auf 0 wird eine HTTPS-Verbindung zum Administrator Tool deaktiviert.
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.

39. Geben Sie an, ob Sie eine sichere Datenbank konfigurieren möchten. Wählen Sie **1**, um eine sichere Datenbank zu konfigurieren, oder **2**, um den Schritt zu überspringen.
40. Um JDBC-Verbindungsinformationen zu konfigurieren, wählen Sie **1** und geben Sie die JDBC-Parameter ein. Wählen Sie **2**, um die Konfiguration der JDBC-Verbindung zu überspringen.
41. Wählen Sie den Datenbanktyp für das Modellrepository aus, und geben Sie die Anmeldeinformationen einschließlich der Datenbankbenutzer-ID und des Benutzerpassworts ein.
42. Optional können Sie die JDBC-Verbindung und ihre Parameter konfigurieren.
43. Geben Sie die folgenden Informationen ein: Modellrepository-Dienstname, Name des Datenintegrationsdiensts und die Portnummer für den Datenintegrationsdienst, wenn Sie den Standardwert nicht verwenden möchten.

Option	Beschreibung
MRS-Name	Name des Modellrepository-Diensts.
DIS-Name	Name des Datenintegrationsdiensts.
HTTP-Protokolltyp	Sicherheitsprotokoll, das vom Datenintegrationsdienst verwendet wird.

Option	Beschreibung
Port	Portnummer.

Es werden Meldungen zum Erstellen des Modellrepository-Diensts und des Datenintegrationsdiensts angezeigt.

In der Installationsübersicht wird nach der Installation angegeben, ob die Installation erfolgreich abgeschlossen wurde. In den Protokolldateien der Installation finden Sie weitere Informationen über die vom Installationsprogramm ausgeführten Aufgaben und die Konfigurationseigenschaften der installierten Komponenten.

Installieren von Enterprise Data Catalog auf einem Domänenknoten

Sie können das Informatica-Installationsprogramm verwenden, um Enterprise Data Catalog nach der Installation von Informatica zu installieren. So installieren Sie Enterprise Data Catalog nach der Installation von Informatica:

1. Melden Sie sich auf dem Computer mit einem System-Benutzerkonto an.
2. Schließen Sie die Informatica-Domäne.
3. Schließen Sie alle Anwendungen.
4. Führen Sie über eine Shell-Befehlszeile die Datei „install.sh“ im Stammverzeichnis aus.
Das Installationsprogramm zeigt die Nachricht an, um sicherzustellen, dass die Gebietsschema-Umgebungsvariablen gesetzt sind.
5. Wählen Sie 1, um die Option zum Installieren oder Aktualisieren von Informatica auszuwählen.
Das Installationsprogramm überprüft, ob die aktuelle Version von Informatica installiert ist.
6. Wählen Sie 2, um Informatica-Dienste mit Enterprise Data Catalog zu installieren.
Das Installationsprogramm fordert Sie auf, zu bestätigen, dass die aktuelle Version der Informatica-Dienste installiert ist.
7. Wählen Sie 2, um Enterprise Data Catalog zu installieren. Wenn Sie diese Option wählen, wird davon ausgegangen, dass die vorliegende Version von Informatica installiert ist.
8. Geben Sie den Speicherort von <INFA_HOME> an, wenn Sie vom Installationsprogramm aufgefordert werden, die Installation abzuschließen. INFA_HOME bezieht sich auf das Verzeichnis, in dem Enterprise Data Catalog installiert werden muss.

In der Installationsübersicht wird nach der Installation angegeben, ob die Installation erfolgreich abgeschlossen wurde. In den Protokolldateien der Installation finden Sie weitere Informationen über die vom Installationsprogramm ausgeführten Aufgaben und die Konfigurationseigenschaften der installierten Komponenten.

Hinweis: Die Anweisungen in diesem Abschnitt setzen voraus, dass Sie die Informatica-Anwendungsdienste bei der Installation von Informatica erstellt haben. Wenn Sie die Dienste nicht erstellt haben, finden Sie im Abschnitt *Installieren durch Beitreten zu einer Domäne* weitere Informationen zum Erstellen von Anwendungsdiensten.

Führen Sie nach Abschluss der Installation die folgenden Schritte aus:

1. Löschen Sie die folgenden Verzeichnisse:
 - INFA_HOME/service/work_dir

- INFA_HOME/tomcat/bin/workspace/.metadata
2. Starten Sie die Informatica-Domäne.
 3. Aktivieren Sie den Modellrepository-Dienst, und aktualisieren Sie den Inhalt des Modellrepository-Diensts mit einer der folgenden Methoden:
 - Informatica Administrator: Wählen Sie den Modellrepository-Dienst und klicken Sie auf **Aktionen > Repository-Inhalte > Upgrade**.
 - Informatica-Befehlszeilenschnittstelle: Führen Sie den Befehl `INFA_HOME/isp/bin/infacmd.sh mrs upgradeContents -dn DOMAINNAME -un domainUsername -pw domainPassword -sn MRSServiceName` aus.
 4. Erstellen und aktivieren Sie den Katalogdienst. Stellen Sie sicher, dass Sie den aktualisierten Modellrepository-Dienst verwenden.

Erstellen der Anwendungsdienste für Enterprise Data Catalog

Für den Enterprise Data Catalog müssen Anwendungsdienste erstellt und ausgeführt werden, bevor Sie sie verwenden können.

Sie können die Anwendungsdienste anhand einer der folgenden Methoden erstellen:

Mit dem Installationsprogramm, wenn Sie Enterprise Data Catalog installieren

Weitere Informationen zur Verwendung des Installationsprogramms zum Erstellen der Anwendungsdienste bei der Installation von Enterprise Data Catalog finden Sie unter https://network.informatica.com/onlinehelp/edc/Install_Help/index.htm

Mit dem Informatica Administrator nach der Installation von Enterprise Data Catalog

Weitere Informationen zur Verwendung des Informatica Administrator zum Erstellen der Anwendungsdienste finden Sie im Kapitel *Erstellen der Anwendungsdienste* in diesem Handbuch.

Mit dem Installationsprogramm nach der Installation von Enterprise Data Catalog

Weitere Informationen zur Verwendung des Installationsprogramms zum Erstellen der Anwendungsdienste nach der Installation von Enterprise Data Catalog finden Sie in den Schritten, die unter dem Thema *Erstellen der Anwendungsdienste für Enterprise Data Catalog mit dem Installationsprogramm* aufgeführt sind.

Wenn die Anwendungsdienste nicht erstellt werden oder der Vorgang fehlgeschlagen ist, können Sie den Vorgang mit dem Installationsprogramm nicht ab dem Fehler fortsetzen. Sie können den Vorgang mit dem Installationsprogramm erneut starten.

Erstellen der Anwendungsdienste für Enterprise Data Catalog unter Verwendung des Installationsprogramms

Führen Sie die folgenden Schritte aus, um die Anwendungsdienste nach der Installation von Enterprise Data Catalog mit dem Installationsprogramm zu erstellen:

1. Melden Sie sich auf dem Computer mit einem System-Benutzerkonto an.
2. Schließen Sie alle Anwendungen, die auf dem Computer ausgeführt werden.
3. Führen Sie über eine Shell-Befehlszeile den Befehl `./install.sh` aus, um das Installationsprogramm zu starten.
4. Drücken Sie **y**, um die Installation fortzusetzen.
5. Drücken Sie **3**, um die Option zum Installieren des Anwendungsdiensts für Enterprise Data Catalog oder Enterprise Data Preparation auszuwählen.

6. Drücken Sie **2**, um die allgemeinen Geschäftsbedingungen zu akzeptieren.
7. Drücken Sie **2**, um zu akzeptieren, dass Sie mit der Installation von Big Data-Produkten fortfahren möchten.
8. Drücken Sie **1**, um die Dienste für Enterprise Data Catalog zu konfigurieren.
9. Drücken Sie **1**, um zu bestätigen, dass die neueste Version von Enterprise Data Catalog-Diensten nicht installiert ist.
10. Geben Sie das Verzeichnis ein, in dem Sie Enterprise Data Catalog installiert haben, und drücken Sie die **Eingabetaste**.
11. Geben Sie die folgenden Domänendetails ein, die Sie bei der Installation des Enterprise Data Catalog konfiguriert hatten:
 - a. Domänenname. Geben Sie den Namen der Informatica-Domäne an, die Sie erstellt haben, und drücken Sie die **Eingabetaste**.
 - b. Knotenname. Geben Sie den Namen des Knotens an, den Sie auf dem Computer erstellt haben, auf dem Enterprise Data Catalog installiert worden ist, und drücken Sie die **Eingabetaste**.
 - c. Benutzerpasswort der Domäne. Geben Sie das Passwort ein, das Sie für den Informatica-Domänenadministrator konfiguriert haben, und drücken Sie die **Eingabetaste**.
12. Drücken Sie **1**, um zu bestätigen, dass Sie den Modellrepository-Dienst und den Datenintegrationsdienst erstellen möchten.
13. Drücken Sie **1**, wenn Sie den Überwachungsmodellrepository-Dienst zum Überwachen der Informatica-Domänenstatistiken erstellen möchten.
14. Drücken Sie **2**, wenn Sie keine Clusterkonfiguration erstellen möchten. Sie müssen eine Clusterkonfiguration in der Informatica-Domäne erstellen, wenn Sie Enterprise Data Preparation-Dienste konfigurieren möchten.
15. Drücken Sie **1**, wenn Sie die Profiling-Warehouse-Verbindung erstellen möchten.
16. Drücken Sie **1**, um den Content-Management-Dienst zu konfigurieren.
17. Sie müssen den Informatica-Clusterdienst erstellen, wenn Sie Enterprise Data Catalog auf einem eingebetteten Cluster bereitstellen. Drücken Sie **1**, wenn Sie den Informatica-Clusterdienst konfigurieren möchten.
Berücksichtigen Sie die folgenden Punkte, um zu entscheiden, wie Sie den Informatica-Clusterdienst erstellen möchten:
 - Informatica-Clusterdienst erstellen. Das Installationsprogramm erstellt den Informatica-Clusterdienst.
 - Wählen Sie die Option aus, dass Sie den Informatica-Clusterdienst nicht erstellen möchten. Das Installationsprogramm fordert Sie auf anzugeben, ob Sie dem Katalogdienst einen Informatica-Clusterdienst zuordnen möchten. Wenn Sie diese Option auswählen, erstellt das Installationsprogramm keinen neuen Informatica-Clusterdienst. Das Installationsprogramm fordert Sie auf, einen Informatica-Clusterdienst anzugeben, den Sie dem Katalogdienst zuordnen möchten.
 - Wählen Sie die Option aus, dass Sie keine Informatica-Clusterdienst erstellen möchten, und ordnen Sie dem Katalogdienst einen vorhandenen Informatica-Clusterdienst zu. Das Installationsprogramm erstellt den Informatica-Clusterdienst nicht und fährt mit der Erstellung des Katalogdienstes fort.
18. Drücken Sie **1**, wenn Sie den Katalogdienst konfigurieren möchten.
19. Führen Sie die Schritte in den folgenden Abschnitten aus, um die Anwendungsdienste zu erstellen.

Erstellen des Modellrepository-Dienstes

Geben Sie die folgenden Details für den Modellrepository-Dienst an:

1. Name des Modellrepository-Dienstes.

2. Name des Knotens, auf dem der Modellrepository-Dienst ausgeführt werden muss.
3. Die Lizenz, die mit dem Modellrepository-Dienst verbunden werden soll.
4. Wählen Sie aus den folgenden Optionen die Datenbank aus, die Sie für das Modellrepository konfigurieren möchten:
 - Oracle
 - SQL Server
 - DB2

Der Standardwert ist Oracle.

5. Geben Sie den Benutzernamen zum Zugriff auf die Datenbank in den Parameter **Datenbankbenutzer-ID** ein und drücken Sie die **Eingabetaste**. Der Standardwert ist **ADMIN**.
6. Geben Sie das Passwort für den Benutzernamen in den Parameter **Benutzerpasswort** ein und drücken Sie die Eingabetaste.
7. Drücken Sie **1**, wenn die Datenbank mit SSL gesichert ist.
Wenn Sie die Option ausgewählt haben, um anzugeben, dass die Datenbank SSL-fähig ist, geben Sie die folgenden Parameter an:

Parameter für die gesicherte Datenbank	Beschreibung
EncryptionMethod	Gibt an, ob Daten bei der Netzwerkübertragung verschlüsselt werden. Dieser Parameter muss auf SSL festgelegt werden.
ValidateServerCertificate	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	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	Gibt das Kryptografieprotokoll an, das für die Verbindung mit einer gesicherten Datenbank verwendet werden soll. Sie können den Parameter auf cryptoProtocolVersion=TLSv1.1 oder cryptoProtocolVersion=TLSv1.2 auf Basis des vom Datenbankserver verwendeten Kryptografieprotokolls.
TrustStore	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	Passwort der Truststore-Datei für die gesicherte Datenbank.

8. Drücken Sie **1**, um die JDBC-URL zum Verbinden mit der Datenbank anzugeben.
9. Geben Sie die Datenbankadresse für den Parameter **Datenbankadresse** im folgenden Format an:
<Vollqualifizierter Domänenname des Hosts>:<port>

10. Geben Sie den Datenbankdienstnamen für den Parameter **Datenbankdienstname** im folgenden Format an: <Vollqualifizierter Domänenname des Diensts>
11. Drücken Sie **1**, um anzugeben, dass Sie die JDBC-Parameter konfigurieren möchten.
12. Geben Sie die erforderlichen Werte für die Parameter an oder drücken Sie die **Eingabetaste**, um die Standardwerte anzuwenden. Drücken Sie die **Eingabetaste**, um die Standardwerte beizubehalten. Verwenden Sie die folgende Syntax für die Verbindungszeichenfolge für den ausgewählten Datenbanktyp:

Datenbanktyp	Syntax der Verbindungszeichenfolge
IBM DB2	<code>jdbc:informatica:db2:// <host_name>:<port_number>;DatabaseName=<database_name>;BatchPerformanceWorkaround=true;DynamicSections=3000</code>
Microsoft SQL Server	<ul style="list-style-type: none"> - Microsoft SQL Server, der die Standardinstanz verwendet <code>jdbc:informatica:sqlserver:// <host_name>:<port_number>;DatabaseName=<database_name>;SnapshotSerializable=true</code> - Microsoft SQL Server, der eine benannte Instanz verwendet <code>jdbc:informatica:sqlserver://<host_name> \<named_instance_name>;DatabaseName=<database_name>;SnapshotSerializable=true</code>
Oracle	<code>jdbc:informatica:oracle:// <Hostname>:<Portnummer>;SID=<Datenbankname>;MaxPooledStatements=20;CatalogOptions=0;BatchPerformanceWorkaround=true</code>

Das Installationsprogramm überprüft den Knotennamen und die Lizenz und erstellt dann den Modellrepository-Dienst. Das Installationsprogramm fährt mit dem Erstellen des Datenintegrationsdiensts fort.

Erstellen des Datenintegrationsdiensts

Geben Sie die folgenden Details für den Datenintegrationsdienst an:

1. Name des Data Integration Service
2. Name des Knotens, auf dem der Datenintegrationsdienst ausgeführt werden muss.
3. Die Lizenz, die mit dem Datenintegrationsdienst verbunden werden soll.
4. Der Name des Modellrepository-Diensts, der mit dem Datenintegrationsdienst verknüpft werden soll.
5. Geben Sie aus den folgenden Optionen das Protokoll an, das Sie für den Dienst verwenden möchten:
 - http
 - https
 - http&https

Wenn Sie **https** oder **http&https** als Protokoll für den Dienst auswählen, geben Sie die folgenden Details an:

 1. HTTPS-Port Der Standardwert ist 18095.

2. Geben Sie das SSL-Zertifikat an, das Sie zur Sicherung des Datenintegrationsdiensts verwenden möchten. Sie können die Standard-SSL-Zertifikate im Standardschlüsselspeicher und im Truststore oder die benutzerdefinierten SSL-Zertifikate verwenden. Wenn Sie benutzerdefinierte SSL-Zertifikate wählen, geben Sie den Pfad an, der den Dateinamen der Schlüsselspeicher- und der Truststore-Datei sowie die Passwörter zum Zugriff auf die Schlüsselspeicher- und die Truststore-Datei enthält.
6. Drücken Sie **1**, wenn der Datenintegrationsdienst die Spark-Engine zum Ausführen der Sqoop-Mappings oder zum Verarbeiten der Java-Umwandlungen verwenden soll.

Das Installationsprogramm validiert den Knotennamen und die Lizenz und erstellt und aktiviert den Datenintegrationsdienst. Das Installationsprogramm fährt mit dem Erstellen des Profiling-Warehouse fort.

Konfigurieren des Profiling-Warehouse

Geben Sie die folgenden Details an, um die Datenbank für das Profiling-Warehouse zu konfigurieren:

1. Name des Datenintegrationsdiensts, der mit dem Profiling-Warehouse verknüpft werden soll.
2. Wählen Sie aus den folgenden Optionen die Datenbank aus, die Sie für das Profiling-Warehouse konfigurieren möchten:
 - Oracle
 - SQL Server
 - DB2

Der Standardwert ist Oracle.

3. Geben Sie den Benutzernamen zum Zugriff auf die Datenbank in den Parameter **Datenbankbenutzer-ID** ein und drücken Sie die **Eingabetaste**. Der Standardwert ist **ADMIN**.
4. Geben Sie das Passwort für den Benutzernamen in den Parameter **Benutzerpasswort** ein und drücken Sie die Eingabetaste.
5. Drücken Sie **1**, wenn die Datenbank mit SSL gesichert ist. Wenn Sie die Option ausgewählt haben, um anzugeben, dass die Datenbank SSL-fähig ist, geben Sie die folgenden Parameter an:

Parameter für die gesicherte Datenbank	Beschreibung
EncryptionMethod	Gibt an, ob Daten bei der Netzwerkübertragung verschlüsselt werden. Dieser Parameter muss auf SSL festgelegt werden.
ValidateServerCertificate	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	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.

Parameter für die gesicherte Datenbank	Beschreibung
cryptoProtocolVersion	Gibt das Kryptografieprotokoll an, das für die Verbindung mit einer gesicherten Datenbank verwendet werden soll. Sie können den Parameter auf <code>cryptoProtocolVersion=TLSv1.1</code> oder <code>cryptoProtocolVersion=TLSv1.2</code> auf Basis des vom Datenbankserver verwendeten Kryptografieprotokolls.
TrustStore	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: <code><Informatica-Installationsverzeichnis>/tomcat/bin</code>
TrustStorePassword	Passwort der Truststore-Datei für die gesicherte Datenbank.

- Drücken Sie **1**, um die JDBC-URL zum Verbinden mit der Datenbank anzugeben.
- Geben Sie die Datenbankadresse für den Parameter **Datenbankadresse** im folgenden Format an:
`<Vollqualifizierter Domänenname des Hosts>:<port>`
- Geben Sie den Datenbankdienstnamen für den Parameter **Datenbankdienstname** im folgenden Format an:
`<Vollqualifizierter Domänenname des Diensts>`
- Drücken Sie **1**, um anzugeben, dass Sie die JDBC-Parameter konfigurieren möchten.
- Geben Sie die erforderlichen Werte für die Parameter an oder drücken Sie die **Eingabetaste**, um die Standardwerte anzuwenden. Drücken Sie die **Eingabetaste**, um die Standardwerte beizubehalten. Verwenden Sie die folgende Syntax für die Verbindungszeichenfolge für den ausgewählten Datenbanktyp:

Datenbanktyp	Syntax der Verbindungszeichenfolge
IBM DB2	<code>jdbc:informatica:db2:// <host_name>:<port_number>;DatabaseName=<database_name>;BatchPerformanceWorkaround=true;DynamicSections=3000</code>
Microsoft SQL Server	<ul style="list-style-type: none"> - Microsoft SQL Server, der die Standardinstanz verwendet <code>jdbc:informatica:sqlserver:// <host_name>:<port_number>;DatabaseName=<database_name>;SnapshotSerializable=true</code> - Microsoft SQL Server, der eine benannte Instanz verwendet <code>jdbc:informatica:sqlserver://<host_name> \<named_instance_name>;DatabaseName=<database_name>;SnapshotSerializable=true</code>
Oracle	<code>jdbc:informatica:oracle:// <Hostname>:<Portnummer>;SID=<Datenbankname>;MaxPooledStatements=20;CatalogOptions=0;BatchPerformanceWorkaround=true</code>

Das Installationsprogramm erstellt das Data Profiling-Warehouse und fährt mit dem Erstellen des Content-Management-Diensts fort.

Erstellen des Content-Management-Diensts

Geben Sie zum Erstellen des Content-Management-Diensts die folgenden Details an:

- Name des Modellrepository-Diensts, der mit dem Dienst verknüpft werden soll.

2. Name des Datenintegrationsdiensts, der mit dem Dienst verknüpft werden soll.
3. Name des Knotens, auf dem der Content-Managementdienst ausgeführt werden muss.
4. Die Lizenz, die mit dem Content-Managementdienst verbunden werden soll.
5. Name des Content Management Service
6. Geben Sie aus den folgenden Optionen das Protokoll an, das Sie für den Dienst verwenden möchten:
 - http
 - https

Wenn Sie **https** als Protokoll für den Service auswählen, geben Sie die folgenden Details an:

1. HTTPS-Port Der Standardwert ist 17466.
2. Geben Sie das SSL-Zertifikat an, das Sie zur Sicherung des Content-Management-Diensts verwenden möchten. Sie können die Standard-SSL-Zertifikate im Standardschlüsselspeicher oder die benutzerdefinierten SSL-Zertifikate verwenden. Wenn Sie benutzerdefinierte SSL-Zertifikate wählen, geben Sie den Pfad an, der den Dateinamen der Schlüsselspeicherdatei sowie das Passwort zum Zugriff auf die Schlüsselspeicherdatei enthält.
7. Führen Sie die folgenden Schritte aus, um die Datenbank für den Content-Management-Dienst zu konfigurieren:
8. Wählen Sie aus den folgenden Optionen die Datenbank aus, die Sie für den Content-Management-Dienst konfigurieren möchten:
 - Oracle
 - SQL Server
 - DB2

Der Standardwert ist Oracle.
9. Geben Sie den Benutzernamen zum Zugriff auf die Datenbank in den Parameter **Datenbankbenutzer-ID** ein und drücken Sie die **Eingabetaste**. Der Standardwert ist **ADMIN**.
10. Geben Sie das Passwort für den Benutzernamen in den Parameter **Benutzerpasswort** ein und drücken Sie die Eingabetaste.
11. Drücken Sie **1**, wenn die Datenbank mit SSL gesichert ist.
Wenn Sie die Option ausgewählt haben, um anzugeben, dass die Datenbank SSL-fähig ist, geben Sie die folgenden Parameter an:

Parameter für die gesicherte Datenbank	Beschreibung
EncryptionMethod	Gibt an, ob Daten bei der Netzwerkübertragung verschlüsselt werden. Dieser Parameter muss auf SSL festgelegt werden.
ValidateServerCertificate	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.

Parameter für die gesicherte Datenbank	Beschreibung
HostNameInCertificate	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	Gibt das Kryptografieprotokoll an, das für die Verbindung mit einer gesicherten Datenbank verwendet werden soll. Sie können den Parameter auf <code>cryptoProtocolVersion=TLSv1.1</code> oder <code>cryptoProtocolVersion=TLSv1.2</code> auf Basis des vom Datenbankserver verwendeten Kryptografieprotokolls.
TrustStore	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: <code><Informatica-Installationsverzeichnis>/tomcat/bin</code>
TrustStorePassword	Passwort der Truststore-Datei für die gesicherte Datenbank.

12. Drücken Sie **1**, um die JDBC-URL zum Verbinden mit der Datenbank anzugeben.
13. Geben Sie die Datenbankadresse für den Parameter **Datenbankadresse** im folgenden Format an:
`<Vollqualifizierter Domänenname des Hosts>:<port>`
14. Geben Sie den Datenbankdienstnamen für den Parameter **Datenbankdienstname** im folgenden Format an:
`<Vollqualifizierter Domänenname des Diensts>`
15. Drücken Sie **1**, um anzugeben, dass Sie die JDBC-Parameter konfigurieren möchten.
16. Geben Sie die erforderlichen Werte für die Parameter an oder drücken Sie die **Eingabetaste**, um die Standardwerte anzuwenden. Drücken Sie die **Eingabetaste**, um die Standardwerte beizubehalten. Verwenden Sie die folgende Syntax für die Verbindungszeichenfolge für den ausgewählten Datenbanktyp:

Datenbanktyp	Syntax der Verbindungszeichenfolge
IBM DB2	<code>jdbc:informatica:db2:// <host_name>:<port_number>;DatabaseName=<database_name>;BatchPerformanceWorkaround=true;DynamicSections=3000</code>
Microsoft SQL Server	<ul style="list-style-type: none"> - Microsoft SQL Server, der die Standardinstanz verwendet <code>jdbc:informatica:sqlserver:// <host_name>:<port_number>;DatabaseName=<database_name>;SnapshotSerializable=true</code> - Microsoft SQL Server, der eine benannte Instanz verwendet <code>jdbc:informatica:sqlserver://<host_name> \<named_instance_name>;DatabaseName=<database_name>;SnapshotSerializable=true</code>
Oracle	<code>jdbc:informatica:oracle:// <Hostname>:<Portnummer>;SID=<Datenbankname>;MaxPooledStatements=20;CatalogOptions=0;BatchPerformanceWorkaround=true</code>

Das Installationsprogramm erstellt und aktiviert den Content-Management-Dienst und fährt mit dem Konfigurieren der Cluster- und Anwendungsdienstoptionen fort.

Konfigurieren der Cluster- und Anwendungsdienstoptionen

Führen Sie die folgenden Schritte aus, um die Cluster- und Anwendungsdienstoptionen zu konfigurieren:

1. Drücken Sie **1**, wenn Sie möchten, dass das Installationsprogramm Apache ZooKeeper, YARN und HDFS anhand der von Ihnen angegebenen Eigenschaften konfiguriert.
2. Wählen Sie aus den folgenden Optionen den Clustertyp aus:
 - Hortonworks
 - Cloudera
 - Azure HDInsight
3. Geben Sie an, ob der Cluster die Kerberos-Authentifizierung verwendet.
4. Geben Sie an, ob der Cluster für SSL aktiviert ist.

Konfigurieren des Informatica-Clusterdiensts

Wenn Sie Enterprise Data Catalog auf einem eingebetteten Cluster installieren, geben Sie die folgenden Details zur Konfiguration des Informatica-Clusterdiensts an:

1. Name des Knotens, auf dem der Informatica-Clusterdienst ausgeführt werden muss.
2. Die Lizenz, die mit dem Informatica-Clusterdienst verbunden werden soll.
3. Benutzername für den Apache Ambari-Server. Der Standardwert ist root.
4. Name des Informatica-Clusterdiensts.
5. Hostname für das Informatica-Hadoop-Cluster-Gateway.
6. Durch Kommas getrennte Liste der Hadoop-Knoten, auf denen die Apache Ambari-Agents ausgeführt werden.
7. Portnummer des Apache Ambari-Servers. Der Standardwert ist 9075.
8. Portnummer des Informatica-Hadoop-Cluster-Gateways. Der Standardwert ist 8080.
9. Geben Sie an, ob Sie das Standardkennwort für Ambari ändern möchten.
10. Geben Sie die folgenden Eigenschaften an, wenn Sie SSL für den Cluster aktivieren möchten:
 - a. Der HTTPS-Port für den Informatica-Clusterdienst. Der Standardwert ist 7500.
 - b. Drücken Sie **1**, wenn Sie den vom Installationsprogramm generierten Standardschlüsselspeicher verwenden möchten.
 - c. 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/ Alternativ können Sie eine Schlüsselspeicherdatei mit einem selbstsignierten Zertifikat oder einem von einer Zertifizierungsbehörde signierten Zertifikat verwenden. Wenn Sie nicht beabsichtigen, die vom Installationsprogramm generierte Schlüsselspeicherdatei zu verwenden, stellen Sie sicher, dass Sie 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.
 - d. Geben Sie den Speicherort der Truststore-Datei an, der für alle Knoten in der Domäne zugänglich ist, und drücken Sie die **Eingabetaste**. Der Standardwert ist `/opt/ssl`.
11. Drücken Sie **2**, wenn Sie ein Verzeichnis zum Speichern der Protokolldateien und Datenverzeichnisse für HDFS, YARN und ZooKeeper angeben möchten.

12. Wenn Sie im vorherigen Schritt **2** ausgewählt haben, geben Sie den Pfad zu dem Verzeichnis an, in dem Sie die Protokolldateien speichern möchten, und drücken Sie die **Eingabetaste**.
13. Das Installationsprogramm erstellt den Informatica-Clusterdienst und fährt mit der Erstellung des Katalogdiensts fort.

Konfigurieren des Katalogdiensts

Geben Sie die folgenden Details an, um den Katalogdienst zu konfigurieren:

1. Name des Katalogdiensts.
2. Name des Modellrepository-Diensts, der mit dem Katalogdienst verknüpft werden soll.
3. Name des Knotens, auf dem der Katalogdienst ausgeführt werden muss.
4. Geben Sie für den Enterprise Data Catalog, der auf einem eingebetteten Cluster bereitgestellt wird, und für den Sie die Option ausgewählt hatten, einen Informatica-Clusterdienst mit dem Katalogdienst zu verbinden, den Namen des Informatica-Clusterdiensts an.
5. Die Lizenz, die mit dem Katalogdienst verknüpft werden soll.
6. Die Cluster-Hadoop-Distributions-URL.
7. Benutzername für den Zugriff auf die Cluster-Hadoop-Distributions-URL. Der Standardwert ist ADMIN.
8. Passwort für den Zugriff auf die Cluster-Hadoop-Distributions-URL.
9. Geben Sie die folgenden Eigenschaften an, falls Sie Enterprise Data Catalog auf einem vorhandenen Cluster bereitgestellt haben:

Eigenschaft	Beschreibung
Name des Clusters.	Wenn Sie Cloudera als Clustertyp ausgewählt haben, können Sie einen Namen für den Cluster angeben.
Name des HDFS-Diensts für hohe Verfügbarkeit	Gilt für vorhandenen hochverfügbaren Cluster. Geben Sie den HDFS-Dienstnamen an.
URI des Yarn-Ressourcenmanager-Schedulers	Der Scheduler-URI-Wert für den Yarn-Ressourcenmanager.

Hinweis: Wenn Sie ClouderaManager oder Hortonworks als Hadoop-Distribution für einen vorhandenen Cluster auswählen, erkennt Enterprise Data Catalog automatisch die folgenden Eigenschaften für den Hadoop-Distributionstyp:

- ZooKeeper-Cluster-URI
- HDFS-NameNode-URI
- URI des Yarn-Ressourcenmanagers
- HTTPS- oder HTTP-URI des Yarn-Ressourcenmanagers
- HTTP-URI des Verlaufsservers
- Name des HDFS-Diensts für hohe Verfügbarkeit
- URI des Yarn-Ressourcenmanager-Schedulers

10. Wenn Sie den Enterprise Data Catalog auf einem Azure HDInsight-Cluster bereitgestellt haben, geben Sie die folgenden Eigenschaften für den Katalogdienst an:

Eigenschaft	Beschreibung
Clustertyp	Externer Cluster
Hadoop-Distribution	HDInsight
Cluster-URL	Vollqualifizierter Hostname für den Zugriff auf den Cluster.
Cluster-URL-Benutzername	Benutzername für den Zugriff auf den Cluster.
Cluster-URL-Passwort	Passwort für den Cluster-URL-Benutzernamen.

Nachdem Sie den Katalogdienst erstellt haben, können Sie die folgenden benutzerdefinierten Eigenschaften in Informatica Administrator für den Katalogdienst konfigurieren:

Benutzerdefinierte Eigenschaft	Beschreibung
LdmCustomOptions.deployment.azure.account.key	Der Schlüssel zum Authentifizieren des Katalogdiensts für die Verbindung mit dem Azure-Speicherkonto. Der Wert des Azure-Speicherkontoschlüssels kann verschlüsselt oder unverschlüsselt sein. Sie können den Wert aus der Eigenschaft <code>fs.azure.account.key.<Name des Speicherkontos></code> in der Datei <code>core-site.xml</code> abrufen, die sich im Azure HDInsight-Cluster befindet.
LdmCustomOptions.deployment.azure.key.decryption.script.path	Wenn der Schlüssel in der Eigenschaft <code>LdmCustomOptions.deployment.azure.account.key</code> im verschlüsselten Format vorliegt, können Sie das Entschlüsselungs-Shell-Skript verwenden, um den Schlüssel mit dem Schlüsselzertifikat zu entschlüsseln. Sie müssen das Entschlüsselungs-Shell-Skript und die Schlüsselzertifikatdatei auf den Domänencomputer (unter demselben Pfad wie der Clustercomputer) kopieren, bevor Sie den Katalogdienst aktivieren. Den Pfad im Azure HDInsight-Clustercomputer müssen Sie für die kopierten Dateien im Domänencomputer beibehalten. Der Wert für die Eigenschaft ist der Speicherort des Entschlüsselungs-Shell-Skripts. Beispiel: <code>/usr/lib/python2.7/dist-packages/hdinsight_common/decrypt.sh</code> . Die Schlüsselzertifikatdatei „ <code>key_decryption_cert.prv</code> “ befindet sich im Verzeichnis <code>/usr/lib/hdinsight-common/certs/key_decryption_cert.prv</code> des Azure HDInsight-Clusters.
LdmCustomOptions.deployment.hdfs.default.fs	Adresse des WASB-Speicherkontos, mit dem der Katalogdienst eine Verbindung herstellen muss. Die Adresse enthält den Namen des WASB-Speichercontainers mit dem Namen des Speicherkontos. Der Wert für die Eigenschaft ist die vollständige WASB-Adresse mit den Namen des Containers und des Speicherkontos. Sie können den Wert für die Eigenschaft aus der Eigenschaft <code>fs.defaultFS</code> in der Datei <code>core-site.xml</code> abrufen, die sich im Azure HDInsight-Cluster befindet.

11. Der Name des Dienstclusters.

12. Geben Sie die folgenden Eigenschaften an, wenn Sie einen sicheren Zugriff auf den Katalogdienst ermöglichen möchten:
- Geben Sie den HTTPS-Port an, den Sie für den Katalogdienst konfigurieren möchten. Der Standardwert ist 9124.
 - Drücken Sie **1**, wenn Sie den vom Installationsprogramm generierten Standardschlüsselspeicher verwenden möchten. Drücken Sie anderenfalls **2**, um eine benutzerdefinierte Schlüsselspeicherdatei zu verwenden.
Wenn Sie nicht beabsichtigen, die vom Installationsprogramm generierte Schlüsselspeicherdatei zu verwenden, stellen Sie sicher, dass Sie 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.
Wenn Sie die Option zum Verwenden einer benutzerdefinierten Schlüsselspeicherdatei ausgewählt haben, geben Sie die folgenden Details an:
 - Pfad zur Schlüsselspeicherdatei.
 - Der Schlüsselspeicher-Alias.
 - Passwort für die Schlüsselspeicherdatei.
 - Passwort für den Solr-Schlüsselspeicher.
13. Wählen Sie aus den folgenden Optionen die Ladegröße der Metadaten aus, die Sie in den Katalog aufnehmen möchten:
- Demo
 - Niedrig
 - Mittel
 - Hoch

Installieren von Enterprise Data Catalog im automatischen Modus

Wenn Sie Enterprise Data Catalog ohne Benutzereingriffe installieren möchten, wählen Sie die Installation im automatischen Modus. Geben Sie die Installationsoptionen mithilfe einer Eigenschaftendatei an. Das Installationsprogramm liest die Datei, um die Installationsoptionen in Erfahrung zu bringen. 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 Installationsdateien von Enterprise Data Catalog auf die Festplatte auf dem Computer, auf dem Sie Enterprise Data Catalog installieren möchten. Stellen Sie bei Installation auf einem Remote-Computer sicher, dass Sie darauf zugreifen und Dateien erstellen können.

Gehen Sie zum automatischen Installieren folgendermaßen vor:

- Konfigurieren Sie die Installationseigenschaftendatei und geben Sie darin die Installationsoptionen an.
- Führen Sie das Installationsprogramm mit der Installationseigenschaftendatei aus.
- Sichern Sie die Passwörter in der Installationseigenschaftendatei.

Konfigurieren der Eigenschaftendatei

Informatica enthält eine Beispiel-Eigenschaftendatei mit Parametern, die vom Installationsprogramm für Enterprise Data Catalog benötigt werden. Sie können die Beispiel-Eigenschaftendatei mit den gewünschten Optionen für Ihre Installation anpassen. Führen Sie anschließend die automatische Installation aus.

Die Beispieldatei `SilentInput.properties` wird im Root-Verzeichnis der DVD oder am Speicherort, an den das Installationsprogramm heruntergeladen wurde, gespeichert. Nachdem Sie die Datei angepasst haben, speichern Sie sie erneut mit dem Dateinamen `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
RESUME_INSTALLATION	Legen Sie die Eigenschaft auf „true“ fest, wenn Sie die Installation ab dem Fehlerpunkt bzw. Beendigungspunkt fortsetzen möchten. Der Standardwert ist FALSE.
LICENSE_KEY_LOC	Der absolute Pfad und Dateiname der Lizenzschlüsseldatei.
USER_INSTALL_DIR	Verzeichnis, in dem Enterprise Data Catalog installiert ist.
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 <code>DEFAULT_HTTPS_ENABLED=1</code> müssen Sie diesen Parameter auf 0 setzen. Falls <code>DEFAULT_HTTPS_ENABLED=0</code> 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. Standardwert ist 8443.

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: <ul style="list-style-type: none"> - 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. Die Eigenschaft stellt den LDAP-Namen für eine Kerberos-aktivierte Domäne dar.
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.
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“.

Eigenschaftsname	Beschreibung
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: <ul style="list-style-type: none"> - 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 Datenbank.
TRUSTSTORE_DB_PASSWD	Passwort für die Truststore-Datei.
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. Setzen Sie diesen Parameter für die Linux-Installation auf 0.
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.

Eigenschaftsname	Beschreibung
DB_CUSTOM_STRING_SELECTION	<p>Legt fest, ob eine JDBC-URL oder eine benutzerdefinierter Verbindungszeichenfolge für die Verbindung zur Domänenkonfigurationsdatenbank verwendet werden soll.</p> <p>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.</p>
DB_SERVICENAME	<p>Erforderlich, wenn DB_CUSTOM_STRING_SELECTION=0.</p> <p>Dienstname für Oracle- und IBM DB2-Datenbanken.</p> <p>Der Datenbankname für Microsoft SQL Server und Sybase ASE.</p>
DB_ADDRESS	<p>Erforderlich, wenn DB_CUSTOM_STRING_SELECTION=0.</p> <p>Hostname und Portnummer für die Datenbankinstanz im Format <i>HostName:Port</i>.</p>
ADVANCE_JDBC_PARAM	<p>Sie können diesen Parameter einstellen, wenn DB_CUSTOM_STRING_SELECTION=0 ist.</p> <p>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.</p>
DB_CUSTOM_STRING	<p>Erforderlich, wenn DB_CUSTOM_STRING_SELECTION=1.</p> <p>Der gültige benutzerdefinierte JDBC-Verbindungs-String.</p>
DOMAIN_NAME	<p>Wenn Sie eine Domäne erstellen, der Name der zu erstellenden Domäne.</p> <p>Wenn Sie einer Domäne beitreten, Name der anzufügenden Domäne, die in einer früheren Installation erstellt wurde.</p> <p>Der Standard-Domänenname lautet <i>Domain_<MachineName></i>. Der Name darf maximal 128 Zeichen umfassen und muss im 7-Bit-ASCII-Format vorliegen. Er darf weder Leerzeichen noch die folgenden Zeichen enthalten: ` % * + ; " ? , < > \ /</p>
DOMAIN_HOST_NAME	<p>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.</p> <p>Bei Anfügen einer Domäne ist dies der Hostname des Rechners, auf dem sich der Gateway-Knoten der anzufügenden Domäne befindet.</p> <p>Hinweis: Verwenden Sie nicht localhost. Der Hostname muss den Computer eindeutig kennzeichnen.</p>
NODE_NAME	<p>Bei CREATE_DOMAIN=1 erforderlich.</p> <p>Name des auf diesem Computer zu erstellenden Knotens. Der Knotenname ist nicht mit dem Hostnamen des Computers identisch.</p>

Eigenschaftsname	Beschreibung
DOMAIN_PORT	<p>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.</p> <p>Bei Anfügen einer Domäne ist dies die Portnummer des Gateway-Knotens der anzufügenden Domäne.</p>
DOMAIN_USER	<p>Benutzername für den Domänenadministrator.</p> <p>Bei Erstellung einer Domäne können Sie diesen Benutzernamen für Ihre Erstanmeldung bei Informatica Administrator verwenden. Beachten Sie folgende Richtlinien:</p> <ul style="list-style-type: none"> - 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. <p>Bei Anfügen einer Domäne ist dies der Benutzername, mit dem Sie sich bei der anzufügenden Domäne anmelden.</p>
DOMAIN_PSSWD	<p>Das Passwort für den Domänenadministrator. Das Passwort muss mehr als zwei Zeichen und darf bis zu 16 Zeichen enthalten.</p>
DOMAIN_CNFRM_PSSWD	<p>Geben Sie das Passwort zur Bestätigung erneut ein.</p>
JOIN_NODE_NAME	<p>Bei JOIN_DOMAIN=1 erforderlich.</p> <p>Name des Knotens, den Sie der Domäne anfügen. Der Knotenname ist nicht mit dem Hostnamen des Computers identisch.</p>
JOIN_HOST_NAME	<p>Bei JOIN_DOMAIN=1 erforderlich.</p> <p>Hostname des Computers, auf dem der Knoten erstellt wird, den Sie der Domäne anfügen. Der Hostname des Knotens darf keine Unterstriche (_) enthalten.</p> <p>Hinweis: Verwenden Sie nicht localhost. Der Hostname muss den Computer eindeutig kennzeichnen.</p>
JOIN_DOMAIN_PORT	<p>Bei JOIN_DOMAIN=1 erforderlich.</p> <p>Die Portnummer des Gateway-Knotens der anzufügenden Domäne.</p>
ADVANCE_PORT_CONFIG	<p>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.</p>
MIN_PORT	<p>Sie können diesen Parameter einrichten, wenn ADVANCE_PORT_CONFIG=1 ist.</p> <p>Niedrigste Portnummer des dynamischen Portnummernbereichs, die den Anwendungsdienstprozessen, die auf diesem Knoten laufen, zugewiesen werden kann.</p>

Eigenschaftsname	Beschreibung
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-Datendienstes. 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.
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.

- 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.
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: <code>EncryptionMethod=SSL;HostNameInCertificate=;ValidateServerCertificate=</code>
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.

Eigenschaft	Beschreibung
MRS_DB2_TABLESPACE	<p>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.</p> <p>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.</p>
MRS_DB_CUSTOM_STRING_SELECTION	<p>Legt fest, ob eine JDBC-URL oder eine benutzerdefinierte Verbindungszeichenfolge für die Verbindung mit der Modellrepository-Datenbank verwendet werden soll.</p> <p>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.</p>
MRS_DB_SERVICENAME	<p>Dienst oder Datenbankname für die Modellrepository-Datenbank. Bei MRS_DB_CUSTOM_STRING_SELECTION=0 erforderlich.</p> <p>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.</p>
MRS_DB_ADDRESS	<p>Bei MRS_DB_CUSTOM_STRING_SELECTION=0 erforderlich. Hostname und Portnummer für die Datenbankinstanz im Format <i>HostName:Port</i>.</p>
MRS_ADVANCE_JDBC_PARAM	<p>Sie können diesen Parameter einrichten, wenn MRS_DB_CUSTOM_STRING_SELECTION=0 ist.</p> <p>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.</p>
MRS_DB_CUSTOM_STRING	<p>Bei MRS_DB_CUSTOM_STRING_SELECTION=1 erforderlich. Der gültige benutzerdefinierte JDBC-Verbindungs-String.</p>
MRS_SERVICE_NAME	<p>Name des Modellrepository-Diensts.</p>

Eigenschaft	Beschreibung
MRS_KEYTAB_FILELOC	<p>Erforderlich, wenn ENABLE_KERBEROS=1 und SPN_SHARE_LEVEL=PROCESS</p> <p>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.</p>
DIS_SERVICE_NAME	Name des Datenintegrationsdiensts.
DIS_KEYTAB_FILELOC	<p>Erforderlich, wenn ENABLE_KERBEROS=1 und SPN_SHARE_LEVEL=PROCESS</p> <p>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.</p>
DIS_PROTOCOL_TYPE	<p>HTTP-Protokolltyp des Datenintegrationsdiensts.</p> <p>Verwenden Sie einen der folgenden Werte:</p> <ul style="list-style-type: none"> - http - https - Beide
DIS_HTTP_PORT	Erforderlich, wenn DIS_PROTOCOL_TYPE http oder beides ist. HTTP-Port des Datenintegrationsdiensts.
DIS_HTTPS_PORT	<p>Erforderlich, wenn DIS_PROTOCOL_TYPE https oder beides ist.</p> <p>HTTP-Port des Datenintegrationsdiensts.</p>
DIS_CUSTOM_SELECTION	<p>Optionaler Parameter, wenn Sie den Wert von DIS_PROTOCOL_TYPE mit https oder beiden festlegen.</p> <p>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.</p>
DIS_KEYSTORE_DIR	<p>Erforderlich, wenn DIS_CUSTOM_SELECTION auf TRUE gesetzt ist.</p> <p>Der Speicherort der KeyStore-Datei für den Datenintegrationsdienst.</p>
DIS_KEYSTORE_PASSWD	<p>Erforderlich, wenn DIS_CUSTOM_SELECTION auf TRUE gesetzt ist.</p> <p>Das Passwort der KeyStore-Datei für den Datenintegrationsdienst.</p>

Eigenschaft	Beschreibung
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. In der folgenden Tabelle sind die Parameter aufgeführt, die Sie für Enterprise Data Catalog konfigurieren können:

Eigenschaft	Beschreibung
INSTALL_TYPE	Geben Sie an, ob Informatica installiert oder aktualisiert werden soll: <ul style="list-style-type: none"> - Wählen Sie die Einstellung INSTALL_TYPE=0, um Informatica zu installieren. - Wählen Sie die Einstellung INSTALL_TYPE=1, um Informatica zu aktualisieren. Hinweis: <ul style="list-style-type: none"> - Verwenden Sie zum Aktualisieren von Informatica die Datei <code>SilentInput_upgrade.properties</code>. - Verwenden Sie die Datei <code>SilentInput_upgrade_NewConfig.properties</code>, um Informatica auf eine andere Knotenkonfiguration zu aktualisieren.
INSTALL_LDM	Geben Sie an, ob Sie Informatica-Dienste mit oder ohne Enterprise Data Catalog installieren möchten: <ul style="list-style-type: none"> - Mit der Einstellung INSTALL_LDM=0 wird Informatica ohne Enterprise Data Catalog-Dienste installiert. - Mit der Einstellung INSTALL_LDM=1 wird Informatica mit Enterprise Data Catalog-Diensten installiert.
CLUSTER_HADOOP_DISTRIBUTION_TYPE	Legen Sie dieses Feld auf einen der folgenden Werte fest, wenn Sie CLUSTER_TYPE=2 angegeben haben: <ul style="list-style-type: none"> - Legen Sie dieses Feld auf <code>HortonWorks</code>, <code>ClouderaManager</code> oder <code>HDInsight</code> fest, wenn Sie die Cluster-URL, den Benutzernamen und das Passwort kennen. - Legen Sie diesen Feldwert auf <code>Andere</code> fest, wenn Sie die Cluster-URL, den Benutzernamen und das Passwort nicht kennen.

Eigenschaft	Beschreibung
KDC_TYPE	<p>Gilt für Kerberos-aktivierten eingebetteten Hadoop-Cluster, der von Informatica verwaltet wird. Diese Eigenschaft verweist auf den Typ des Schlüsselverteilungszentrums (KDC, Key Distribution Center) für den Hadoop-Cluster. Sie können entweder ein MIT KDC oder ein Microsoft Active Directory auswählen. Legen Sie diese Eigenschaft fest, wenn CLUSTER_TYPE=1 und IS_CLUSTER_SECURE=true ist.</p> <p>Hinweis: Verwenden Sie diese Eigenschaft nicht, wenn der Cluster nicht für Kerberos aktiviert ist.</p>
LDAP_URL	<p>Gilt für Kerberos-aktivierten eingebetteten Hadoop-Cluster, der von Informatica verwaltet wird. Diese Eigenschaft gibt an, dass Microsoft Active Directory KDC für die Authentifizierung verwendet wird, und stellt die URL zum LDAP-Serververzeichnis dar.</p>
CONTAINER_DN	<p>Gilt für Kerberos-aktivierten eingebetteten Hadoop-Cluster, der von Informatica verwaltet wird. Diese Eigenschaft gibt an, dass Microsoft Active Directory KDC für die Authentifizierung verwendet wird, und stellt den Distinguished Name des Containers dar, zu dem der Benutzer gehört.</p>
KDC_HOST	<p>Name des KDC-Hostcomputers. Legen Sie diese Eigenschaft fest, wenn Sie CLUSTER_TYPE=1 und IS_CLUSTER_SECURE=true konfiguriert haben. Wenn Sie CLUSTER_TYPE=2 konfiguriert haben, verwenden Sie die Eigenschaft nicht.</p>
IHS_REALM	<p>Name des Kerberos-Bereichs auf dem Computer, auf dem der KDC-Server gehostet wird. Legen Sie diese Eigenschaft fest, wenn Sie CLUSTER_TYPE=1 und IS_CLUSTER_SECURE=true konfiguriert haben. Wenn Sie CLUSTER_TYPE=2 konfiguriert haben, verwenden Sie die Eigenschaft nicht.</p>
IHS_ADMINISTRATOR_SERVER_HOST	<p>Der Name des Administratorservers, auf dem der KDC-Server gehostet wird. Legen Sie diese Eigenschaft fest, wenn Sie CLUSTER_TYPE=1 und IS_CLUSTER_SECURE=true konfiguriert haben. Wenn Sie CLUSTER_TYPE=2 konfiguriert haben, verwenden Sie die Eigenschaft nicht.</p>
IHS_ADMINISTRATOR_PRINCIPAL	<p>Der Kerberos-Administratorprinzipal. Legen Sie diese Eigenschaft fest, wenn Sie CLUSTER_TYPE=1 und IS_CLUSTER_SECURE=true konfiguriert haben. Wenn Sie CLUSTER_TYPE=2 konfiguriert haben, verwenden Sie die Eigenschaft nicht.</p>
IHS_ADMINISTRATOR_PASSWORD	<p>Das Kerberos-Administratorpasswort. Legen Sie diese Eigenschaft fest, wenn Sie CLUSTER_TYPE=1 und IS_CLUSTER_SECURE=true konfiguriert haben. Wenn Sie CLUSTER_TYPE=2 konfiguriert haben, verwenden Sie die Eigenschaft nicht.</p>

Eigenschaft	Beschreibung
KERBEROS_CONF_FILE_LOC	Speicherort der Datei <code>krb5.conf</code> . Sie müssen die Eigenschaft für den Kerberos-aktivierten eingebetteten Hadoop-Cluster oder den Kerberos-aktivierten vorhandenen Hadoop-Cluster im Unternehmen angeben.
CATALOGE_SERVICE_KEYTAB_LOCATION	Speicherort der Keytab-Datei, die Sie für den Katalogdienst angegeben haben. Legen Sie diese Eigenschaft fest, wenn Sie die folgenden Eigenschaften konfiguriert haben: <ul style="list-style-type: none"> - CLUSTER_TYPE=1 - IS_CLUSTER_SECURE=true - Wenn der Katalogdienst auf einem eingebetteten Hadoop-Cluster konfiguriert ist Wenn Sie CLUSTER_TYPE=2 konfiguriert haben, verwenden Sie die Eigenschaft nicht.
CLUSTER_HADOOP_DISTRIBUTION_URL_USER	Der Benutzername für den Zugriff auf die Hadoop-Verteilungs-URL. Geben Sie die Eigenschaft an, wenn Sie Cloudera Manager, HortonWorks oder HDInsight für CLUSTER_HADOOP_DISTRIBUTION_TYPE konfiguriert haben.
CLUSTER_HADOOP_DISTRIBUTION_URL_PASSWD	Das Passwort für den Benutzernamen, der für den Zugriff auf die Hadoop-Verteilungs-URL verwendet wird. Geben Sie die Eigenschaft an, wenn Sie Cloudera Manager, HortonWorks oder HDInsight für CLUSTER_HADOOP_DISTRIBUTION_TYPE konfiguriert haben.
INFA_SERVICES_INSTALLED	Legt fest, ob Enterprise Data Catalog mit oder ohne Informatica installiert werden soll. Legen Sie <code>INFA_SERVICES_INSTALLED=true</code> fest, wenn die aktuelle Version von Informatica bereits installiert ist und Sie nur Enterprise Data Catalog installieren möchten. Legen Sie <code>INFA_SERVICES_INSTALLED=false</code> fest, wenn die aktuelle Version von Informatica nicht installiert ist und Sie Enterprise Data Catalog einschließlich Informatica installieren möchten.
CLUSTER_TYPE	Geben Sie 1 für einen eingebetteten Hadoop-Cluster an. Das Installationsprogramm erstellt einen Informatica-Cluster-Dienst für die Konfiguration von Ambari-Serverhost und -Agent und erstellt dann einen Katalogdienst. Geben Sie 2 für einen vorhandenen Hadoop-Cluster an. Das Installationsprogramm erstellt den Katalogdienst.
ASSOCIATE_PROFILE_CONNECTION	Legen Sie den Wert auf 1 fest, um dem Datenintegrationsdienst eine Profiling-Warehouse-Verbindung und eine Datenbank zuzuordnen. Legen Sie den Wert auf 0 fest, wenn Sie die Profiling-Warehouse-Verbindung und die Datenbank nicht dem Datenintegrationsdienst zuordnen möchten.
PWH_DB_TYPE	Stellt den Datenbanktyp für die Profiling-Warehouse-Verbindung dar. Legen Sie die Eigenschaft auf einen der folgenden Datenbanktypen fest: Oracle oder DB2. Bei den aufgelisteten Datenbanktypoptionen wird die Groß-/Kleinschreibung beachtet.

Eigenschaft	Beschreibung
PWH_DB_UNAME	Stellt den Namen des Datenbank-Benutzerkontos für das Domänenkonfigurations-Repository dar.
PWH_DB_PASSWD	Stellt das Datenbankpasswort für das Datenbankbenutzerkonto dar.
PWH_SQLSERVER_SCHEMA_NAME	Stellt den Namen des Schemas dar, das Domänenkonfigurationstabellen enthält. Legen Sie diese Eigenschaft fest, wenn DB_TYPE=MSSQLServer ist. Wenn PWH_SQLSERVER_SCHEMA_NAME leer ist, erstellt das Installationsprogramm die Tabellen im Standardschema.
PWH_DB2_TABLESPACE	Stellt den Namen des Tablespace dar, in dem die Tabellen erstellt werden müssen. Legen Sie die Eigenschaft fest, wenn DB_TYPE=DB2 ist. Geben Sie einen Tablespace an, der die Anforderungen an die Seitengröße (pageSize) von 32768 Byte erfüllt. Wenn PWH_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.
PWH_DB_CUSTOM_STRING_SELECTION	Legt fest, ob eine JDBC-URL oder eine benutzerdefinierte Verbindungszeichenfolge für die Verbindung zur Domänenkonfigurationsdatenbank verwendet werden soll. Legen Sie PWH_DB_CUSTOM_STRING_SELECTION=1 fest, wenn PWH_TRUSTED_CONNECTION=1 ist. Geben Sie die gültige Standardverbindungszeichenfolge in PWH_DB_CUSTOM_STRING an. Wenn Sie 0 angeben, erstellt das Installationsprogramm eine JDBC-URL aus den von Ihnen angegebenen Datenbankeigenschaften. Wenn Sie 1 angeben, verwendet das Installationsprogramm die benutzerdefinierte Verbindungszeichenfolge, die Sie angeben.
PWH_DB_SERVICENAME	Stellt den Dienstnamen oder den Datenbanknamen der Datenbank dar. Legen Sie die Eigenschaft fest, wenn PWH_DB_CUSTOM_STRING_SELECTION=0 ist. Legen Sie die Eigenschaft auf den Dienstnamen für Oracle- und IBM DB2-Datenbanken fest. Legen Sie die Eigenschaft auf den Datenbanknamen für Microsoft SQL Server- und Sybase ASE-Datenbanken fest. Lassen Sie die Eigenschaft leer, wenn PWH_DB_CUSTOM_STRING_SELECTION=1 ist.
PWH_DB_ADDRESS	Stellt den Hostnamen und die Portnummer für die Datenbankinstanz dar. Legen Sie die Eigenschaft fest, wenn PWH_DB_CUSTOM_STRING_SELECTION=0 ist. Legen Sie die Eigenschaft im folgenden Format fest: Hostname:Portnummer. Lassen Sie die Eigenschaft leer, wenn PWH_DB_CUSTOM_STRING_SELECTION=1 ist.

Eigenschaft	Beschreibung
PWH_ADVANCE_JDBC_PARAM	Stellt zusätzliche Parameter in der JDBC-URL-Verbindungszeichenfolge dar. Wenn PWH_DB_CUSTOM_STRING_SELECTION=0 ist, können Sie die Eigenschaft so festlegen, dass optionale Parameter in der JDBC-URL-Verbindungszeichenfolge enthalten sind. Die Parameterzeichenfolge muss gültig sein. Ist dieser Parameter leer, wird die JDBC-URL vom Installationsprogramm ohne zusätzliche Parameter erstellt.
PWH_DB_CUSTOM_STRING	Stellt eine gültige benutzerdefinierte JDBC-Verbindungszeichenfolge dar. Legen Sie die Eigenschaft fest, wenn PWH_DB_CUSTOM_STRING_SELECTION=1 ist.
PWH_DATA_ACCESS_CONNECT_STRING	Geben Sie diese Eigenschaftszeichenfolge an, wenn ASSOCIATE_PROFILE_CONNECTION=1 ist.
LOAD_DATA_DOMAIN	Legen Sie den Wert dieser Eigenschaft auf 1 fest, um den Content-Management-Dienst mit Staging-Datenbankverbindung zu erstellen und dann die erweiterten Datendomänen zu laden.
CMS_SERVICE_NAME	Name des Content-Management-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: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () []
CMS_PROTOCOL_TYPE	Geben Sie als Protokolltyp <code>http</code> oder <code>https</code> an. Bei den Optionen wird die Groß-/Kleinschreibung beachtet.
CMS_HTTP_PORT	HTTP-Portnummer für den Dienst.
CMS_HTTPS_PORT	HTTPS-Portnummer für den Dienst.
CMS_KEYSTORE_FILE	Pfad und Dateiname der Schlüsselspeicherdatei.
CMS_KEYSTORE_PASSWD	Passwort für die Schlüsselspeicherdatei.
CMS_DB_TYPE	Der Datenbanktyp für die Staging-Datenbankverbindung des Content-Management-Diensts. Als Datenbanktyp können Sie <code>Oracle</code> oder <code>DB2</code> auswählen. Bei den Optionen des Datenbanktyps wird die Groß-/Kleinschreibung beachtet.
CMS_DB_UNAME	Name des Datenbankbenutzerkontos für das Domänenkonfigurations-Repository.
CMS_DB_PASSWD	Datenbankpasswort für das Datenbankbenutzerkonto.
CMS_SQLSERVER_SCHEMA_NAME	Der Name des Schemas, das die Domänenkonfigurationstabellen enthält. Wenn CMS_SQLSERVER_SCHEMA_NAME leer ist, erstellt das Installationsprogramm die Tabellen im Standardschema. Legen Sie die Eigenschaft fest, wenn DB_TYPE=MSSQLServer ist.

Eigenschaft	Beschreibung
CMS_DB2_TABLESPACE	Der Name des Tablespace, in dem Tabellen erstellt werden müssen. Legen Sie die Eigenschaft fest, wenn DB_TYPE=DB2 ist. Geben Sie einen Tablespace an, der die Anforderungen an die Seitengröße (pageSize) von 32768 Byte erfüllt. Wenn CMS_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.
CMS_DB_CUSTOM_STRING_SELECTION	Legt fest, ob eine JDBC-URL oder eine benutzerdefinierte Verbindungszeichenfolge für die Verbindung zur Domänenkonfigurationsdatenbank verwendet werden soll. Legen Sie CMS_DB_CUSTOM_STRING_SELECTION=1 fest, wenn CMS_TRUSTED_CONNECTION=1 ist. Geben Sie die gültige Standardverbindungszeichenfolge in CMS_DB_CUSTOM_STRING an. Wenn Sie 0 angeben, erstellt das Installationsprogramm eine JDBC-URL aus den von Ihnen angegebenen Datenbankeigenschaften. Wenn Sie 1 angeben, verwendet das Installationsprogramm die von Ihnen angegebene benutzerdefinierte Verbindungszeichenfolge.
CMS_DB_SERVICENAME	Stellt den Dienstnamen oder den Datenbanknamen der Datenbank dar. Legen Sie die Eigenschaft fest, wenn CMS_DB_CUSTOM_STRING_SELECTION=0 ist. Legen Sie die Eigenschaft auf den Dienstnamen für Oracle- und IBM DB2-Datenbanken fest. Legen Sie die Eigenschaft auf den Datenbanknamen für Microsoft SQL Server- und Sybase ASE-Datenbanken fest. Lassen Sie die Eigenschaft leer, wenn CMS_DB_CUSTOM_STRING_SELECTION=1 ist.
CMS_DB_ADDRESS	Stellt den Hostnamen und die Portnummer für die Datenbankinstanz dar. Legen Sie die Eigenschaft fest, wenn CMS_DB_CUSTOM_STRING_SELECTION=0 ist. Legen Sie die Eigenschaft im Format Hostname:Portnummer fest. Lassen Sie die Eigenschaft leer, wenn CMS_DB_CUSTOM_STRING_SELECTION=1 ist.
CMS_ADVANCE_JDBC_PARAM	Stellt zusätzliche Parameter in der JDBC-URL-Verbindungszeichenfolge dar. Wenn CMS_DB_CUSTOM_STRING_SELECTION=0 ist, können Sie die Eigenschaft so festlegen, dass optionale Parameter in der JDBC-URL-Verbindungszeichenfolge enthalten sind. Stellen Sie sicher, dass die Parameterzeichenfolge gültig ist. Ist diese Eigenschaft leer, wird die JDBC-URL vom Installationsprogramm ohne zusätzliche Parameter erstellt.
CMS_DB_CUSTOM_STRING	Stellt eine gültige benutzerdefinierte JDBC-Verbindungszeichenfolge dar. Legen Sie die Eigenschaft fest, wenn CMS_DB_CUSTOM_STRING_SELECTION=1 ist.
CMS_DATA_ACCESS_CONNECT_STRING	Sie müssen diese Eigenschaft angeben, wenn LOAD_DATA_DOMAIN=1 ist.

Eigenschaft	Beschreibung
SERVICE_ENABLE_TLS	Legen Sie diese Eigenschaft auf <code>true</code> fest, wenn der Dienst für TLS (Transport Layer Security) aktiviert werden muss. Sie können diese Eigenschaft leer lassen, wenn Sie TLS für den Dienst nicht aktivieren möchten. Wenn <code>CLUSTER_TYPE=1</code> und <code>SERVICE_ENABLE_TLS=true</code> ist, aktiviert das Installationsprogramm sowohl den Informatica-Cluster-Dienst als auch den Katalogdienst für SSL (Secure Sockets Layer). Wenn <code>CLUSTER_TYPE=2</code> und <code>SERVICE_ENABLE_TLS=true</code> ist, aktiviert das Installationsprogramm den Katalogdienst für SSL.
IS_CLUSTER_SSL_ENABLE	Legen Sie diese Eigenschaft auf <code>true</code> fest, wenn Sie über einen vorhandenen Cluster verfügen, der für SSL aktiviert ist. Wenn Sie SSL nicht auf dem Cluster aktivieren möchten, lassen Sie diese Eigenschaft leer.
IS_CLUSTER_HA_ENABLE	Legen Sie diese Eigenschaft auf <code>true</code> fest, wenn Sie über einen vorhandenen Cluster verfügen, der für hohe Verfügbarkeit aktiviert ist. Wenn Sie die hohe Verfügbarkeit des Clusters nicht aktivieren möchten, lassen Sie diese Eigenschaft leer.
IS_CLUSTER_SECURE	Legen Sie diese Eigenschaft auf <code>true</code> fest, wenn der Cluster für Kerberos aktiviert werden muss. Sie können diese Eigenschaft leer lassen, wenn Sie Kerberos für den Cluster nicht aktivieren möchten.
GATEWAY_USERNAME	Geben Sie den Benutzernamen für einen eingebetteten Cluster an, in dem Sie ohne ein SSH-Passwort eine Verbindung mit anderen Hosts vom Enterprise Data Catalog-Domänenhost herstellen. Der Standardbenutzername ist <code>root</code> . Bei <code>CLUSTER_TYPE=2</code> lassen Sie diese Eigenschaft leer.
HADOOP_SERVICE_NAME	Geben Sie den Namen des Informatica-Cluster-Diensts an, wenn <code>CLUSTER_TYPE=1</code> ist. Lassen Sie diese Eigenschaft für <code>CLUSTER_TYPE=2</code> leer.
HADOOP_SERVICE_PORT	Geben Sie den Port für den Informatica-Cluster-Dienst an, wenn <code>CLUSTER_TYPE=1</code> ist. Lassen Sie diese Eigenschaft für <code>CLUSTER_TYPE=2</code> leer. Lassen Sie diese Eigenschaft leer, wenn <code>SERVICE_ENABLE_TLS=true</code> ist.
HADOOP_TLS_HTTPS_PORT	Geben Sie den HTTPS-Port für den Informatica-Cluster-Dienst an, wenn <code>SERVICE_ENABLE_TLS=true</code> ist. Lassen Sie diese Eigenschaft für <code>CLUSTER_TYPE=2</code> leer.
HADOOP_KEYSTORE_FILE	Pfad und Dateiname der Schlüsselspeicherdatei. Sie müssen diesen Parameter angeben, wenn <code>SERVICE_ENABLE_TLS=true</code> ist. Lassen Sie diese Eigenschaft für <code>CLUSTER_TYPE=2</code> leer.
HADOOP_KEYSTORE_ALIAS	Geben Sie den Schlüsselspeicher-Alias an, wenn <code>SERVICE_ENABLE_TLS=true</code> und <code>SSL_ENABLED=true</code> ist. Lassen Sie diese Eigenschaft für <code>CLUSTER_TYPE=2</code> leer.

Eigenschaft	Beschreibung
HADOOP_KEYSTORE_PASSWD	Geben Sie das Schlüsselspeicherpasswort an, wenn SERVICE_ENABLE_TLS=true ist. Lassen Sie diese Eigenschaft für CLUSTER_TYPE=2 leer.
HADOOP_TRUSTSTORE_FILE	Geben Sie den Speicherort der Truststore-Datei an, wenn SSL_ENABLED=true ist. Lassen Sie diese Eigenschaft für CLUSTER_TYPE=2 leer. Der Speicherort muss ein allgemeiner Speicherort auf allen Hadoop-Knoten sein, an den Sie die Truststore-Datei nach dem Export und Import von HADOOP_KEYSTORE_FILE kopieren können. Legen Sie diese Eigenschaft fest, wenn die Domäne für SSL aktiviert ist.
HADOOP_GATEWAY_HOST	Geben Sie den Gateway-Host-Parameter an, bei dem der Ambari-Server installiert ist, wenn CLUSTER_TYPE=1 ist. Lassen Sie diese Eigenschaft für CLUSTER_TYPE=2 leer.
HADOOP_NODES	Geben Sie den durch Komma getrennten Ambari-Agent-Hostnamen an, auf dem der Ambari-Agent installiert ist. Sie müssen diese Eigenschaft angeben, wenn CLUSTER_TYPE=1 ist. Lassen Sie diese Eigenschaft für CLUSTER_TYPE=2 leer.
HADOOP_GATEWAY_PORT	Geben Sie den Port für die Verbindung mit dem Ambari-Server an, wenn CLUSTER_TYPE=1 ist. Lassen Sie diese Eigenschaft für CLUSTER_TYPE=2 leer.
CATALOGUE_SERVICE_NAME	Name des Katalogdiensts. Sie müssen diesen Parameter sowohl für eingebettete als auch für vorhandene Cluster angeben.
CATALOGUE_SERVICE_PORT	Der Port für den Katalogdienst. Geben Sie die Eigenschaft sowohl für eingebettete als auch für vorhandene Cluster an. Lassen Sie diese Eigenschaft für SERVICE_ENABLE_TLS=true leer.
CATALOGUE_SERVICE_TLS_HTTPS_PORT	Der HTTPS-Port für den Informatica-Cluster-Dienst. Geben Sie die Eigenschaft an, wenn für den vorhandenen Cluster SERVICE_ENABLE_TLS=true ist.
CATALOGUE_SERVICE_KEYSTORE_FILE	Dateiname und Pfad der Katalogdienst-Schlüsselspeicherdatei. Sie müssen diesen Parameter angeben, wenn SERVICE_ENABLE_TLS=true ist.
CATALOGUE_SERVICE_KEYSTORE_ALIAS	Geben Sie die Schlüsselspeicher-Alias-Eigenschaft an, wenn SERVICE_ENABLE_TLS=true und SSL_ENABLED=true ist.
CATALOGUE_SERVICE_KEYSTORE_PASSWD	Geben Sie das Passwort für die Schlüsselspeicherdatei an, wenn SERVICE_ENABLE_TLS=true ist.
DOMAIN_KEYSTORE_ALIAS	Geben Sie den Domänenschlüsselspeicher-Alias an, wenn SERVICE_ENABLE_TLS=true und SSL_ENABLED=true ist. Sie müssen diese Eigenschaft angeben, wenn die Domäne im SSL-Modus erstellt wird und wenn TLS_CUSTOM_SELECTION=true ist.

Eigenschaft	Beschreibung
CATALOGUE_SERVICE_SOLR_KEYSTORE_FILE	Dateiname und Pfad der Solr-Schlüsselspeicherdatei für den Katalogdienst. Sie müssen diese Eigenschaft angeben, wenn IS_CLUSTER_SSL_ENABLE=true ist. Stellen Sie sicher, dass der Pfad zu der Datei auf den Cluster und nicht auf die Domäne verweist. Legen Sie diese Eigenschaft fest, wenn der Cluster für SSL oder Kerberos oder sowohl für SSL als auch für Kerberos aktiviert ist.
CATALOGUE_SERVICE_SOLR_KEYSTORE_PASSWD	Passwort für die Solr-Schlüsselspeicherdatei. Sie müssen diese Eigenschaft angeben, wenn IS_CLUSTER_SSL_ENABLE=true ist.
YARN_RESOURCE_MANAGER_URI	Der URI für den YARN-Ressourcenmanager. Sie müssen diese Eigenschaft angeben, wenn CLUSTER_TYPE=2 ist. Sie müssen die Eigenschaft im folgenden Format angeben: Hostname:Port. Lassen Sie diese Eigenschaft für CLUSTER_TYPE=1 leer.
YARN_RESOURCE_MANAGER_HTTP_URI	Der HTTP-URI zum YARN-Ressourcenmanager. Sie müssen diese Eigenschaft angeben, wenn CLUSTER_TYPE=2 ist. Sie müssen die Eigenschaft im folgenden Format angeben: Hostname:Port. Lassen Sie diese Eigenschaft für CLUSTER_TYPE=1 leer.
YARN_RESOURCE_MANAGER_SCHEDULER_URI	Der Scheduler-URI zum YARN-Ressourcenmanager. Sie müssen diesen Parameter angeben, wenn CLUSTER_TYPE=2 ist. Sie müssen die Eigenschaft im folgenden Format angeben: Hostname:Port. Lassen Sie diese Eigenschaft für CLUSTER_TYPE=1 leer.
ZOOKEEPER_URI	Der ZooKeeper-URI. Geben Sie diese Eigenschaft an, wenn CLUSTER_TYPE=2 ist. Sie müssen diese Eigenschaft im folgenden Format angeben: Zookeeper-Host:Client-Port. Lassen Sie diese Eigenschaft für CLUSTER_TYPE=1 leer.
HDFS_HOST_NAME	Der HDFS-NameNode-URI. Geben Sie diesen Parameter an, wenn CLUSTER_TYPE=2 ist. Sie müssen diese Eigenschaft im folgenden Format angeben: Hostname:Port. Lassen Sie diese Eigenschaft für CLUSTER_TYPE=1 leer.
SERVICE_CLUSTER_NAME	Der Name des HDFS-Dienst-Clusters. Sie müssen diese Eigenschaft angeben, wenn CLUSTER_TYPE=2 ist. Der Standardwert ist der DOMAIN_NAME_CATALOGUE_SERVICE_NAME. Lassen Sie diese Eigenschaft für CLUSTER_TYPE=1 leer.
HDFS_SERVICE_NAME_HA	Der HDFS-Dienstname, wenn der Cluster für hohe Verfügbarkeit aktiviert ist. Sie müssen diese Eigenschaft angeben, wenn CLUSTER_TYPE=2 ist und wenn IS_CLUSTER_HA_ENABLE=true ist. Lassen Sie diese Eigenschaft für CLUSTER_TYPE=1 leer.

Eigenschaft	Beschreibung
IS_CLUSTER_SECURE	Geben Sie an, ob der Cluster sicher ist oder nicht. Sie müssen diese Eigenschaft konfigurieren, wenn für einen Kerberos-aktivierten Cluster CLUSTER_TYPE=2 und IS_CLUSTER_SECURE=true ist. Lassen Sie diese Eigenschaft für CLUSTER_TYPE=1 leer.
HDFS_SERVICE_PRINCIPAL	Der Dienstprinzipal für HDFS. Sie müssen diese Eigenschaft angeben, wenn für einen Kerberos-aktivierten Cluster CLUSTER_TYPE=2 und IS_CLUSTER_SECURE=true ist. Lassen Sie diese Eigenschaft für CLUSTER_TYPE=1 leer.
YARN_SERVICE_PRINCIPAL	Der Dienstprinzipal für YARN. Sie müssen diese Eigenschaft angeben, wenn für einen Kerberos-aktivierten Cluster CLUSTER_TYPE=2 und IS_CLUSTER_SECURE=true ist. Lassen Sie diese Eigenschaft für CLUSTER_TYPE=1 leer.
KDC_DOMAIN_NAME	Der Domänenname des Kerberos-Schlüsselverteilungszentrums (KDC). Sie müssen diese Eigenschaft angeben, wenn für einen Kerberos-aktivierten Cluster CLUSTER_TYPE=2 und IS_CLUSTER_SECURE=true ist. Lassen Sie diese Eigenschaft für CLUSTER_TYPE=1 leer.
KDC_KEYTAB_LOCATION	Der Speicherort des Kerberos-Schlüsselverteilungszentrums (KDC). Sie müssen diesen Parameter angeben, wenn für einen Kerberos-aktivierten Cluster CLUSTER_TYPE=2 und IS_CLUSTER_SECURE=true ist. Lassen Sie diese Eigenschaft für CLUSTER_TYPE=1 leer.
HISTORY_SERVER_HTTP_URI	Der HTTP-URI zum Verlaufsserver. Sie müssen diesen Parameter angeben, wenn CLUSTER_TYPE=2 ist. Lassen Sie diese Eigenschaft für CLUSTER_TYPE=1 leer.

- 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.

- Öffnen Sie eine Linux-Shell.
- Gehen Sie zum Root-Verzeichnis für das Verzeichnis, das die Installationsdateien enthält.
- Stellen Sie sicher, dass das Verzeichnis die Datei `SilentInput.properties` enthält, die Sie bearbeitet und erneut gespeichert haben.
- Führen Sie `silentInstall.sh` aus, um die unbeaufsichtigte Installation zu starten.

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.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.

Installieren der Anwendungsdienste für Enterprise Data Catalog im automatischen Modus

Wenn Sie bei der Installation von Enterprise Data Catalog die Anwendungsdienste für Enterprise Data Catalog nicht installiert haben, können Sie diese mit dem Installationsprogramm installieren. Wenn Sie die Anwendungsdienste für Enterprise Data Catalog ohne Benutzereingriffe installieren möchten, installieren Sie die Anwendungsdienste im automatischen Modus. Geben Sie die Installationsoptionen mithilfe einer Eigenschaftendatei an. Das Installationsprogramm liest die Datei, um die Installationsoptionen in Erfahrung zu bringen. Mit der automatischen Installation können Sie die Informatica-Dienste auf mehreren Computern im Netzwerk installieren oder die Installation auf den verschiedenen Computern standardisieren.

Gehen Sie zum Installieren der Anwendungsdienste im automatischen Modus folgendermaßen vor:

1. Konfigurieren Sie die Installationseigenschaftendatei und geben Sie darin die Installationsoptionen für den Anwendungsdienst an.
2. Führen Sie das Installationsprogramm mit der Installationseigenschaftendatei aus.
3. Sichern Sie die Passwörter in der Installationseigenschaftendatei.

Konfigurieren der Eigenschaftendatei

Führen Sie die folgenden Schritte aus, um die Datei `SilentInput_configure.properties` zu konfigurieren:

1. Wechseln Sie zum Root-Verzeichnis, das die Installationsdateien enthält.
2. Suchen Sie die Datei `SilentInput_configure.properties`.
3. Erstellen Sie eine Sicherungskopie der Datei „`SilentInput_configure.properties`“
4. Öffnen Sie die Datei in einem Texteditor und geben Sie die Werte der Anwendungsdienstparameter an.
Weitere Informationen zu den Anwendungsdienstparametern finden Sie unter dem Thema [“Erstellen der Anwendungsdienste für Enterprise Data Catalog unter Verwendung des Installationsprogramms” auf Seite 97](#).
5. Speichern Sie die Datei.

Ausführen des automatischen Installationsprogramms zum Installieren der Dienste

Öffnen Sie nach dem Konfigurieren der Eigenschaftendatei eine Eingabeaufforderung, um die automatische Installation zu starten.

1. Öffnen Sie eine Linux-Shell.
2. Wechseln Sie zum Root-Verzeichnis, das die Installationsdateien enthält.
3. Vergewissern Sie sich, dass das Verzeichnis die Datei `SilentInput_configure.properties` enthält, die Sie bearbeitet und gespeichert haben.
4. Führen Sie `silentinstallConfig.sh` aus, um die automatische Installation zu starten.

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.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.

Teil IV: Nach der Installation von Enterprise Data Catalog

Dieser Teil enthält die folgenden Kapitel:

- [Durchführen der Domänenkonfiguration, 131](#)
- [Vorbereiten zum Erstellen der Anwendungsdienste, 137](#)
- [Erstellen der Anwendungsdienste, 143](#)
- [Konfigurieren von Single Sign-On mithilfe der SAML-Authentifizierung, 162](#)

KAPITEL 6

Durchführen der Domänenkonfiguration

Dieses Kapitel umfasst die folgenden Themen:

- [Durchführen der Domänenkonfiguration - Übersicht, 131](#)
- [Überprüfen der Kompatibilität der Codepage, 131](#)
- [Konfigurieren der Umgebungsvariablen, 132](#)
- [Berechtigungen des Katalogdiensts, 134](#)

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 Kompatibilität der Codepage

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 Domänenkonfigurationsdatenbank mit den Codepages 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 Repositories in der Domäne kompatibel sind.

Ist die Gebietsschemaeinstellung nicht mit der Codepage für das Repository kompatibel, kann kein Anwendungsdienst erstellt werden.

Konfigurieren von Gebietsschema-Umgebungsvariablen unter Linux

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 zum Einrichten der Linux-Codepage LANG, LC_CTYPE oder LC_ALL.

Überprüfen Sie mithilfe des folgenden Befehls, ob der Wert der Gebietsschema-Umgebungsvariablen mit den Spracheinstellungen des Computers und des Codepage-Typs kompatibel ist, den Sie für das Repository verwenden möchten:

```
locale -a
```

Der Befehl gibt die auf Linux-Betriebssystemen installierten Sprachen und die vorhandenen Gebietsschemaeinstellungen zurück.

Richten Sie die folgenden lokalen Umgebungsvariablen ein:

Gebietsschema unter Linux

Unter Linux können unterschiedliche Gebietsschemawerte dasselbe Gebietsschema darstellen. So stellen beispielsweise „utf8“, „UTF-8“, „UTF8“ und „utf-8“ auf einem Linux-Computer ein und dasselbe Gebietsschema dar. Für Informatica müssen Sie auf einem Linux-Computer einen speziellen Wert für jedes Gebietsschema verwenden. Achten Sie darauf, die Umgebungsvariable LANG entsprechend auf allen Linux-Computern einzustellen.

Gebietsschema für Oracle-Datenbank-Clients

Stellen für NLS_LANG bei Oracle-Datenbank-Clients das Gebietsschema ein, das der Datenbank-Client und -Server bei der Anmeldung verwenden sollen. 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
```

Konfigurieren der Umgebungsvariablen

Enterprise Data Catalog 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.

Um Umgebungsvariablen unter Linux zu konfigurieren, melden Sie sich mit dem Systembenutzerkonto an, das Sie zur Installation von Enterprise Data Catalog verwendet haben.

Konfigurieren von Umgebungsvariablen für Enterprise Data Catalog

Sie können Umgebungsvariablen für Enterprise Data Catalog konfigurieren, um Speicher-, Domänen- und Standorteinstellungen zu speichern.

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 Enterprise Data Catalog verwendeten Systemspeichers zu konfigurieren. Um zum Beispiel 1 GB Systemspeicher für den Informatica-Daemon unter Linux in einer C-Shell zu konfigurieren, verwenden Sie den folgenden Befehl:

```
setenv INFA_JAVA_OPTS "-Xmx1024m"
```

Starten Sie den Knoten neu, damit die Änderungen wirksam werden.

INFA_DOMAINS_FILE

Das Installationsprogramm erstellt im Installationsverzeichnis von Enterprise Data Catalog eine domains.infa-Datei. Die domains.infa-Datei enthält die Konnektivitätsinformationen der Gateway-Knoten in einer Domäne, einschließlich der Domänennamen, Domänenhostnamen und Domänenhost-Portnummern.

Stellen Sie den Wert der Variable INFA_DOMAINS_FILE auf den Pfad und Dateinamen der Datei domains.infa ein.

Konfigurieren Sie die INFA_DOMAINS_FILE-Variable auf dem Computer, auf dem Sie die Enterprise Data Catalog-Dienste installieren.

INFA_HOME

Legen Sie das Installationsverzeichnis für Enterprise Data Catalog mithilfe von INFA_HOME fest. Wenn Sie die Verzeichnisstruktur von Enterprise Data Catalog ändern, müssen Sie als Umgebungsvariable den

Speicherort des Installationsverzeichnisses von Enterprise Data Catalog oder das Verzeichnis festlegen, in dem sich die Dateien der Enterprise Data Catalog-Installation befinden.

Unter Linux verwenden Sie beispielsweise einen Softlink für alle Enterprise Data Catalog-Verzeichnisse. Um INFA_HOME so zu konfigurieren, dass alle Anwendungen bzw. Dienste von Enterprise Data Catalog die anderen Enterprise Data Catalog-Komponenten finden können, die für die Ausführung erforderlich sind, legen Sie für INFA_HOME den Speicherort des Installationsverzeichnisses für Enterprise Data Catalog fest.

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.

Hinweis: Sie müssen die Variablen INFA_TRUSTSTORE und INFA_TRUSTSTORE_PASSWORD auf allen Knoten im Cluster konfigurieren.

Konfigurieren der Bibliothekspfad-Umgebungsvariablen unter Linux

Konfigurieren Sie Bibliothekspfad-Umgebungsvariablen auf den Computern, auf denen die Prozesse des Datenintegrationsdiensts ausgeführt werden. Der Name der Variable und die Anforderungen hängen von der Plattform und der Datenbank ab.

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	<Datenbankpfad>/lib
IBM DB2	<Datenbankpfad>/lib
Sybase ASE	"\${SYBASE_OCS}/lib:\${SYBASE_ASE}/lib:\${LD_LIBRARY_PATH}"
ODBC	<CLOSEDODBCHOME>/lib

Berechtigungen des Katalogdiensts

Von den Berechtigungen des Katalogdiensts hängt ab, welche Aktionen die Benutzer für Catalog Administrator und Enterprise Data Catalog ausführen können.

In der folgenden Tabelle sind die erforderlichen Berechtigungen in der Berechtigungsgruppe "Katalog" und die Aktionen, die die Benutzer durchführen können, aufgeführt:

Name der Berechtigung	Beschreibung
Katalogverwaltung: Katalogansicht	Benutzer können die folgenden Aktionen ausführen: <ul style="list-style-type: none"> - Benutzerdefinierte Attribute anzeigen - Datenobjekte suchen - Datenobjekte mit Suchfiltern filtern - Übersicht über Datenobjekte anzeigen - Herkunft von Datenobjekten anzeigen - Datenobjektbeziehungen anzeigen
Katalogverwaltung: Katalogbearbeitung	Benutzer können die folgenden Aktionen ausführen: <ul style="list-style-type: none"> - Benutzerdefinierte Attribute bearbeiten - Suchfilter konfigurieren - Suchfilter anzeigen
Ressourcenverwaltung: Admin – Ressource anzeigen	Benutzer können die folgenden Aktionen ausführen: <ul style="list-style-type: none"> - Ressource anzeigen - Zeitplan anzeigen
Ressourcenverwaltung: Admin – Profiling bearbeiten	Benutzer können die folgenden Aktionen ausführen: <ul style="list-style-type: none"> - Ressource anzeigen - Zeitplan anzeigen - Profileinstellungen aktualisieren - Globale Profiling-Konfiguration erstellen - Globale Profiling-Konfiguration aktualisieren - Globale Profiling-Konfiguration löschen - Globale Profiling-Konfiguration anzeigen
Ressourcenverwaltung: Admin – Ressource bearbeiten	Benutzer können die folgenden Aktionen ausführen: <ul style="list-style-type: none"> - Ressource erstellen - Ressource aktualisieren - Ressource anzeigen - Ressource löschen - Ressource bereinigen - Profiling-Einstellungen bearbeiten - Zeitplan erstellen - Zeitplan aktualisieren - Zeitplan löschen - Zeitplan anzeigen - Zeitplan der Ressource zuordnen - Zeitplan bereinigen - Verbindung zuweisen - Zuweisung von Verbindung aufheben
Admin – Attribut erstellen	Benutzer können die folgenden Aktionen ausführen: <ul style="list-style-type: none"> - Systemattribut aktualisieren - Benutzerdefiniertes Attribut erstellen - Benutzerdefiniertes Attribut aktualisieren - Benutzerdefiniertes Attribut löschen
Admin – Überwachung	Benutzer können die folgenden Aktionen ausführen: <ul style="list-style-type: none"> - Überwachungsjob anzeigen - Drilldown für Überwachungsjob ausführen - Überwachungsjob fortsetzen - Überwachungsjob anhalten - Überwachungsjob abbrechen - E-Mail-Benachrichtigung aktivieren

In der folgenden Tabelle sind die erforderlichen Berechtigungen und die Aktion aufgeführt, die Benutzer mit der Berechtigung in der Gruppe API-Berechtigungen ausführen können:

Name der Berechtigung	Beschreibung
REST-API-Berechtigung	Benutzer können Funktionen von Enterprise Data Catalog mithilfe von REST-APIs ausführen.

KAPITEL 7

Vorbereiten zum Erstellen der Anwendungsdienste

Dieses Kapitel umfasst die folgenden Themen:

- [Vorbereitung zum Erstellen der Anwendungsdienste – Übersicht, 137](#)
- [Anmelden beim Informatica Administrator, 137](#)
- [Erstellen von Verbindungen, 138](#)

Vorbereitung zum Erstellen der Anwendungsdienste – Übersicht

Bevor Sie einen Anwendungsdienst erstellen, überprüfen Sie die Installation und Konfiguration auf den Knoten.

Melden Sie sich beim Administrator Tool an und erstellen Sie Verbindungen zu den Datenbanken, auf die die Anwendungsdienste über die Cluster-Konnektivität zugreifen.

Anmelden beim Informatica Administrator

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

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 im Dialogfeld **Adresse** 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://<Name des vollqualifizierten Hosts>:<HTTP-Port>/administrator/
```

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

```
https://<Name des vollqualifizierten Hosts>:<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.

3. Geben Sie den Benutzernamen, das Passwort und die Sicherheitsdomäne für Ihr Benutzerkonto ein, und klicken Sie dann auf **Anmeldung**.

Das Dialogfeld **Sicherheitsdomäne** wird angezeigt, 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.

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 <code>dbname</code> 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: <code>jdbc:informatica:sqlserver:// <host>:<port>;databaseName=<dbname></code>
Verbindungszeichenfolge für den Datenzugriff	Die Verbindungszeichenfolge für die Datenvorschau und das Ausführen von Mappings. Geben Sie <code><ServerName>@<DBName></code> 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
Eigentümernamen	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 <code>dbname.world</code> 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 > Verbindung**.
Das Dialogfeld **Neue Verbindung** wird eingeblendet.
5. Wählen Sie im Dialogfeld **Neue Verbindung** den Verbindungstyp aus und klicken Sie dann auf **OK**.
Der Assistent **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 **Fertigstellen**.

KAPITEL 8

Erstellen der Anwendungsdienste

Dieses Kapitel umfasst die folgenden Themen:

- [Erstellen der Anwendungsdienste – Übersicht, 143](#)
- [Überprüfen der Voraussetzungen für Anwendungsdienste, 143](#)
- [Abhängigkeiten von Anwendungsdiensten, 145](#)
- [Erstellen und Konfigurieren des Modellrepository-Dienstes, 145](#)
- [Erstellen und Konfigurieren des Datenintegrationsdienstes, 150](#)
- [Erstellen eines Katalogdiensts, 153](#)
- [Erstellen und Konfigurieren des Content-Management-Dienstes, 160](#)

Erstellen der Anwendungsdienste – Übersicht

Wenn Sie beim Installieren von Enterprise Data Catalog keine Anwendungsdienste erstellen möchten, können Sie die Anwendungsdienste mit dem Informatica Administrator Tool in der erforderlichen Reihenfolge 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 z. B. den Modellrepository-Dienst und den Datenintegrationsdienst erstellen, bevor Sie den Katalogdienst 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

Bevor Sie einen Anwendungsdienst erstellen, überprüfen Sie, ob Sie die folgenden erforderlichen Aufgaben ausgeführt haben:

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 zum Speichern der Profiling- und Datenqualitätsstatistiken
- Referenzdaten-Warehouse zum Speichern von Daten für den Content-Managementdienst.

Installieren der Datenbank-Clientsoftware auf den Servercomputern

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.

Konfigurieren von Datenbank-Client-Umgebungsvariablen unter Linux

Sie müssen die Datenbank-Client-Umgebungsvariablen auf den Computern konfigurieren, auf denen der Datenintegrationsdienst ausgeführt wird.

Erstellen einer Keytab-Datei für den Dienst

Wenn Sie die Dienstprinzipalebene auf der Prozessebene festlegen, müssen Sie eine eindeutige Keytab-Datei für die folgenden Dienste erstellen:

- Modellrepository-Dienst
- Datenintegrationsdienst
- Content-Management-Dienst
- Katalogdienst

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 den Katalogdienst.

Bestimmen der Codepage für das Repository

Stellen Sie sicher, dass die Domänenkonfigurationsdatenbank mit den Codepages der Anwendungsdienste, die Sie in der Domäne erstellen, kompatibel ist.

Konfigurieren der Gebietsschema-Umgebungsvariablen unter Linux

Überprüfen Sie, ob die Gebietsschemaeinstellungen auf Computern, die auf das Informatica Administrator Tool und die Enterprise Data Catalog-Tools zugreifen, mit den Codepages der Repositorys in der Domäne kompatibel sind.

Konfigurieren der Bibliothekspfad-Umgebungsvariablen unter Linux

Konfigurieren Sie Bibliothekspfad-Umgebungsvariablen auf den Computern, auf denen der Datenintegrationsdienst ausgeführt wird.

Erstellen Sie Verbindungen zu den Datenbanken, auf die die Anwendungsdienste über die Cluster-Konnektivität zugreifen.

Erstellen Sie im Informatica Administrator Tool Verbindungen zu den folgenden Datenbanken:

- Referenzdaten-Warehouse
- Datenobjekt-Cache-Datenbank

- Profiling-Warehouse-Datenbank

Abhängigkeiten von Anwendungsdiensten

Ein abhängiger Anwendungsdienst ist ein Anwendungsdienst, der mindestens einen anderen Anwendungsdienst benötigt. Vor dem Erstellen eines abhängigen Diensts müssen Sie alle Anwendungsdienste erstellen, die der abhängige Dienst benötigt.

Beispiel: Der Datenintegrationsdienst ist vom Modellrepository-Dienst abhängig. Beim Erstellen eines Datenintegrationsdiensts müssen Sie im Informatica Administrator Tool den Namen eines Modellrepository-Diensts angeben. Daher müssen Sie vor dem Erstellen eines Datenintegrationsdiensts zunächst einen Modellrepository-Dienst erstellen.

Dienste, die auf Modellrepository-Objekte zugreifen, können 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. Katalogdienst.
Der Katalogdienst ist vom Modellrepository-Dienst und vom Datenintegrationsdienst abhängig.
4. Content-Management-Dienst.
Der Content-Management-Dienst ist vom Modellrepository-Dienst und vom Datenintegrationsdienst abhängig.

Erstellen und Konfigurieren des Modellrepository-Dienstes

Der Modellrepository-Dienst ist ein Anwendungsdienst, der das Modellrepository verwaltet. Im Modellrepository werden Metadaten gespeichert, die von Enterprise Data Catalog-Tools und Anwendungsdiensten in einer relationalen Datenbank erstellt wurden, um die Zusammenarbeit zwischen den Tools und den Diensten zu ermöglichen. Im Modellrepository werden außerdem die Ressourcenkonfiguration und die Datendomäneninformationen gespeichert.

Wenn Sie über die Tools von Enterprise Data Catalog oder über den Datenintegrationsdienst auf ein Modellrepository-Objekt zugreifen, sendet der Client oder der Dienst eine Anfrage an den Modellrepository-Dienst. Der Modellrepository-Dienstprozess ruft die 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	<code>jdbc:informatica:db2:// <host_name>:<port_number>;DatabaseName=<database_name>;BatchPerformanceWorkaround=true;DynamicSections=3000</code>
Microsoft SQL Server	<ul style="list-style-type: none"> - Microsoft SQL Server, der die Standardinstanz verwendet <code>jdbc:informatica:sqlserver:// <host_name>:<port_number>;DatabaseName=<database_name>;SnapshotSerializable=true</code> - Microsoft SQL Server, der eine benannte Instanz verwendet <code>jdbc:informatica:sqlserver://<host_name> \<named_instance_name>;DatabaseName=<database_name>;SnapshotSerializable=true</code>
Oracle	<code>jdbc:informatica:oracle:// <host_name>:<port_number>;SID=<database_name>;MaxPooledStatements=20;CatalogOptions=0;BatchPerformanceWorkaround=true</code>

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 <code>HostNameInCertificate</code> -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 <code>cryptoProtocolVersion=TLSv1.1</code> oder <code>cryptoProtocolVersion=TLSv1.2</code> 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-Diensts

Führen Sie nach dem Erstellen des Modellrepository-Diensts die folgenden Aufgaben durch:

- Erstellen des Modellrepository-Benutzers
- Erstellen Sie weitere Anwendungsdienste.

Erstellen des Modellrepository-Benutzers

Die Domäne verwendet ein Benutzerkonto, um andere Anwendungsdienste zu authentifizieren, die Anfragen an den Modellrepository-Dienst senden. 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-Diensts 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 **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-Diensts erstellen Sie die Anwendungsdienste, die vom Modellrepository-Dienst abhängig sind.

Erstellen Sie die abhängigen Dienste in der folgenden Reihenfolge:

1. Datenintegrationsdienst
2. Informatica-Cluster-Dienst, wenn Sie für die Installation von Enterprise Information Catalog die Option für den eingebetteten Hadoop-Cluster auswählen.
3. Katalogdienst
4. Content-Management-Dienst

Erstellen und Konfigurieren des Datenintegrationsdienstes

Der Datenintegrationsdienst ist ein Anwendungsdienst, der Datenintegrationsjobs für die Enterprise Data Catalog-Tools ausführt, z. B. für Informatica Administrator, das Suchwerkzeug in Enterprise Data Catalog und Informatica Catalog Administrator.

Wenn Sie Scans auf Ressourcen ausführen und die Metadaten und Profiling-Statistiken in Enterprise Data Catalog anzeigen, sendet das Client-Tool Anfragen an den Datenintegrationsdienst, um die Datenintegrations-Jobs auszuführen.

Erstellen des Datenintegrationsdienstes

Erstellen Sie den Dienst mithilfe des Diensterstellungs-Assistenten im Administrator Tool.

Überprüfen Sie vor dem Erstellen des Datenintegrationsdienstes, ob Sie der Modellrepository-Dienst erstellt und aktiviert wurde. Außerdem müssen Sie überprüfen, ob ein Modellrepository-Benutzer erstellt wurde, den der Datenintegrationsdienst für den Zugriff auf den Modellrepository-Dienst verwenden 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: <code>` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () []</code>
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.
Knoten	Knoten, auf dem der Dienst ausgeführt wird.

Eigenschaft	Beschreibung
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-Proxysereigenschaften 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 Datenintegrationsdiensts

Führen Sie nach dem Erstellen des Datenintegrationsdiensts die folgenden Aufgaben durch:

- Überprüfen Sie die Hostdateikonfiguration unter Linux.
- Erstellen Sie weitere Anwendungsdienste.

Überprüfen der Hostdateikonfiguration unter Linux

Wenn Sie den Datenintegrationsdienst unter Linux 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 Aufträge fehl, wenn die Eigenschaft **Jobs als separate Prozesse starten** für den Datenintegrationsdienst aktiviert ist.

Erstellen weiterer Dienste

Nach dem Erstellen des Datenintegrationsdiensts erstellen Sie die Anwendungsdienste, die vom Datenintegrationsdienst abhängig sind.

Erstellen Sie die abhängigen Dienste in der folgenden Reihenfolge:

1. Informatica-Cluster-Dienst, wenn Sie für die Bereitstellung von Enterprise Data Catalog die Option für den eingebetteten Hadoop-Cluster wählen.
2. Katalogdienst.
3. Content-Management-Dienst.

Erstellen eines Katalogdiensts

Erstellen Sie einen Katalogdienst, um die Enterprise Data Catalog-Anwendung auszuführen und die Verbindungen zwischen Enterprise Data Catalog-Komponenten zu verwalten. Sie können die allgemeinen Eigenschaften des Katalogdiensts sowie dessen Eigenschaften für den Anwendungsdienst und für die Sicherheit konfigurieren.

Wenn Sie Enterprise Data Catalog auf mehreren Knoten bereitstellen möchten, stellen Sie sicher, dass Sie den Informatica-Cluster-Dienst und den Katalogdienst auf separaten Knoten konfigurieren.

Hinweis: Der Katalogdienst weist dieselben Berechtigungen auf wie das Benutzerkonto, mit dem er erstellt wird. Stellen Sie sicher, dass das Benutzerkonto nicht über Berechtigungen zum Lesen oder Ändern vertraulicher Dateien auf dem System verfügt.

1. Wählen Sie im Administrator Tool eine Domäne aus, und klicken Sie auf die Registerkarte **Dienste und Knoten**.
2. Klicken Sie im Menü "Aktionen" auf **Neu > Katalogdienst**.
Das Dialogfeld **Neuer Katalogdienst – Schritt 1 von 4** wird geöffnet.
3. Konfigurieren Sie die allgemeinen Eigenschaften im Dialogfeld.
In der folgenden Tabelle werden die Eigenschaften beschrieben:

Eigenschaft	Beschreibung
Name	Name des Diensts. Der Name unterliegt nicht der Groß- und Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf maximal 128 Zeichen umfassen und nicht mit @ beginnen. Der Name darf keine Leerzeichen enthalten. Die Zeichen im Namen müssen mit der Codepage des Modellrepositorys kompatibel sein, das Sie mit dem Katalogdienst verknüpfen. Der Name darf folgende Zeichen nicht enthalten: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () []
Beschreibung	Beschreibung des Diensts. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Domäne, in der der Dienst ausgeführt wird.
Lizenz	Lizenz für die Zuweisung zum Katalogdienst. Wählen Sie die mit Informatica installierte Lizenz aus.
Knoten	Knoten in der Informatica-Domäne, auf dem der Katalogdienst ausgeführt wird. Wenn Sie den Knoten ändern, müssen Sie den Katalogdienst deaktivieren und erneut aktivieren.
Sicherungsknoten	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**.
Das Dialogfeld **Neuer Katalogdienst – Schritt 2 von 4** wird geöffnet.
5. Konfigurieren Sie die Eigenschaften des Anwendungsdiensts im Dialogfeld.
In der folgenden Tabelle werden die Eigenschaften beschrieben:

Eigenschaft	Beschreibung
Modellrepository-Dienst	Modellrepository-Dienst für die Zuordnung zum Katalogdienst. Der Modellrepository-Dienst verwaltet das von Enterprise Data Catalog verwendete Modellrepository. Wenn Sie die Eigenschaft aktualisieren, um einen anderen Modellrepository-Dienst anzugeben, müssen Sie den Katalogdienst deaktivieren und erneut aktivieren.
Benutzername	Der Datenbankbenutzername für das Modellrepository.

Eigenschaft	Beschreibung
Passwort	Eine verschlüsselte Version des Datenbankpassworts für das Modellrepository.
Sicherheitsdomäne	Name der Sicherheitsdomäne, die den Benutzernamen enthält.

- Klicken Sie auf **Weiter**.
Das Dialogfeld **Neuer Katalogdienst – Schritt 3 von 4** wird geöffnet.
- Konfigurieren Sie die Sicherheitseigenschaften im Dialogfeld.
In der folgenden Tabelle werden die Eigenschaften beschrieben:

Eigenschaft	Beschreibung
HTTP-Port	Eine eindeutige HTTP-Portnummer, die für jeden Datenintegrationsdienst-Prozess verwendet wird. Der Standard ist 8085.
TLS (Transport Layer Security) aktivieren	Gibt an, dass der Katalogdienst HTTPS verwenden muss. Wenn Sie den Datenintegrationsdienst nicht für die Verwendung von HTTPS konfiguriert haben, wird der Katalogdienst nicht gestartet.
HTTPS-Port	Portnummer für die HTTPS-Verbindung.
Schlüsselspeicherdatei	Pfad und Dateiname der Schlüsselspeicherdatei. Die Schlüsselspeicherdatei enthält die Schlüssel und Zertifikate, die bei Verwendung des SSL-Sicherheitsprotokolls mit Catalog Administrator erforderlich sind. Erforderlich, wenn Sie die Option TLS (Transport Layer Security) aktivieren auswählen. Wenn Enterprise Data Catalog den Katalogdienst erstellt, exportiert es den Schlüsselspeicher in ein Zertifikat und speichert das Zertifikat im Schlüsselspeicherverzeichnis. Stellen Sie sicher, dass Sie die Lese- und Schreibberechtigungen für das Verzeichnis für Enterprise Data Catalog so konfigurieren, dass das Zertifikat erfolgreich gespeichert wird.
Schlüsselspeicherpasswort	Passwort für die Schlüsselspeicherdatei. Erforderlich, wenn Sie die Option TLS (Transport Layer Security) aktivieren auswählen.
SSL-Protokoll	Zu verwendendes Secure Sockets Layer-Protokoll.

- Klicken Sie auf **Weiter**.
Das Dialogfeld **Neuer Katalogdienst – Schritt 4 von 4** wird geöffnet.
- Konfigurieren Sie die Hadoop-Clustereigenschaften im Dialogfeld.

In der folgenden Tabelle werden die Eigenschaften beschrieben:

Eigenschaft	Beschreibung
Cluster-Typ	<p>Wählen Sie eine der folgenden Optionen aus, um den Bereitstellungstyp für Enterprise Data Catalog anzugeben:</p> <ul style="list-style-type: none"> - Externer Cluster. Bereitstellung von Enterprise Data Catalog in einem vorhandenen Hadoop-Cluster auf Hortonworks, ClouderaManager oder Azure HDInsight. - Interner Cluster. Bereitstellung von Enterprise Data Catalog im eingebetteten Hadoop-Cluster auf Hortonworks.
Hadoop-Verteilung	<p>Anwendbar, wenn Sie die Option Externer Cluster als Clustertyp auswählen. Wählen Sie eine der folgenden Optionen aus, um die Hadoop-Verteilung anzugeben:</p> <ul style="list-style-type: none"> - ClouderaManager. Verwenden Sie diese Option, wenn Sie eine ClouderaManager-Hadoop-Verteilung verwenden möchten. - Hortonworks. Verwenden Sie diese Option, wenn Sie eine Hortonworks-Hadoop-Verteilung verwenden möchten. <p>Hinweis: Wenn Sie ClouderaManager oder Hortonworks als Hadoop-Verteilung auswählen, erkennt Enterprise Data Catalog automatisch die folgenden Eigenschaften für den Hadoop-Verteilungstyp:</p> <ul style="list-style-type: none"> - ZooKeeper-Cluster-URI - HDFS-NameNode-URI - URI des Yarn-Ressourcenmanagers - HTTPS- oder HTTP-URI des Yarn-Ressourcenmanagers - HTTP-URI des Verlaufsservers - Name des HDFS-Diensts für hohe Verfügbarkeit - URI des Yarn-Ressourcenmanager-Schedulers <p>- HDInsight. Verwenden Sie diese Option, wenn Sie eine Azure HDInsight-Hadoop-Verteilung verwenden möchten.</p> <p>- Andere. Verwenden Sie diese Option, wenn Sie alle Eigenschaften für eine ClouderaManager-, Hortonworks- oder Azure HDInsight-Hadoop-Verteilung manuell angeben möchten. Konfigurieren Sie die folgenden benutzerdefinierten Optionen für den Katalogdienst:</p> <ul style="list-style-type: none"> - LdmCustomOptions.yarn-site.yarn.application.classpath - LdmCustomOptions.yarn-site.yarn.nodemanager.webapp.address - LdmCustomOptions.yarn-site.yarn.nodemanager.webapp.https.address <p>Hinweis: Wenn Sie ClouderaManager oder Hortonworks auswählen, müssen Sie die folgenden Eigenschaften mit den anderen erforderlichen Eigenschaften konfigurieren:</p> <ul style="list-style-type: none"> - Cluster-URL. Die Cluster-URL für den Zugriff auf die ausgewählte Hadoop-Verteilung. - Cluster-URL-Benutzername. Der Benutzername für den Zugriff auf die Cluster-URL. - Cluster-URL-Passwort. Das dem Cluster-URL-Benutzernamen zugeordnete Passwort.
ZooKeeper-Cluster-URI	<p>Gilt für vorhandenen Cluster. Mehrere ZooKeeper-Adressen in einer durch Kommas getrennten Liste.</p>

Eigenschaft	Beschreibung
HDFS-NameNode-URI	Gilt für vorhandenen Cluster. Der URI für den Zugriff auf HDFS. Verwenden Sie das folgende Format, um den NameNode-URI in der Cloudera-Verteilung anzugeben: <Hostname>:<Port> Wobei <ul style="list-style-type: none"> - <Hostname> der Hostname bzw. die IP-Adresse von NameNode ist. - <Portnummer> die Nummer des Ports ist, den der NameNode auf Remoteprozedurabrufe (RPC) abhört.
URI des Yarn-Ressourcenmanagers	Gilt für vorhandenen Cluster. Der Dienst innerhalb von Hadoop, der die MapReduce-Aufgaben an bestimmte Knoten im Cluster sendet. Verwenden Sie das folgende Format:<Hostname>:<Port> Wobei <ul style="list-style-type: none"> - <Hostname> der Hostname bzw. die IP-Adresse des Yarn-Ressourcenmanagers ist. - <Portnummer> die Nummer des Ports ist, den der Yarn-Ressourcenmanager auf Remoteprozeduraufrufe (RPC) abhört.
HTTPS- oder HTTP-URI des Yarn-Ressourcenmanagers	Gilt für vorhandenen Cluster. HTTPS- oder HTTP-URI-Wert für den Yarn-Ressourcenmanager.
HTTP-URI des Verlaufsservers	Gilt für vorhandenen Cluster. Geben Sie einen Wert für die Generierung von YARN-Zuordnungsprotokolldateien für Scanner an. Catalog Administrator zeigt die Protokoll-URL im Zuge der Aufgabenüberwachung an.
Name des HDFS-Diensts für hohe Verfügbarkeit	Gilt für vorhandenen hochverfügbaren Cluster. Geben Sie den HDFS-Dienstnamen an.
URI des Yarn-Ressourcenmanager-Schedulers	Gilt für vorhandenen Cluster. Der Scheduler-URI-Wert für den Yarn-Ressourcenmanager.
Dienst-Clustername	Gilt für eingebettete und vorhandene Cluster. Name des Dienst-Clusters. Stellen Sie sicher, dass in HDFS ein Verzeichnis /Informatica/LDM/<ServiceClusterName> in HDFS vorhanden ist. Hinweis: Wenn Sie keinen Dienst-Clusternamen angeben, betrachtet Enterprise Data Catalog DomainName_CatalogServiceName als Standardwert. Das Verzeichnis /Informatica/LDM/<DomainName>_<CatalogServiceName> muss sich dann in HDFS befinden. Andernfalls kann der Katalogdienst fehlschlagen.
Ladetyp	Wählen Sie eine der folgenden Optionen aus, um die Datengröße anzugeben, die Sie im Katalog laden möchten: <ul style="list-style-type: none"> - Demo - Niedrig - Mittel - Hoch Weitere Informationen zur Datengröße, zu Ladetypen und zu den Werten der Leistungsoptimierungsparameter, die Enterprise Data Catalog für jeden Ladetyp konfiguriert, finden Sie im Artikel <i>Optimieren der Leistung von Enterprise Data Catalog</i> in der Informatica-Ratgeber-Bibliothek.
Aktivieren der Kerberos-Authentifizierung	Wählen Sie diese Option aus, um die Kerberos-Authentifizierung für den vorhandenen Cluster zu aktivieren.

Eigenschaft	Beschreibung
HDFS-Dienstprinzipalname	Gilt für die Kerberos-Authentifizierung. Prinzipalname für den HDFS-Dienst.
YARN-Dienstprinzipalname	Gilt für die Kerberos-Authentifizierung. Prinzipalname für den YARN-Dienst.
Dienst-Keytab-Speicherort	Gilt für die Kerberos-Authentifizierung. Pfad zur Keytab-Datei.
Kerberos-Domänenname	Gilt für die Kerberos-Authentifizierung. Der Name der Kerberos-Domäne.
Cluster-SSL aktivieren	Wählen Sie diese Option aus, um die SSL-Authentifizierung für sichere Kommunikation im vorhandenen Cluster zu aktivieren.
Solr-Schlüsselspeicher	Gilt für die SSL-Authentifizierung. Pfad zur Solr-Schlüsselspeicherdatei.
Solr-Schlüsselspeicherpasswort	Gilt für die SSL-Authentifizierung. Passwort für die Solr-Schlüsselspeicherdatei.
Benachrichtigungen per E-Mail erhalten	Gilt für eingebettete und vorhandene Cluster. Wählen Sie diese Option, um E-Mail-Benachrichtigungen über den Status des Katalogdiensts zu erhalten. Hinweis: Wenn Sie diese Option auswählen, müssen Sie den E-Mail-Dienst aktivieren. Weitere Informationen zum Aktivieren des E-Mail-Diensts finden Sie im Handbuch <i>Administrator-Referenz für Enterprise Data Catalog</i> .
Katalogdienst aktivieren	Gilt für eingebettete und vorhandene Cluster. Wählen Sie diese Option, um den Katalogdienst zu aktivieren.
Informatica-Cluster-Dienst	Gilt für eingebetteten Cluster. Name des Informatica-Cluster-Diensts, bei dem es sich um einen Anwendungsdienst handelt, den Enterprise Data Catalog in der eingebetteten Clusterbereitstellung verwendet.

10. Klicken Sie auf **Fertig stellen**.

- Vergewissern Sie sich, dass sich die `krb5.conf`-Datei auf allen Clusterknoten und Domänencomputern unter dem Verzeichnis `/etc` befindet.
- Wenn Sie den Katalogdienst bisher noch nicht aktiviert haben, müssen Sie ihn aktivieren und wieder deaktivieren, um ihn starten zu können.

Konfigurieren des Katalogdiensts für Azure HDInsight

Führen Sie die folgenden Schritte aus, um den Katalogdienst für einen Azure HDInsight-Cluster zu konfigurieren:

1. Geben Sie die folgenden Eigenschaften und Werte in das Dialogfeld **Neuer Katalogdienst – Schritt 4 von 4** ein:

Eigenschaft	Beschreibung
Cluster-Typ	Externer Cluster
Hadoop-Verteilung	HDInsight

Eigenschaft	Beschreibung
Cluster-URL	Vollqualifizierter Hostname für den Zugriff auf den Cluster.
Cluster-URL-Benutzername	Benutzername für den Zugriff auf den Cluster.
Cluster-URL-Passwort	Passwort für den Cluster-URL-Benutzernamen.

2. Nachdem Sie den Katalogdienst erstellt haben, können Sie die folgenden benutzerdefinierten Eigenschaften in Informatica Administrator für den Katalogdienst konfigurieren:

Benutzerdefinierte Eigenschaft	Beschreibung
LdmCustomOptions.deployment.azure.account.key	Der Schlüssel zum Authentifizieren des Katalogdiensts für die Verbindung mit dem Azure-Speicherkonto. Der Wert des Azure-Speicherkontoschlüssels kann verschlüsselt oder unverschlüsselt sein. Sie können den Wert aus der Eigenschaft <code>fs.azure.account.key.<Name des Speicherkontos></code> in der Datei <code>core-site.xml</code> abrufen, die sich im Azure HDInsight-Cluster befindet.
LdmCustomOptions.deployment.azure.key.decryption.script.path	Wenn der Schlüssel in der Eigenschaft <code>LdmCustomOptions.deployment.azure.account.key</code> im verschlüsselten Format vorliegt, können Sie das Entschlüsselungs-Shell-Skript verwenden, um den Schlüssel mit dem Schlüsselzertifikat zu entschlüsseln. Sie müssen das Entschlüsselungs-Shell-Skript und die Schlüsselzertifikatdatei auf den Domänencomputer (unter demselben Pfad wie der Clustercomputer) kopieren, bevor Sie den Katalogdienst aktivieren. Den Pfad im Azure HDInsight-Clustercomputer müssen Sie für die kopierten Dateien im Domänencomputer beibehalten. Der Wert für die Eigenschaft ist der Speicherort des Entschlüsselungs-Shell-Skripts. Beispiel: <code>/usr/lib/python2.7/dist-packages/hdinsight_common/decrypt.sh</code> . Die Schlüsselzertifikatdatei <code>"key_decryption_cert.prv"</code> befindet sich im Verzeichnis <code>/usr/lib/hdinsight-common/certs/key_decryption_cert.prv</code> des Azure HDInsight-Clusters.
LdmCustomOptions.deployment.hdfs.default.fs	Adresse des WASB-Speicherkontos, mit dem der Katalogdienst eine Verbindung herstellen muss. Die Adresse enthält den Namen des WASB-Speichercontainers mit dem Namen des Speicherkontos. Der Wert für die Eigenschaft ist die vollständige WASB-Adresse mit den Namen des Containers und des Speicherkontos. Sie können den Wert für die Eigenschaft aus der Eigenschaft <code>fs.defaultFS</code> in der Datei <code>core-site.xml</code> abrufen, die sich im Azure HDInsight-Cluster befindet.

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 Referenztabelle 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
- Referenztabelle

Erstellen des Content-Management-Dienstes

Erstellen Sie den Dienst mithilfe des Diensterstellungs-Assistenten im Administrator Tool.

Überprüfen Sie vor dem Erstellen des Content-Management-Dienstes, ob Sie den Modellrepository-Dienst und den Datenintegrationsdienst erstellt und aktiviert haben. Außerdem müssen Sie überprüfen, ob Sie einen Modellrepository-Benutzer erstellt haben, den der Content-Management-Dienst für den Zugriff auf den Modellrepository-Dienst verwenden kann.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie auf **Aktionen > Neu > Content-Management-Dienst**.
Das Dialogfeld **Neuer Content-Management-Dienst** wird angezeigt.
3. Geben Sie auf der Seite **Neuer Content-Management-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: <code>` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () []</code>
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.

Eigenschaft	Beschreibung
Lizenz	Lizenzobjekt für die Verwendung des Diensts.
Knoten	Knoten, auf dem der Dienst ausgeführt wird.
HTTP-Port	HTTP-Portnummer für den Content-Management-Dienst.
Datenintegrationsdienst	Datenintegrationsdienst , der dem Dienst zugeordnet werden soll. Der Datenintegrationsdienst und der Content-Management-Dienst 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 Zugriff des Content-Management-Diensts auf das Referenzdaten-Warehouse erstellt haben. Klicken Sie auf Auswählen , um die Verbindung auszuwählen.

4. Klicken Sie auf **Weiter**.

Die Seite **Neuer Content-Management-Dienst – Schritt 2 von 2** wird angezeigt.

5. Übernehmen Sie die Standardwerte für die Sicherheitseigenschaften.

6. Wählen Sie **Dienst aktivieren**.

Der Modellrepository-Dienst und der Datenintegrationsdienst müssen ausgeführt werden, um den Content-Management-Dienst aktivieren zu können.

7. Klicken Sie auf **Fertig stellen**.

Die Domäne erstellt und aktiviert den Content-Management-Dienst.

Nachdem Sie den Dienst mithilfe des Assistenten erstellt haben, können Sie die Eigenschaften bearbeiten oder andere Eigenschaften konfigurieren.

KAPITEL 9

Konfigurieren von Single Sign-On mithilfe der SAML-Authentifizierung

- [Übersicht über Single Sign-On mithilfe der SAML-Authentifizierung, 162](#)

Übersicht über Single Sign-On mithilfe der SAML-Authentifizierung

Sie können Single Sign-On mithilfe der SAML-Authentifizierung für Enterprise Data Catalog-Anwendungen aktivieren.

Wenn Sie die SAML-Authentifizierung bei der Installation von Enterprise Data Catalog aktiviert hatten, können Sie sie auf eine der folgenden Arten aktivieren:

- OKTA mit Active Directory
- Active Directory-Verbunddienste (Active Directory Federation Services, AD FS) mit Active Directory

Je nach SAML-Authentifizierungsmethode, die Sie implementieren, müssen Sie einen der folgenden Schritte durchführen:

- Konfigurieren des standardmäßigen RelayState-URL-Parameters in OKTA.
- Konfigurieren von Anwendungs-URL-Endpunkten für Enterprise Data Catalog in AD FS.

Wenn Sie die SAML-Authentifizierung bei der Installation von Enterprise Data Catalog nicht aktiviert hatten, befolgen Sie die Anweisungen im Abschnitt zum *SAML-basierten Single Sign-on für Informatica-Webanwendungen* im *Informatica 10.2.1-Sicherheitshandbuch*.

Konfigurieren des standardmäßigen RelayState-URL-Parameters in OKTA

Wenn Sie die SAML-Authentifizierung mit OKTA und Active Directory nutzen möchten, stellen Sie sicher, dass Sie den Standard RelayState-URL-Parameter in OKTA im folgenden Format konfigurieren:

```
namespaceINFA_SAML_IDP_DATA_VALUE_SEPERATOR<namespace-  
value>INFA_SAML_IDP_DATA_SEPERATORdef_webapp_urlINFA_SAML_IDP_DATA_VALUE_SEPERATOR/<app-  
context>/INFA_SAML_IDP_DATA_SEPERATORrequested_urlINFA_SAML_IDP_DATA_VALUE_SEPERATOR/  
<app-context>/INFA_SAML_IDP_DATA_SEPERATOR
```

In der folgenden Tabelle sind die Eigenschaften und Werte aufgeführt, die Sie in der RelayState-URL ersetzen müssen:

Eigenschaft	Wert
<namespace-value>	Ersetzen Sie diese Eigenschaft durch den für OKTA konfigurierten Namespace.
<app-context>	ldmadmin

Konfigurieren von Anwendungs-URL-Endpunkten für Enterprise Data Catalog in den Active Directory-Verbunddiensten

Wenn Sie die SAML-Authentifizierung mit AD FS und Active Directory verwenden möchten, müssen Sie URLs hinzufügen, um auf die folgenden Informatica-Anwendungen als Endpunkte in AD FS zuzugreifen:

- Informatica Administrator
- Analyst-Tool
- Catalog Administrator
- Enterprise Data Catalog

Weitere Informationen zum Hinzufügen der URLs zu AD FS finden Sie im Abschnitt zum *Hinzufügen von Informatica-Webanwendungs-URLs zu AD FS* im *Informatica 10.2.1-Sicherheitshandbuch*.

Teil V: Deinstallation

- [Deinstallation, 165](#)

KAPITEL 10

Deinstallation

Dieses Kapitel umfasst die folgenden Themen:

- [Deinstallation - Übersicht, 165](#)
- [Regeln und Richtlinien für die Deinstallation, 165](#)
- [Deinstallation von Enterprise Data Catalog, 166](#)

Deinstallation - Übersicht

Deinstallieren Sie Enterprise Data Catalog, um die Enterprise Data Catalog-Dateien zu entfernen.

Beim Deinstallationsprozess für Enterprise Data Catalog werden alle Enterprise Data Catalog-Dateien gelöscht und alle Konfigurationen von Enterprise Data Catalog entfernt. Dabei werden nur die Dateien gelöscht, die mit Enterprise Data Catalog installiert wurden. 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.

Wenn Sie Enterprise Data Catalog installieren, erstellt das Installationsprogramm ein Deinstallationsprogramm. Das Deinstallationsprogramm wird im Verzeichnis für die Deinstallation innerhalb des Installationsverzeichnisses gespeichert.

Verwenden Sie zum Deinstallieren von Enterprise Data Catalog die Befehlszeile.

Regeln und Richtlinien für die Deinstallation

Halten Sie sich an die folgenden Regeln und Richtlinien, wenn Sie Enterprise Data Catalog-Komponenten deinstallieren:

- Der Deinstallationsmodus für Enterprise Data Catalog hängt davon ab, welchen Modus Sie für die Installation von Enterprise Data Catalog verwenden. Beispiel: Wenn Sie Enterprise Data Catalog im Konsolenmodus installieren, dann wird das Deinstallationsprogramm ebenfalls im Konsolenmodus ausgeführt.
- Die Deinstallation von Enterprise Data Catalog hat keine Auswirkungen auf die Enterprise Data Catalog-Repositories. Das Deinstallationsprogramm entfernt die Enterprise Data Catalog-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 Enterprise Data Catalog werden die Metadatentabellen nicht aus der Domänenkonfigurationsdatenbank entfernt. Wenn Sie Enterprise Data Catalog erneut mit der gleichen Domänenkonfigurationsdatenbank und dem gleichen Benutzerkonto installieren, müssen Sie die Tabellen manuell entfernen oder sie überschreiben. Sie können den Befehl `infasetup BackupDomain` ausführen, um die Domänenkonfigurationsdatenbank zu sichern, bevor Sie die Metadatentabellen überschreiben. Führen Sie den Befehl `infasetup DeleteDomain` vor dem Deinstallationsprogramm aus, um die Metadatentabellen manuell zu entfernen.
- Beim Deinstallieren von Enterprise Data Catalog werden alle Installationsdateien und Unterverzeichnisse aus dem Installationsverzeichnis von Enterprise Data Catalog entfernt. Bevor Sie Enterprise Data Catalog deinstallieren, müssen Sie alle Dienste und Prozesse von Enterprise Data Catalog beenden und sicherstellen, 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 von Enterprise Data Catalog wird für Dateien und Bibliotheken, die von mithilfe der Informatica Developer Platform-APIs erstellten Drittanbieteradaptern benötigt werden, der folgende Ordner erstellt:

```
<Enterprise Data Catalog-Installationsverzeichnis>/services/shared/extensions
```

Durch das Deinstallieren von Enterprise Data Catalog wird dieser Ordner mitsamt den darunter erstellten Unterordnern gelöscht.

Deinstallation von Enterprise Data Catalog

Sie können Enterprise Data Catalog unter Linux im Konsolenmodus oder im automatischen Modus deinstallieren.

Deinstallieren von Enterprise Data Catalog im automatischen Modus

Bevor Sie das Deinstallationsprogramm ausführen, halten Sie alle Enterprise Data Catalog-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:

```
<Enterprise Data Catalog-Installationsverzeichnis>/Uninstaller
```

2. Geben Sie den folgenden Befehl ein, um das automatische Deinstallationsprogramm auszuführen:

```
./uninstaller
```

Wenn Sie Enterprise Data Catalog im automatischen Modus installiert haben, wird das Deinstallationsprogramm im automatischen Modus gestartet. 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.

Teil VI: Fehlerbehebung

- [Fehlerbehebung , 168](#)

KAPITEL 11

Fehlerbehebung

Dieses Kapitel umfasst die folgenden Themen:

- [Fehlerbehebung – Übersicht, 168](#)
- [Fehlerbehebung bei Installationsprotokolldateien, 168](#)
- [Fehlerbehebung von Domänen und Knoten, 170](#)
- [Fehlerbehebung bei häufig auftretenden Problemen bei der Cluster-Bereitstellung, 172](#)
- [Fehlerbehebung bei der Bereitstellung auf einem vorhandenen Cluster, 179](#)
- [Fehlerbehebung bei der Bereitstellung auf einem eingebetteten Cluster, 180](#)
- [Fehlerbehebung bei Problemen mit Anwendungsdiensten, 184](#)

Fehlerbehebung – Übersicht

Dieses Kapitel enthält Informationen zum Informatica-Installationsprozess sowie zu Ursache und Behebung von Fehlern, die möglicherweise während der Installation auftreten. Das Kapitel enthält außerdem einige nützliche Tipps, die auf einigen realen Szenarios basieren, in denen die Probleme und Lösungen für die Bereitstellung auf einem eingebetteten Cluster, die Bereitstellung auf vorhandenen Clustern und die gemeinsame Clusterbereitstellung beschrieben werden.

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	<ul style="list-style-type: none">- 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	<ul style="list-style-type: none">- 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
- Pinggen der Domäne
- Hinzufügen einer Lizenz

Erstellen des Domänenkonfigurations-Repository

Bei Erstellung einer Domäne wird ein Domänenkonfigurations-Repository erstellt, in dem Metadaten gespeichert werden. Das Installationsprogramm fügt dem Domänenkonfigurations-Repository entsprechend den von Ihnen während der Installation eingegebenen Optionen Konfigurations-Metadaten hinzu. Das Installationsprogramm kommuniziert mittels JDBC mit der Datenbank. ODBC oder native Konnektivität auf dem Computer, auf dem Sie die Enterprise Data Catalog-Dienste installieren, brauchen Sie nicht zu konfigurieren.

Zur Überprüfung der Verbindungsdaten erstellt und löscht das Installationsprogramm eine Tabelle in der Domänenkonfigurations-Repository-Datenbank. Das Benutzerkonto für die Datenbank muss über Erstellungsrechte in der Datenbank verfügen. Jede Domäne muss über ein separates Domänenkonfigurations-Repository verfügen.

Erstellen einer Domäne oder Beitreten zu einer Domäne

Das Installationsprogramm führt je nachdem, ob Sie eine Domäne erstellen oder einer Domäne beitreten, unterschiedliche Aufgaben 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 Computer basierend auf den im Fenster Domäne konfigurierten eingegebenen Daten aus.
- **Beitreten zu einer Domäne.** Das Installationsprogramm führt den Befehl `infasetup DefineWorkerNode` zum Erstellen eines Knotens auf dem aktuellen Computer 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 Computer gehört. 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.

Ausführen einer Ressource

Der Wert für die Laufzeitanzahl ist negativ, wenn Sie eine Ressource ausführen.

Dieses Problem tritt auf, wenn die Systemuhr für den Informatica-Katalogdienst und die Uhr des Dienstknotencomputers nicht synchronisiert sind. Um dieses Problem zu beheben, müssen Sie sicherstellen, dass die Systemuhr für den Informatica-Katalogdienst und die Uhr des Dienstknotencomputers synchronisiert werden.

Starten von Enterprise Data Catalog

Das Installationsprogramm führt `infaservice` aus, um die Informatica-Dienste zu starten. Wenn Enterprise Data Catalog nicht startet, können Sie anhand der Informationen im Informatica-Debug-Protokoll Fehler beheben und die Fehlerursache mithilfe der Dienstmanager-Protokolldateien `"node.log"` und `"catalina.out"` 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 Domäne anfügen, melden Sie sich bei Informatica Administrator an, nachdem der Informatica-Dienst geprüft hat, ob der Knoten erfolgreich erstellt und gestartet wurde.

Enterprise Data Catalog kann aus folgenden Gründen nicht gestartet werden:

- **Der Dienstmanager hat nicht genügend Systemspeicher.** Die Java-Laufzeitumgebung (Java Runtime Environment, JRE), die Informatica startet und den Dienstmanager ausführt, hat eventuell nicht genügend Systemspeicher, um zu starten. Legen Sie die Umgebungsvariable `INFA_JAVA_OPTS` fest, um die Größe des von Enterprise Data Catalog verwendeten Systemspeichers zu konfigurieren. Unter Linux können Sie die Speicherkonfiguration beim Starten von Informatica festlegen.
- **Die Domänenkonfigurationsdatenbank ist nicht verfügbar.** Enterprise Data Catalog kann nicht auf einem Knoten gestartet werden, wenn der Dienstmanager auf einem Gateway-Knoten innerhalb von 30 Sekunden

keine Verbindung mit der Domänenkonfigurationsdatenbank herstellen konnte. Vergewissern Sie sich, dass das Domänenkonfigurations-Repository verfügbar ist.

- **Einige Ordner im Informatica-Installationsverzeichnis verfügen nicht über die entsprechenden Ausführungsberechtigungen.** Gewähren Sie die Ausführungsberechtigung für das Informatica-Installationsverzeichnis.
- **Localhost wird nicht erfolgreich aufgelöst.** Wenn Sie einen eingebetteten Cluster verwenden und localhost nicht erfolgreich aufgelöst wird, schlägt der Informatica-Cluster-Dienst möglicherweise fehl. Sie müssen überprüfen, ob localhost erfolgreich aufgelöst wird.

Pingen der Domäne

Das Installationsprogramm führt den Ping-Befehl *infacmd* aus, um zu überprüfen, ob die Domäne verfügbar ist, bevor die Installation fortgesetzt wird. Die Domäne muss verfügbar sein, damit ihr Lizenzobjekte hinzugefügt werden können. Wenn der Ping-Befehl fehlschlägt, starten Sie Enterprise Data Catalog 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. In Informatica Administrator finden Sie weitere Informationen zu vorhandenen Lizenzen für die Domäne.

Fehlerbehebung bei häufig auftretenden Problemen bei der Cluster-Bereitstellung

Aufnahme schlägt mit dem Fehler `org.apache.zookeeper.KeeperException$AuthFailedException: KeeperErrorCode = AuthFailed` fehl.

Fügen Sie der Datei `/etc/krb5.conf` für alle Cluster folgende Zeilen hinzu:

- `[[libdefaults]`
- `kdc_timeout=60000`
- `max_retries = 6`

Aufnahme schlägt mit dem Fehler `org.apache.zookeeper.KeeperException$SessionExpiredException: KeeperErrorCode = Session expired` fehl.

Legen Sie die folgenden benutzerdefinierten Eigenschaften für den Katalogdienst mit Informatica Administrator fest:

- `LdmCustomOptions.hclient.hbase.client.scanner.timeout.period = 900000`
- `LdmCustomOptions.hclient.hbase.rpc.timeout = 900000`
- `LdmCustomOptions.zkclient.zookeeper.session.timeout = 90000`

Scanner-Ausführung schlägt in einem Cluster fehl, der für hohe Verfügbarkeit konfiguriert ist.

Stellen Sie sicher, dass alle Cluster-Dienste wie HDFS, YARN und ZooKeeper im Cluster für hohe Verfügbarkeit konfiguriert sind.

Die Apache Zookeeper-Client-Verbindungsanzahl ist niedrig, und in der Zookeeper-Protokolldatei wird der folgende Fehler angezeigt: `"Too many connections from /<ip-adresse>- max is 60"`. Möglicherweise kommt es auch zu Fehlern beim Aufnahmedienst und in den Protokolldateien werden folgende Fehlermeldungen ausgewiesen: `"Unexpected error, closing socket connection and attempting reconnect java.io.IOException: Connection reset by peer"`.

Apache Zookeeper ist eine gemeinsame Anwendung und erfordert mehrere offene und konfigurierte Verbindungen. Ändern Sie den Wert des Parameters `maxclientCnxns` in den empfohlenen Wert für die jeweilige Cluster-Auslastung und starten Sie den gesamten Cluster erneut.

Der Katalogdienst kann nicht gestartet werden, nachdem Sie den Informatica-Cluster-Dienst neu gestartet haben.

Sie müssen den Katalogdienst manuell neu starten, wenn Sie den Informatica-Cluster-Dienst neu starten.

Eine der Clusterkomponenten wird nicht gestartet und in der Protokolldatei wird der folgende Fehler gemeldet: `"Caused by: java.lang.NumberFormatException: For input string: "0LdmCustomOptions.HbaseMasterProperties"`.

Dieses Problem kann auftreten, wenn in Informatica Administrator fehlerhafte Einstellungen der benutzerdefinierten Eigenschaften für den Katalogdienst konfiguriert wurden. Überprüfen Sie, ob jede benutzerdefinierte Eigenschaft, die Sie aktualisieren müssen, als separater `LdmCustomOptions`-Parameter in Informatica Administrator definiert ist. Anschließend können Sie den Katalogdienst erneut starten, um den Cluster aufzurufen.

Der Katalogdienst antwortet, und in der Protokolldatei wird die folgende Fehlermeldung ausgewiesen: `"Connection timed out for connection string () and timeout () / elapsed () org.apache.curator.CuratorConnectionLossException: KeeperErrorCode = ConnectionLoss at org.apache.curator.ConnectionState.checkTimeouts(ConnectionState.java:197)"`. Die Protokolldatei des Aufnahme-Clients oder von HBase kann die folgende Fehlermeldung enthalten: `"Possibly transient ZooKeeper, quorum=..., exception=org.apache.zookeeper.KeeperException ConnectionLossException: KeeperErrorCode = ConnectionLoss for /hbase/meta-region-server"`.

Dieses Problem kann auftreten, weil der Katalogdienst nicht in der Lage ist, einige der Kern-Clusterkomponenten, wie z. B. Apache Zookeeper, zu erreichen. Die Zookeeper-Probleme können aufgrund von temporären Datenträgerproblemen auftreten. Beheben Sie die Datenträgerprobleme, und überprüfen Sie, ob Apache Zookeeper läuft.

Die Protokolldatei von Apache Zookeeper zeigt aufgrund der hohen Datenträgerlatenz die folgende Fehlermeldung: `"fsync-ing the write ahead log in SyncThread:3 took 25115ms which will adversely affect operation latency"`.

Es wird empfohlen, dass Sie Apache Zookeeper einen dedizierten Datenträger anstelle einer Festplattenpartition zuweisen, da Apache Zookeeper eine hohe Konsistenz für den Client gewährleisten muss. Überprüfen Sie, ob Sie die empfohlene Anzahl von Festplatten für die Arbeitslastgröße zugewiesen haben. Außerdem müssen Sie das Zookeeper-Datenverzeichnis auf den dedizierten Datenträger von Apache Zookeeper verweisen lassen.

Einige der Quorum-Mitglieder der Apache Zookeeper-Gruppe sind nicht erreichbar, und in der Protokolldatei wird sinngemäß die folgende Warnmeldung angezeigt: `"[QuorumPeer[myid=3]/0:0:0:0:0:0:2181:QuorumCnxManager@383]`

- Cannot open channel to 2 at election address 10.65.144.18:3888 java.net.ConnectException: Connection refused at java.net.PlainSocketImpl.socketConnect(Native Method)"

Überprüfen Sie, ob die Zookeeper-Hosts über das Netzwerk erreichbar sind. Es ist wichtig, dass Zookeeper-Quorum-Mitglieder über genügend Arbeitsspeicher verfügen. Stellen Sie sicher, dass die Knoten die empfohlenen Speicheranforderungen erfüllen. Stellen Sie sicher, dass nur Prozesse im Zusammenhang mit dem Katalogdienst auf demselben Host ausgeführt werden.

Mehrere Quorum-Mitglieder von Apache Zookeeper zeigen am Client sinngemäß die folgenden Meldungen über beendete Sitzungen an: "Caught end of stream exception EndOfStreamException: Unable to read additional data from client sessionid 0x0, likely client has closed socket, Processed session termination for sessionid".

Überwachen Sie die Heap-Speichernutzung für Zookeeper-Quorum-Mitglieder. Sie können erwägen, den Heap-Speicher für Zookeeper zu erhöhen und den gesamten Cluster erneut zu starten.

Der Aufnahmedienst kann nicht gestartet werden, und die Protokolldatei zeigt sinngemäß die folgende Fehlermeldung an: "Initial job has not accepted any resources; check your cluster UI to ensure that workers are registered and have sufficient memory".

Dieser Fehler weist auf unzureichende Speicherkapazität oder CPU-Kerne im gesamten Cluster hin. Überprüfen Sie, ob der Cluster über ausreichende Ressourcen zum Starten neuer Anwendungen verfügt.

Der Katalogdienst kann nicht gestartet werden, nachdem Sie die benutzerdefinierte Eigenschaft `LdmCustomOptions.loadType` in Informatica Administrator geändert haben, und die Protokolldatei enthält folgenden Fehler: "Caused by: org.springframework.beans.factory.BeanCreationException: Error creating bean with name 'hbaseGraphFactory': Invocation of init method failed; nested exception is com.thinkaurelius.titan.core.TitanConfigurationException: Local settings present for one or more globally managed options: [cluster.max-partitions]. These options are controlled through the ManagementSystem interface; local settings have no effect".

Sie müssen alle Daten sichern, bevor Sie die benutzerdefinierte Ladetyp-Eigenschaft ändern, die Einstellung für den Ladetyp ändern, den Cluster erneut starten und dann die gesicherten Daten laden.

Der Katalogdienst oder der Aufnahmedienst schlägt fehl, da einige HBase-Datenbanktabellen nicht verfügbar sind, und in den Protokolldateien wird der folgende Fehler ausgewiesen: "Caused by: com.thinkaurelius.titan.diskstorage.TemporaryBackendException: Temporary failure in storage backend at com.thinkaurelius.titan.diskstorage.hbase.HBaseStoreManager.ensureTableExists (HBaseStoreManager.java:754) Caused by: org.apache.hadoop.hbase.TableNotFoundException: Idmns:titan_db".

Dieser Fehler tritt aufgrund einer unsachgemäßen Bereinigung von Daten im Zusammenhang mit dem Katalogdienst oder dem Aufnahmedienst auf. Wenn Sie den Ladetyp mit der benutzerdefinierten Eigenschaft `LdmCustomOptions.loadType` in Informatica Administrator geändert haben, müssen Sie überprüfen, ob Sie alle dienstbezogenen Daten gesichert, die Daten vollständig entfernt und anschließend neu geladen haben.

Der Katalogdienst oder der Aufnahmedienst schlägt fehl, da einige HBase-Datenbanktabellen vorhanden sind, und in den Protokolldateien wird der folgende Fehler ausgewiesen: "Caused by: org.apache.hadoop.hbase.ipc.RemoteWithExtrasException (org.apache.hadoop.hbase.TableExistsException): org.apache.hadoop.hbase.TableExistsException: Idmns:exDocStore at org.apache.hadoop.hbase.master.procedure.CreateTableProcedure.prepareCreate".

Dieser Fehler tritt aufgrund einer unsachgemäßen Bereinigung von Daten im Zusammenhang mit dem Katalogdienst oder dem Aufnahmedienst auf. Wenn Sie den Ladetyp mit der benutzerdefinierten Eigenschaft `LdmCustomOptions.loadType` in Informatica Administrator geändert haben, müssen Sie überprüfen, ob Sie alle dienstbezogenen Daten gesichert, die Daten vollständig entfernt und anschließend neu geladen haben.

Der Katalogdienst oder der Aufnahmedienst schlägt aufgrund einiger deaktivierter HBase-Datenbanktabellen fehl, und in den Protokolldateien wird der folgende Fehler ausgewiesen: "Caused by: org.apache.hadoop.hbase.TableNotEnabledException: Idmns:DataDomain_stage is disabled at

***org.apache.hadoop.hbase.client.HConnectionManager
\$HConnectionImplementation.relocateRegion(HConnectionManager.java:1139)***".

Dieser Fehler tritt aufgrund einer unsachgemäßen Bereinigung von Daten im Zusammenhang mit dem Katalogdienst oder dem Aufnahmedienst auf. Wenn Sie den Ladetyp mit der benutzerdefinierten Eigenschaft `LdmCustomOptions.loadType` in Informatica Administrator geändert haben, müssen Sie überprüfen, ob Sie alle dienstbezogenen Daten gesichert, die Daten vollständig entfernt und anschließend neu geladen haben.

Der Katalogdienst oder der Aufnahmedienst schlägt fehl und in den Protokolldateien wird einer der folgende Fehler ausgewiesen bzw. die HBase-Protokolldatei enthält die Fehlermeldung: "Caused by: com.thinkaurelius.titan.diskstorage.TemporaryBackendException: Temporary failure in storage backend Caused by: org.apache.hadoop.hbase.client.RetriesExhaustedException: Failed after attempts=4, exceptions: failed on local exception: java.io.IOException: Connection reset by peer This server is in the failed servers list". Die Protokolldatei des Aufnahmediensts enthält möglicherweise den Fehler: "Caused by: org.apache.spark.SparkException: Job aborted due to stage failure: Task 0 in stage 9468.0 failed 4 times, most recent failure: Lost task 0.3 in stage 9468.0 (TID 12018): org.apache.hadoop.hbase.client.RetriesExhaustedException: Failed after attempts=4, exceptions: This server is in the failed servers list".

Der Fehler kann auftreten, wenn der HBase-Server aufgrund von Faktoren wie Netzwerkpartitionierung, arbeitslastbedingter Nichtverfügbarkeit des HBase-Regionservers oder dessen interner Wartungstätigkeiten wie Datensplitting und -komprimierung nicht erreichbar ist. Sie können versuchen, den Katalogdienst mit erhöhtem Arbeitsspeicher für HBase neu zu starten.

HBase-Server können fehlschlagen, wenn Apache Zookeeper oder HDFS nicht erreichbar ist. Der Katalogdienst versucht, HBase-Instanzen bis zur konfigurierten Anzahl von Versuchen automatisch zu starten, sofern es sich nicht um einen schwerwiegenden Fehler handelt. In solchen Fällen müssen Sie den Katalogdienst möglicherweise manuell neu starten.

Die Apache YARN-Anwendung wird zeitweilig heruntergefahren, und Clusterknoten werden nicht zum Übermitteln von Clusteranwendungen verwendet. Die Protokolldatei des YARN-Ressourcenmanagers enthält die folgende Fehlermeldung: "Node irl66dsg04.xxx.com:8041 reported UNHEALTHY with details: 1/1 log-dirs are bad: /var/log/hadoop-yarn/container, Node Transitioned from RUNNING to UNHEALTHY, Container Transitioned from RUNNING to KILLED, Removed node irl66dsg04.xxx.com:8041 cluster capacity: <memory:184320, vCores:96>".

Überprüfen Sie den Speicherplatz für `/ partition` auf der Festplatte mithilfe von Befehlen wie `df`. Apache YARN betrachtet einen Knoten als fehlerhaft und beendet die Knotenanwendungen, wenn die Speicherplatznutzung mehr als 80 % beträgt. Löschen Sie unnötige Daten aus Partition '/'. Wenn Sie über mehrere Festplatten verfügen, lassen Sie `/ partition` auf eine unbestrittene Festplatte verweisen.

Der HBase-Regionsserver wird heruntergefahren und in der Protokolldatei wird sinngemäß folgende Fehlermeldung ausgewiesen: "Sleeper: Slept 15559ms instead of 3000ms, this is likely due to a long garbage collecting pause and it's usually bad. HeapMemoryManager: heapOccupancyPercent 0,9935025 liegt über Warnungsschwelle für Heap-Belegung (0,95). JvmPauseMonitor: Pause in JVM oder Hostcomputer (z. B. GC) erkannt: Pause von ca. 3733 ms. GC-Pool 'ParNew' hatte Erfassung(en): Anzahl=1 Dauer=4075 ms".

Dieser Fehler tritt aufgrund von Arbeitsspeicherproblemen bei HBase auf. Überprüfen Sie mithilfe der benutzerdefinierten Eigenschaft `LdmCustomOptions.loadType` in Informatica Administrator, ob Sie den richtigen Arbeitslast- oder Datensatztyp für die Arbeitslast von Enterprise Data Catalog konfiguriert haben. In einigen Fällen müssen Sie möglicherweise die Heap-Einstellungen für HBase mithilfe von Informatica Administrator manuell erhöhen und dann den Katalogdienst neu starten.

Der Aufnahmedienst schlägt mit Arbeitsspeicherproblemen fehl, und die Protokolldatei des Aufnahmediensts enthält in etwa die folgende Fehlermeldung: "TaskSetManager: Lost task 1.0 in stage 18.0 (TID 39, INVRLX65CMD03.informatica.com): org.apache.spark.util.TaskCompletionListenerException: GC overhead limit exceeded

at org.apache.spark.TaskContextImpl.markTaskCompleted(TaskContextImpl.scala:83) at org.apache.spark.scheduler.Task.run(Task.scala:72)".

Dieser Fehler tritt aufgrund eines reduzierten Arbeitsspeichers für HBase auf. Überprüfen Sie mithilfe der benutzerdefinierten Eigenschaft `LdmCustomOptions.loadType` in Informatica Administrator, ob Sie den richtigen Arbeitslast- oder Datensatztyp für die Arbeitslast von Enterprise Data Catalog konfiguriert haben. In einigen Fällen müssen Sie möglicherweise die Heap-Einstellungen für HBase mithilfe von Informatica Administrator manuell erhöhen und dann den Katalogdienst neu starten.

Der Aufnahmedienst schlägt fehl und in der Protokolldatei wird der folgende Fehler ausgewiesen: "ERROR executor.CoarseGrainedExecutorBackend: RECEIVED SIGNAL 15: SIGTERM spark.TaskContextImpl: Error in TaskCompletionListener java.io.IOException: Filesystem closed at org.apache.hadoop.hdfs.DFSCClient.checkOpen(DFSCClient.java:761)".

Dieser Fehler weist darauf hin, dass das Hadoop-Dateisystem nicht erreichbar ist. Überprüfen Sie anhand der Apache Ambari-Benutzeroberfläche, ob HDFS ausgeführt wird.

Ein HDFS-Datenknoten schlägt fehl, und es wird in etwa die folgende Fehlermeldung angezeigt: "BlockStateChange: BLOCK NameSystem.addToCorruptReplicasMap: blk_1073876841 added as corrupt on 10.65.145.216:50010 by irlcmg07.informatica.com/10.65.145.216 because reported RWR replica with genstamp 136273 does not match COMPLETE block's genstamp in block map 138353".

Dieser Fehler tritt normalerweise in einer Bereitstellung mit einem Knoten auf, da die Daten nicht repliziert werden. Das Problem kann aufgrund von Datenbeschädigungen in einigen HDFS-Datenblöcken auftreten. Die Datenbeschädigung kann aufgrund eines beschädigten Datenvolumens auftreten oder aufgrund eines Datenträgers, dessen Speicher voll ist.

Wenn Sie mehr als ein Datenträgerverzeichnis für HDFS konfiguriert haben, können Sie versuchen, den Wert 0 für `dfs.datanode.failed.volumes.tolerated` zu ändern. Der Wert 0 führt zum Herunterfahren des Datenknotens, wenn mindestens ein Datenträger-Volumen beschädigt ist.

Wo finde ich alle Protokolldateien zum Informatica-Cluster-Dienst und wie kann ich mithilfe der Protokolldateien Fehler beheben?

Die Details zu den Problemen im Zusammenhang mit dem Informatica-Cluster-Dienst können Sie anhand der folgenden Schritte ermitteln:

1. Öffnen und überprüfen Sie die Protokolldatei zum Informatica-Cluster-Dienst an folgendem Speicherort: `<Installationsverzeichnis>/logs/<Name des Informatica-Cluster-Dienstknotens>/services/InfahadoopService/<Name des Informatica-Cluster-Diensts>`.
2. Öffnen und überprüfen Sie die Protokolldatei für den Apache Ambari-Server auf dem Ambari-Serverhost an folgendem Speicherort: `/var/log/ambari-server`.
3. Öffnen und überprüfen Sie die Protokolldatei für den Apache Ambari-Agent auf dem Ambari-Agent-Host an folgendem Speicherort: `/var/log/ambari-agent`.
4. Falls Sie das Problem mit diesen Schritten nicht beheben können, gehen Sie wie folgt vor:
 - a. Starten Sie die Apache Ambari-Anwendung mit der URL `http://<Ambari-Serverhost>:8080/`.
 - b. Klicken Sie oben in der Anwendung auf **ops**, um die fehlgeschlagenen Anfragen zu überprüfen:



- c. Notieren Sie den Namen des Hosts, auf dem die Anfrage fehlgeschlagen ist, und die Hadoop-Komponente, die sich auf die fehlgeschlagene Anfrage bezieht.
- d. Melden Sie sich bei dem Host an, bei dem die Anfrage fehlgeschlagen ist.

- e. Überprüfen Sie die Protokolldatei für die spezifische Hadoop-Komponente, die sich auf die fehlerhafte Anfrage bezieht, an den folgenden Speicherorten:

Name der Komponente	Speicherort der Protokolldatei
NameNode	/var/log/hadoop/hdfs oder /var/log/hadoop-hdfs
SecondaryNameNode	/var/log/hadoop/hdfs oder /var/log/hadoop-hdfs
JournalNode	/var/log/hadoop/hdfs oder /var/log/hadoop-hdfs
ZKFC	/var/log/hadoop/hdfs oder /var/log/hadoop-hdfs
DataNode	/var/log/hadoop/hdfs oder /var/log/hadoop-hdfs
HistoryServer	/var/log/hadoop/mapreduce oder /var/log/hadoop-mapreduce
MetricsCollector	/var/log/ambari-metrics-collector
MetricsMonitor	/var/log/ambari-metrics-monitor
AppTimelineServer	/var/log/hadoop-yarn oder /var/log/hadoop/yarn
ResourceManager	/var/log/hadoop-yarn oder /var/log/hadoop/yarn
NodeManager	/var/log/hadoop-yarn oder /var/log/hadoop/yarn
ZookeeperServer	/var/log/zookeeper

Hinweis: Wenn einige Hadoop-Dienste ausgeführt werden, die beim vorherigen Herunterfahren des Informatica-Clusterdienstes nicht beendet wurden, wird in der Protokolldatei möglicherweise der Text `java.net.BindException: Address already in use` angezeigt. Sie müssen diese Prozesse dann auf den in der Ausnahme genannten Ports herunterfahren.

Wo finde ich alle Protokolldateien für Apache YARN-Anwendungen, wie Solr, HBase und den Aufnahmediens?

Mit dem folgenden Verfahren können Sie die Protokolldateien anzeigen:

1. Melden Sie sich bei der Apache Ambari-Benutzeroberfläche an und klicken Sie auf die Registerkarte **Dienst** oben auf der Seite, um die folgende Seite zu öffnen:



2. Klicken Sie auf **Quick Links > ResourceManager UI**, um die folgende Seite mit einer Liste aller Anwendungen zu öffnen:

Sie können die verschiedenen Anwendungen anzeigen, die von dem betreffenden Katalogdienst auf Apache YARN gestartet wurden. In der Spalte Status wird der aktuelle Status der Anwendungen angegeben.

3. Klicken Sie auf den Link unter der Spalte **ID**, um die folgende Seite zu öffnen:

4. Um die Protokolldatei anzuzeigen, klicken Sie auf **logs**.

Der Aufnahmedienst schlägt beim Ausführen von Jobs in einer Sequenz mit der folgenden Fehlermeldung fehl:

"java.io.IOException: Connection reset by peer."

Dieses Problem tritt aufgrund von begrenzten Zookeeper-Clientverbindungen auf, die für Enterprise Data Catalog zulässig sind. Sie können den Zookeeper-Client Verbindungswert in 0 ändern, was auf unbegrenzte Verbindungen hinweist.

Die Apache Ambari-Installation schlägt fehl, wenn das Yum-Repository für den Download von Apache Ambari aus einem benutzerdefinierten Verzeichnis konfiguriert ist.

Dieses Problem tritt auf, wenn Sie ein benutzerdefiniertes Repository zum Herunterladen von Apache Ambari konfiguriert haben. Um dieses Problem zu beheben, müssen Sie die yum.conf- und .repo-Dateien unter dem Verzeichnis `/etc/yum.repos.d/` aktualisieren, um auf den Speicherort zu verweisen, an dem sich die Apache Ambari-Installationsdateien befinden.

Eine PowerCenter-Ressource kann keine Verbindung mit der SSL-aktivierten Informatica-Domäne herstellen.

Dieses Problem tritt normalerweise auf, wenn Sie das Sicherheitszertifikat nicht in den lokalen Truststore importieren. Sie können das Sicherheitszertifikat in den lokalen Truststore importieren, um dieses Problem zu beheben.

Der Katalogdienst kann nicht aktiviert werden

Dieses Problem kann auftreten, wenn Sie die Option Benachrichtigungen per E-Mail erhalten für den Katalogdienst aktiviert haben und sich der E-Mail-Dienst zugleich im deaktivierten Zustand befindet. Sie müssen den E-Mail-Dienst aktivieren.

Weitere Informationen zum Aktivieren des E-Mail-Diensts finden Sie im Handbuch *Administrator-Referenz für Enterprise Data Catalog*.

Fehlerbehebung bei der Bereitstellung auf einem vorhandenen Cluster

Die Aufnahme von Metadaten in den Katalog wird nicht korrekt durchgeführt.

Überprüfen Sie, ob die Skriptdateien im Installationsprogramm für Enterprise Data Catalog, die die Solr- und Ingestion-Jobs starten, auf den Zielhost des vorhandenen Clusters kopiert werden.

Kann ich Kerberos-Sicherheit implementieren, wenn ich Enterprise Data Catalog auf einem vorhandenen Cluster installiere?

Ja. Enterprise Data Catalog unterstützt die Kerberos-Netzwerkauthentifizierung auf einem vorhandenen Cluster.

Ich sehe, dass der Katalogdienst unerwartet beendet wurde, und die Fehlermeldung in der Protokolldatei lautet wie folgt: "GSSEException: No valid credentials provided (Mechanism level: Server not found in Kerberos database)". Wie kann ich das Problem beheben?

Überprüfen Sie, ob alle Clusterknoten in der Domäne `/etc/hosts` vollqualifizierte Hostnamen aufweisen, und korrigieren Sie die fehlerhaften Hostnamen.

Ich habe eine Cloudera Version 4-Clusterumgebung und kann Enterprise Data Catalog nicht auf dem Cluster installieren.

Enterprise Data Catalog unterstützt Cloudera Version 5.8 oder höher oder Hortonworks Version 2.5 für die Bereitstellung auf vorhandenen Hadoop-Clustern. Aktualisieren Sie die Cloudera-Version auf 5.8 oder höher.

Ich habe einige Hosts mit CDH Manager hinzugefügt, die Hochverfügbarkeitsdienste für den Cluster enthalten. Allerdings scheinen die Knoten nicht aktiviert zu sein.

Wenn Sie einem vorhandenen Cluster Knoten hinzugefügt haben, überprüfen Sie, ob Sie diese der Hadoop-Knotenliste in Informatica Administrator hinzugefügt haben. Starten Sie den Katalogdienst dann neu.

Es treten Probleme mit der Verfügbarkeit des Kerberos-Schlüsselverteilungscenters (KDC) auf, und es wird sinngemäß die folgende Meldung angezeigt: "(java.security.PrivilegedActionException: javax.security.sasl.SaslException: GSS-Initiierung fehlgeschlagen [Verursacht durch GSSEException: Keine gültigen Anmeldedaten angegeben (Mechanismusstufe: Zurücksetzen der Verbindung)]) bei der Auswertung des vom Zookeeper-Quorum-Mitglied empfangenen SASL-Tokens. Zookeeper-Client wird zu AUTH_FAILED-Zustand wechseln." Wie kann ich diese Probleme beheben?

Ein Kerberos-aktivierter Cluster erfordert ein hochverfügbares KDC. Stellen Sie sicher, dass die hohe Verfügbarkeit für KDC aktiviert ist.

Der Aufnahmedienst wird aufgrund einer Arbeitsspeicherüberlastung durch Apache Yarn beendet und es wird sinngemäß die folgende Fehlermeldung angezeigt: "Container-Kill durch YARN, Grund: Speicherlimit überschritten. 10,0 GB von 10 GB physischem Speicher verwendet. Ziehen Sie die Verstärkung von spark.yarn.executor.memoryOverhead in Betracht." Wie kann ich diesen Fehler beheben?

Der Fehler tritt aufgrund einer Apache YARN-Speicherprüfung auf. Es wird empfohlen, die folgenden beiden Eigenschaften auf FALSE festzulegen:

- `yarn.nodemanager.pmem-check-enabled`
- `yarn.nodemanager.vmem-check-enabled`

Nachdem Sie eine Domäne und einen Katalogdienst abrupt heruntergefahren haben, sehen Sie, dass die YARN-Anwendung weiter ausgeführt wird.

Wenn Sie die Domäne nicht ordnungsgemäß herunterfahren, werden die YARN-Anwendungen für HBase, Solr und Spark möglicherweise weiter ausgeführt. Sie müssen diese YARN-Anwendungen manuell herunterfahren, bevor Sie die Domäne und die Anwendungsdienste erneut starten können.

Fehlerbehebung bei der Bereitstellung auf einem eingebetteten Cluster

Ich sehe Ausfälle bei der hohen Verfügbarkeit im eingebetteten Cluster.

Hohe Verfügbarkeit ist möglich, wenn Sie Enterprise Data Catalog das erste Mal auf mehr als zwei Knoten installieren. Stellen Sie sicher, dass die Anzahl der Clusterknoten für Enterprise Data Catalog mindestens drei beträgt. Wenn Sie während der Installation einen einzelnen Knoten für Enterprise Data Catalog verwenden oder nach der Installation nachträglich weitere einzelne Knoten hinzufügen, können Sie keine hohe Verfügbarkeit implementieren. Wenn einer der hochverfügbaren Hosts heruntergefahren wird oder nicht erreichbar ist, wird Enterprise Data Catalog möglicherweise weiterhin ausgeführt, aber der Cluster ist eventuell nicht mehr hochverfügbar. Den Knoten, der heruntergefahren wurde oder nicht erreichbar ist, müssen Sie dann erneut starten, um den Cluster hochverfügbar zu machen.

Wenn Oracle und der Informatica-Cluster-Dienst auf demselben Computer ausgeführt werden, kann der Informatica-Cluster-Dienst nicht gestartet werden.

Überprüfen Sie, ob Oracle auf Port 8080 ausgeführt wird. Port 8080 ist für Apache Ambari reserviert. Stellen Sie sicher, dass Oracle auf einem anderen Port ausgeführt wird, wenn Sie Oracle und den Informatica-Cluster-Dienst auf demselben Computer ausführen.

Das Apache Ambari-Tool funktioniert nicht, nachdem ich Enterprise Data Catalog auf einem eingebetteten Hadoop-Cluster installiert habe.

- Bei dem Ambari-Hostnamen, den Sie während der Installation angeben, wird die Groß-/Kleinschreibung beachtet. Überprüfen Sie, ob der Hostname den Anforderungen entspricht. Informatica empfiehlt die Verwendung von Kleinbuchstaben für Hostnamen. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob der Hostname korrekt eingerichtet wurde:

```
#hostname -f
```

Der Befehl gibt den vollqualifizierten Domännennamen zurück, den Sie konfiguriert haben.

- Wenn Sie Enterprise Data Catalog unter Red Hat Enterprise Linux (RHEL) Version 6.5 oder höher installiert haben, überprüfen Sie, ob alle Repositories des Basisbetriebssystems verfügbar sind. Das Installationsprogramm für Enterprise Data Catalog bezieht viele Pakete von den Repositories des Basisbetriebssystems. Beispielsweise müssen die Hosts auf das Red Hat Enterprise Linux-Repository `rhel-6-server-optional-rpms` zugreifen können, damit die Installation erfolgreich abgeschlossen werden kann. Wenn Sie nicht über den vollständigen Satz von Repositories des Basis-Betriebssystems verfügen, könnten bei der Installation Probleme auftreten.
- Überprüfen Sie die installierte Python-Version. Enterprise Data Catalog unterstützt die Python-Version 2.6.8-0.15.1 oder früher. Python-Version 2.7.9 oder höher wird nicht unterstützt.
- Überprüfen Sie vor der Installation von Enterprise Data Catalog, ob die Ports 8080, 8440 und 8411 frei sind. Apache Ambari verwendet diese Ports während der Installation.

Der Informatica-Cluster-Dienst reagiert nicht.

Stellen Sie sicher, dass Sie keine 777-Berechtigungen für das Verzeichnis `/var` haben. Sie müssen jedoch über die Schreibberechtigung für das Verzeichnis `/var` verfügen.

Der Ambari-Server auf der Standard-PostgreSQL-Datenbank wird heruntergefahren oder Sie möchten den Ambari-Server von einem Host auf einen anderen verschieben.

Sie können die folgenden Schritte ausführen, um den Ambari-Server auf einem neuen Host einzurichten:

1. Deaktivieren Sie den Informatica-Cluster-Dienst mit Informatica Administrator.
2. Starten Sie die PostgreSQL-Instanz auf dem Ambari Serverhost neu. Sichern Sie die PostgreSQL-Datenbanken `ambarirca` und `ambari`.

Hinweis: Weitere Informationen zum Sichern von PostgreSQL-Datenbanken finden Sie im Abschnitt zum *Verschieben des Ambari-Servers* in der Hortonworks-Dokumentation.

3. Aktualisieren Sie den Wert des Ambari-Serverhostnamens für den Informatica-Cluster-Dienst auf den neuen Ambari-Serverhostnamen. Um den Hostnamen in Informatica Administrator zu aktualisieren, können Sie den Katalogdienst auswählen und dann im Feld **Informatica-Cluster-Dienst** unter **Optionen für Hadoop-Cluster** den Hostnamen eingeben.
4. Aktivieren Sie den Informatica-Cluster-Dienst. Mit dieser Aktion wird Ambari Server im neuen Hadoop-Gateway-Host installiert, den Sie angegeben haben, und der Ambari-Agent wird mit dem neuen Ambari-Serverhost aktualisiert.
5. Deaktivieren Sie den Informatica-Cluster-Dienst.
6. Legen Sie die beiden Datenbanken `ambarirca` und `ambari` aus der PostgreSQL-Instanz auf dem neuen Hadoop-Gateway-Host ab.
7. Stellen Sie die Datenbanken `ambarirca` und `ambari` aus der Sicherung des vorherigen Hadoop-Gateway-Hosts wieder her.

Hinweis: Weitere Informationen zum Wiederherstellen von PostgreSQL-Datenbanken aus einer Sicherung finden Sie im Abschnitt zum *Verschieben des Ambari-Servers* in der Hortonworks-Dokumentation.

8. Aktivieren Sie den Informatica-Cluster-Dienst.

Der Apache Ambari-Server startet nicht, und in der Protokolldatei des Ambari-Servers wird die folgende Fehlermeldung ausgewiesen: `About to start PostgreSQLERROR: Exiting with exit code 1.REASON: Unable to start PostgreSQL server. Exiting`

Fügen Sie `127.0.0.1 localhost localhost.localdomain` der Datei `/etc/hosts` hinzu.

Ich sehe, dass der Cluster nicht hochverfügbar ist.

Stellen Sie sicher, dass alle Knoten, auf denen Komponenten für hohe Verfügbarkeit gehostet werden, ausgeführt werden. Wenn einer der Knoten, auf denen Komponenten für hohe Verfügbarkeit gehostet werden, heruntergefahren wird, ist der Cluster nicht mehr hochverfügbar. Sie müssen den Knoten, der heruntergefahren wurde, erneut starten.

Wenn einer der Slave-Knoten im Cluster nicht erreichbar ist, kann ich den Informatica-Cluster-Dienst nicht aktivieren.

Wenn einer der Slave-Knoten aufgrund eines unerwarteten Fehlers nicht erreichbar ist, müssen Sie entweder den Host aus der Liste der Apache-Ambari-Agenten in Informatica Administrator entfernen oder den Slave-Knoten erneut einrichten, bevor Sie den Informatica-Cluster-Dienst neu starten.

Ich habe einen vorhandenen Katalogdienst gelöscht und einen neuen aktiviert. Aber jetzt kann ich nicht auf die Daten im Katalog zugreifen und ich kann diese nicht verwenden.

Wenn Sie einen neuen Katalogdienst auf die vorhandenen Daten im Katalog verweisen lassen möchten, müssen Sie für den neuen Katalogdienst denselben Dienst-Clusternamen angeben, den Sie für den gelöschten Katalogdienst verwendet haben. Den Dienst-Clusternamen geben Sie in Informatica Administrator unter dem Abschnitt **Hadoop-Cluster-Optionen** auf der Registerkarte **Eigenschaften** an.

Nachdem ich ein paar Knoten zu einem vorhandenen eingebetteten Cluster hinzugefügt habe, kann das Apache Ambari Metrics-System nicht gestartet werden.

Dieser Fehler kann auftreten, wenn einige Computer, insbesondere virtuelle Maschinen, nicht über die erforderlichen Systempakete verfügen. Stellen Sie sicher, dass die neuen Hosts, die Sie hinzufügen, die Voraussetzungen für die Bereitstellung von Enterprise Data Catalog auf einem eingebetteten Cluster erfüllen. Lesen Sie die Abschnitte *Voraussetzungen* und *Vorbereiten der eingebetteten Hadoop-Clusterumgebung* im Kapitel *Bereitstellungsmethoden* dieses Handbuchs.

Der Apache Ambari-Agent schlägt mit einer der folgenden Fehlermeldungen in der Ambari-Agent-Protokolldatei fehl: `NetUtil.py:67 - SSLError: Failed to connect. Please check openssl library versions` oder `INFO`

```
2014-04-02 04:25:22,669 NetUtil.py:55 - Failed to connect to https://{ambari-server}:8440/
cert/ca due to [Errno 1] _ssl.c:492: error:100AE081:elliptic curve
routines:EC_GROUP_new_by_curve_name:unknown group
```

Eine der Voraussetzungen für die korrekte Funktion des Apache Ambari-Agenten ist OpenSSL Version 1.0.1 oder höher. Sie können wie folgt vorgehen:

1. Überprüfen Sie mit dem folgenden Befehl, welche Version der OpenSSL-Bibliothek auf Ihren Hosts installiert ist:

```
rpm -qa | grep openssl
```

2. Wenn die Ausgabe des vorherigen Befehls openssl-1.0.1e-15.x86_64 (1.0.1 build 15) lautet, müssen Sie die OpenSSL-Bibliothek aktualisieren. Führen Sie zum Aktualisieren der OpenSSL-Bibliothek den folgenden Befehl aus:

```
yum upgrade openssl
```

3. Überprüfen Sie mit dem Befehl rpm, ob die neuere Version von OpenSSL installiert ist.
4. Starten Sie Apache Ambari-Agenten neu und klicken Sie in der Benutzeroberfläche des Assistenten auf **Erneut versuchen** > **Fehlgeschlagen**.

Wenn Sie Enterprise Data Catalog auf einem eingebetteten Cluster installieren, erstellt das Installationsprogramm aufgrund von Berechtigungsproblemen keinen Informatica-Cluster-Dienst.

Wenn der Root-Benutzer nicht über die erforderliche Berechtigung zum Hinzufügen von Benutzern unter dem Benutzer-Basisverzeichnis verfügt, wird in der Aufgabenprotokolldatei die folgende Fehlermeldung angezeigt:

```
Execution of 'useradd -m -G hadoop -g hadoop mapred' returned 12. useradd: cannot
create directory /home/mapred
```

Sie können dann das Benutzer-Basisverzeichnis für die virtuelle Maschine in das Verzeichnis ändern, für das der Root-Benutzer über die erforderliche Berechtigung verfügt, um ein Verzeichnis darin zu erstellen:

```
sudo vim /etc/default/useradd
```

Ändern Sie das Basisverzeichnis in HOME=/export/home.

Der Apache Ambari Application Timeline Server schlägt mit folgendem Fehler fehl: ps -p 'hadoop-yarn/yarn/yarn-yarn-timelineserver.pid' failed: <https://issues.apache.org/jira/browse/AMBARI-4825>

Dieses Problem kann auftreten, wenn mehr als ein Terminal aktiv ist. Verwenden Sie die Befehle w, whoami und kill, um alle Terminals mit Ausnahme des relevanten zu überprüfen und zu beenden. Anschließend können Sie den YARN-Cluster neu starten.

Die Apache Ambari-Serverinstallation schlägt auf einigen Hostcomputern fehl, und in den Protokolldateien für Ambari Server wird der folgende Fehler ausgewiesen: Ambari-server status Traceback (most recent call last)
File "/usr/sbin/ambari-server.py", line 26, in <module> from ambari_commons.exceptions import
FatalException, NonFatalException ImportError: No module named ambari_commons.exceptions.

Dieses Problem tritt auf, wenn Sie versuchen, den Ambari-Server auf einem einzelnen Host zu installieren, der über einen Ambari-Agent aus einer früheren Installation verfügt. Der Link /usr/lib/python2.6/site-packages/ambari_commons muss auf /usr/lib/ambari-server/lib/ambari_commons anstelle von /usr/lib/ambari-agent/lib/ambari_commons verweisen.

Wenn Sie dem Cluster nur zwei Knoten hinzufügen, schlägt das Cluster-Setup mit dem Fehlercode 00030 fehl: Cannot create a cluster with 2 hosts. Minimum 3 hosts are required for creating the High Availability cluster.

Sie können keinen Cluster mit nur zwei Knoten erstellen. Sie müssen mindestens drei Knoten für einen hochverfügbaren Cluster und einen Host für einen nicht hochverfügbaren Cluster bereitstellen. Sie können einem bereits eingerichteten Cluster mit einem Knoten weitere Knoten hinzufügen. Sie können den Cluster jedoch nicht als hochverfügbaren Cluster konfigurieren.

Wenn Sie einen Cluster erstellen, schlägt die Überprüfung der Mindestsystemkonfiguration mit einem der folgenden Fehlercodes fehl: 00026, 00027 oder 00028.

Wenn Sie einen Cluster mit einem einzelnen Knoten haben, muss der Hostcomputer die Mindestkonfigurationskriterien für Masterknoten erfüllen. Wenn Sie über einen Cluster mit hoher Verfügbarkeit verfügen, müssen mindestens drei der Hostcomputer die Mindestkonfigurationskriterien für Masterknoten erfüllen. Die verbleibenden Hostcomputer müssen die Mindestkonfigurationskriterien für Slave-Knoten erfüllen.

Sie können einen Knoten aus dem Cluster nicht löschen, und es wird einer der folgenden Fehlercodes in der Protokolldatei angezeigt: 00035 oder 00036.

Fehlercode 00035 zeigt an, dass beim Löschen des Knotens die Anzahl der Live Datenknoten im Cluster auf weniger als drei reduziert wird. Die Mindestanzahl der im Cluster erforderlichen Live-Knoten beträgt drei. Fehlercode 0036 zeigt an, dass ein Versuch unternommen wurde, einen Knoten zu entfernen, der die Master-Dienste hostet. Ein Knoten, der die Master-Dienste hostet, kann nicht entfernt werden.

HDFS-Datenknoten zeigt häufig Fehlermeldungen über unbekannte Vorgänge an. In den Datenknoten-Protokolldateien werden die folgenden Fehler ausgewiesen:

```
DataXceiver error processing unknown operation src: /
127.0.0.1:33349 dst: /127.0.0.1:50010 java.io.EOFException at
java.io.DataInputStream.readShort(DataInputStream.java:315) at
org.apache.hadoop.hdfs.protocol.datatransfer.Receiver.readOp(Receiver.java:58)
```

Apache Ambari öffnet jede Minute eine Socket-Verbindung zum HDFS-Datenknoten, um diesen zu überwachen. Sie können diese Fehler ignorieren, da sie sich nicht auf die Clustervorgänge auswirken.

Ich habe die Informatica-Domäne, den Datenintegrationsdienst und den Content-Management-Dienst mit dem SSL-Protokoll gesichert. Wenn ich die Einstellungen des Katalogdiensts ändere, um den SSL-Modus zu aktivieren, kann der Dienst nicht gestartet werden. Wie kann ich das Problem beheben?

Führen Sie im LDM-Installationsprogramm die folgenden Schritte durch, nachdem Sie die Informatica-Domäne, den Datenintegrationsdienst und den Content-Management-Dienst konfiguriert haben, um diese mit dem SSL-Protokoll zu sichern.

1. Exportieren Sie das Zertifikat des Schlüsselspeichers für den Katalogdienst.
2. Importieren Sie das Schlüsselspeicherzertifikat in die Truststore-Datei von Informatica.
3. Legen Sie die Informatica-Truststore-Datei auf allen Hadoop-Knoten ab. Achten Sie darauf, dass Sie auf allen Hostcomputern die gleiche Verzeichnisstruktur für die Truststore-Datei verwenden.
4. Geben Sie in Informatica Administrator den allgemeinen Informatica Truststore-Dateispeicherort im Feld **Speicherort der Domänen-TrustStore-Datei** des Abschnitts **Erweiterte Optionen** für den Informatica-Cluster-Dienst ein.
5. Wählen Sie im Dialogfeld **Sicherheitseigenschaften bearbeiten** auf der Registerkarte **Prozesse** des Informatica-Cluster-Diensts die Option **TLS (Transport Layer Security) aktivieren** aus und geben Sie den Pfad zu der in Schritt 1 genannten Schlüsselspeicherdatei an.
6. Aktivieren Sie den Informatica-Cluster-Dienst. Wenn der Dienst bereits aktiviert ist, deaktivieren Sie den Dienst im Modus **Abgeschlossen** und aktivieren Sie ihn anschließend erneut.
7. Navigieren Sie zum Abschnitt Sicherheitseigenschaften des Katalogdiensts, und geben Sie den Pfad zu der in Schritt 1 genannten Schlüsselspeicherdatei an.
8. Aktivieren Sie den Katalogdienst.

Ich kann die Apache Ambari-Dateien im Installationsprogramm nicht finden, um den Informatica-Cluster-Dienst auf dem eingebetteten Cluster zu erstellen.

Wenn Sie den Informatica-Cluster-Dienst auf dem eingebetteten Cluster erstellen möchten, können Sie die ambaribinaries.tar.gz-Dateien in das Verzeichnis `Installer/services/InfahadoopService/Binaries` kopieren.

Fehlerbehebung bei Problemen mit Anwendungsdiensten

Der Katalogdienst kann nicht gestartet werden, wenn er auf NFS (Network File System) konfiguriert ist.

Sie müssen das lokale Dateisystem für den Katalogdienst mounten und konfigurieren.

ANHANG A

Starten und Beenden von Enterprise Data Catalog-Diensten

Dieser Anhang umfasst die folgenden Themen:

- [Starten und Beenden von Enterprise Data Catalog-Diensten unter Linux, 185](#)
- [Beenden der Enterprise Data Catalog-Dienste im Administrator Tool, 185](#)
- [Regeln und Richtlinien zum Starten oder Beenden von Enterprise Data Catalog, 186](#)

Starten und Beenden von Enterprise Data Catalog-Diensten unter Linux

Führen Sie unter Linux `infaservice.sh` aus, um den Enterprise Data Catalog-Daemon zu starten und zu beenden. `infaservice.sh` ist standardmäßig im folgenden Verzeichnis installiert:

```
<Enterprise Data Catalog 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, müssen Sie für die Umgebungsvariable `INFA_HOME` den Speicherort des Enterprise Data Catalog-Installationsverzeichnisses festlegen.

Beenden der Enterprise Data Catalog-Dienste im Administrator Tool

Wenn Sie einen Knoten mithilfe von Informatica Administrator ausschalten, wird der Katalogdienst auf diesem Knoten beendet.

Sie können die laufenden Vorgänge abrechnen oder zum Abschluss bringen, bevor der Dienst geschlossen wird. Wenn Sie einen Knoten ausschalten und die Repository-Dienst-Prozesse abrechnen, 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 Integrationsdienstvorgänge ausgeführt werden, werden die Arbeitsabläufe ebenfalls 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 Enterprise Data Catalog

Beachten Sie die folgenden Regeln und Richtlinien, wenn Sie Enterprise Data Catalog auf einem Knoten starten und beenden:

- 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 Enterprise Data Catalog, ob der vom Dienst auf dem Knoten verwendete Port verfügbar ist. Beispiel: Wenn Sie Enterprise Data Catalog an auf einem Knoten beenden, vergewissern Sie sich vor dem Neustart von Enterprise Data Catalog, dass der Port von keinem anderen Prozess auf dem Computer verwendet wird. Wenn der Port nicht verfügbar ist, wird Enterprise Data Catalog nicht gestartet.
- 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 Enterprise Data Catalog auf dem Primärknoten, bevor Sie den Sicherungsknoten starten. Andernfalls wird der Anwendungsdienst auf dem Sicherungsknoten, nicht auf dem Primärknoten ausgeführt.

ANHANG B

Entfernen des sudo-Zugriffs, nachdem ein eingebetteter Cluster erstellt wurde

- [Entfernen des sudo-Zugriffs, nachdem ein eingebetteter Cluster erstellt wurde, 187](#)

Entfernen des sudo-Zugriffs, nachdem ein eingebetteter Cluster erstellt wurde

Sie können einen eingebetteten Cluster verwalten, ohne sudo-Zugriff auf Benutzerkonten zu gewähren. Sie können die Sicherheitsbedrohungen in Ihrem Unternehmen reduzieren, indem Sie den sudo-Zugriff für Benutzerkonten einschränken. Wenn Sie einem Benutzerkonto sudo-Zugriff gewähren, können Sie mit dem Benutzerkonto Programme oder Anwendungen mit den Sicherheitsberechtigungen eines anderen Benutzers ausführen. Die Sicherheitsberechtigungen können die eines Benutzers sein, der über Root- oder Superuser-Berechtigungen verfügt.

Voraussetzungen

Die Voraussetzungen zum Erstellen eines eingebetteten Clusters ohne Sudo-Zugriff für Benutzerkonten sind folgende:

- Wenn Sie den eingebetteten Cluster zum ersten Mal erstellen, löschen Sie den Inhalt des Verzeichnisses `<Installationsverzeichnis>/tomcat/temp//temp/<Clusternamen>`.
- Wenn der eingebettete Cluster erstellt wurde und vorhanden ist, vergewissern Sie sich vor dem Starten des Informatica-Cluster-Diensts, dass der Ambari-Server und -Agent ausgeführt werden.

Ausführen eines eingebetteten Clusters ohne sudo-Zugriff

1. Erstellen Sie den Informatica-Cluster-Dienst mit einem Benutzerkonto, das nicht über Root-Berechtigungen verfügt.
Hinweis: Starten Sie nicht den Informatica-Cluster-Dienst.
2. Gewähren Sie sudo-Zugriff für das Benutzerkonto, mit dem Sie den Informatica-Cluster-Dienst erstellt haben.
3. Fügen Sie die benutzerdefinierte Eigenschaft `lcsCustomOptions.ihs.gateway.user.sudo.enabled` für den Informatica-Cluster-Dienst hinzu und legen Sie den Wert der Eigenschaft auf **false** fest.

4. Starten Sie Informatica Administrator und dann den Informatica-Cluster-Dienst, um den eingebetteten Cluster auf den gewünschten Knoten zu erstellen.
5. Nachdem Sie den eingebetteten Cluster auf allen Knoten erstellt haben, widerrufen Sie den sudo-Zugriff für das Benutzerkonto.

Häufig gestellte Fragen (FAQ)

Wird der eingebettete Cluster weiter ausgeführt, wenn ich den Cluster erstelle, den sudo-Zugriff für das Benutzerkonto widerrufe und den Informatica-Cluster-Dienst deaktiviere?

Der eingebettete Cluster wird im Hintergrund weiter ausgeführt.

Überwacht der Informatica-Cluster-Dienst den eingebetteten Cluster und startet die Dienste, die für die Ausführung auf dem Cluster konfiguriert sind, wenn ich den Informatica-Cluster-Dienst starte?

Nachdem Sie den Dienst gestartet haben, wird der eingebettete Cluster ausgeführt, der Dienst überwacht den Cluster und startet die Dienste, die für die Ausführung auf dem Cluster konfiguriert sind.

Ich habe den sudo-Zugriff für ein Benutzerkonto auf allen Knoten konfiguriert und das Konto dazu verwendet, den eingebetteten Cluster zu stoppen. Wird der Informatica-Cluster-Dienst weiter ausgeführt?

Der eingebettete Cluster und der Informatica-Cluster-Dienst werden heruntergefahren.

Kann ich ohne sudo-Zugriff den Informatica-Cluster-Dienst starten und stoppen?

Sie können den Informatica-Cluster-Dienst ohne sudo-Zugriff nicht starten und stoppen. Sie können dem Administrator sudo-Zugriff gewähren, damit die Cluster-Computer den Dienst mit den folgenden Befehlen starten oder stoppen können:

- `sudo ambari-server*`
- `sudo ambari-agent*`

ANHANG C

Konfigurieren eines benutzerdefinierten Protokollverzeichnisses für Ambari

- [Konfigurieren eines benutzerdefinierten Protokollverzeichnisses für Ambari, 189](#)

Konfigurieren eines benutzerdefinierten Protokollverzeichnisses für Ambari

Die Ambari-Protokolldateien werden standardmäßig im Verzeichnis `/var/log` gespeichert. Sie können für die Ambari-Protokolldateien ein benutzerdefiniertes Verzeichnis konfigurieren.

Um ein benutzerdefiniertes Verzeichnis für die Speicherung der Ambari-Protokolldateien anzugeben, führen Sie die folgenden Schritte aus:

1. Melden Sie sich bei Informatica Administrator an.
2. Klicken Sie auf den Informatica-Cluster-Dienst, den Sie konfiguriert haben, und klicken Sie auf **Bearbeiten**.
3. Fügen Sie die benutzerdefinierte Eigenschaft `IcsCustomOptions.ihs.hadoop.dir` für den Informatica-Cluster-Dienst hinzu und geben Sie das benutzerdefinierte Verzeichnis im Textfeld **Wert** der Eigenschaft an.
4. Klicken Sie auf **Fertig stellen**.

Konfigurieren von Enterprise Data Catalog für WANdisco Fusion-fähigen Cluster

- [Konfigurieren von Enterprise Data Catalog für WANdisco Fusion-fähigen Cluster, 190](#)

Konfigurieren von Enterprise Data Catalog für WANdisco Fusion-fähigen Cluster

Sie können Enterprise Data Catalog auf einem vorhandenen Cluster bereitstellen, auf dem WANdisco Fusion aktiviert ist. Unternehmen verwenden WANdisco Fusion zum Replizieren und Übertragen von Daten zwischen Hadoop-Clustern. Enterprise Data Catalog unterstützt Cloudera- und Hortonworks-Hadoop-Cluster mit WANdisco Fusion.

Voraussetzungen:

Erstellen Sie ein Verzeichnis mit `Leseberechtigung` auf dem Computer, auf dem die Informatica-Domäne ausgeführt wird, und kopieren Sie die folgenden JAR-Dateien vom Hadoop-Cluster in das Verzeichnis:

- Für einen Cloudera-Hadoop-Cluster:
 - `hadoop-yarn-api-<Version>-cdh<Version>.jar`
 - `hadoop-yarn-common-<Version>-cdh<Version>.jar`
 - `hadoop-yarn-client-<Version>-cdh<Version>.jar`
- Für einen Hortonworks-Hadoop-Cluster:
 - `hadoop-yarn-api-<Version>-hdp<Version>.jar`
 - `hadoop-yarn-common-<Version>-hdp<Version>.jar`
 - `hadoop-yarn-client-<Version>-hdp<Version>.jar`

Sie können die Dateien `hadoop-yarn-api-<Version>-<Hadoop-Clustertyp><Version>.jar`, `hadoop-yarn-common-<Version>-<Hadoop-Clustertyp><Version>.jar` und `hadoop-yarn-client-<version>-<Hadoop-Clustertyp><Version>.jar` von dem Computer kopieren, auf dem Sie den Hadoop-Cluster installiert haben.

- Kopieren Sie alle JAR-Dateien von dem Computer, auf dem Sie den WANdisco Fusion-Client installiert haben, in das von Ihnen erstellte Verzeichnis. Der Standardspeicherort, von dem aus Sie die Fusion-JAR-Dateien kopieren können, ist `/opt/wandisco/fusion/client/lib` auf dem Computer, auf dem Sie den WANdisco Fusion-Client installiert haben.
- Stellen Sie sicher, dass die in der WANdisco Fusion-Benutzerschnittstelle aufgelisteten **Plug-Ins** den Status **Aktiv** haben.
- Wenn Sie das Profiling auf der Blaze-Engine für Ressourcen basierend auf dem verwendeten Hadoop-Clustertyp ausführen möchten, müssen Sie die folgenden Dateien in das Verzeichnis `<INFA_HOME>/services/shared/hadoop/<Distributionsversion>/lib` kopieren:
 - Kopieren Sie alle JAR-Dateien aus dem Pfad der Fusion-Client-Bibliotheken. Der Standardpfad ist `/opt/wandisco/fusion/client/lib`
 - Die folgenden Dateien von dem Computer, auf dem Sie den Hadoop-Cluster installiert haben:
 - `hadoop-yarn-api-<Version>-<Hadoop-Clustertyp><Version>.jar`
 - `hadoop-yarn-common-<Version>-<Hadoop-Clustertyp><Version>.jar`
 - `hadoop-yarn-client-<Version>-<Hadoop-Clustertyp><Version>.jar`

Hinweis: Stellen Sie sicher, dass Sie die Leseberechtigung für das Verzeichnis konfigurieren, in dem sich die JAR-Dateien befinden.

Um den Enterprise Data Catalog auf einem WANdisco Fusion-fähigen vorhandenen Cluster bereitzustellen, führen Sie die folgenden Schritte aus:

1. Melden Sie sich bei Informatica Administrator an.
2. Wählen Sie den von Ihnen konfigurierten Katalogdienst aus und klicken Sie auf **Bearbeiten**.
3. Fügen Sie die folgenden benutzerdefinierten Eigenschaften für den Katalogdienst hinzu:
 - `LdmCustomOptions.deployment.is.wandisco.cluster`. Geben Sie im Textfeld **Wert** den Wert **true** an. Der Standardwert ist **false**.
 - `LdmCustomOptions.ldm.extra.jars.location`. Geben Sie im Textfeld **Wert** den Pfad zu dem Verzeichnis an, in dem sich die JAR-Dateien befinden.
4. Klicken Sie auf **Fertig stellen**.

Wenn Sie den Katalogdienst mit dem Installationsprogramm erstellt haben, wird der Dienst erstellt, aber nicht gestartet. Sie müssen die benutzerdefinierten Eigenschaften

`LdmCustomOptions.ldm.extra.jars.location` und `LdmCustomOptions.deployment.is.wandisco.cluster` für den Katalogdienst mit Informatica Administrator konfigurieren und dann den Dienst starten.

ANHANG E

Konfigurieren des Informatica Custom Service-Deskriptors

Dieser Anhang umfasst die folgenden Themen:

- [Übersicht, 192](#)
- [Voraussetzungen, 193](#)
- [Erstellen des Informatica Custom Service-Deskriptordiensts, 193](#)
- [Häufig gestellte Fragen \(FAQ\), 195](#)

Übersicht

Enterprise Data Catalog stellt einen Custom Service Descriptor (CSD) bereit, den Sie zum Erstellen des CSD-basierten Informatica-Diensts auf einem vorhandenen Kerberos-fähigen Cloudera-Hadoop-Cluster verwenden können.

Wenn Sie Enterprise Data Catalog auf einem vorhandenen Kerberos-fähigen Cloudera-Hadoop-Cluster bereitstellen, müssen Sie die Hostnamen-Keytabs und die HTTP-Keytabs für alle Knoten zusammenführen, auf denen der Cloudera NodeManger ausgeführt wird. Sie müssen dann die zusammengeführte Keytab in der Eigenschaft **Dienst-Keytab-Speicherort** angeben, wenn Sie den Katalogdienst zum Authentifizieren des Clientzugriffs auf den Enterprise Data Catalog konfigurieren.

Ein CSD stellt eine JAR-Datei dar, die den Dienst definiert, den Sie auf einem Cloudera-Hadoop-Cluster erstellen möchten, der CSD-basierte Dienste unterstützt. Nachdem Sie den CSD-basierten Informatica-Dienst erstellt haben, der in Cloudera Service and Configuration Manager (SCM) als Informatica-Datenkatalogdienst bezeichnet wird, können Sie über Cloudera Manager auf den Dienst zugreifen. Sie können den Informatica-Datenkatalogdienst zum Kopieren der HTTP-Keytab von jedem Knoten an einen Speicherort der RAM-Disk verwenden, der auf diesem Knoten angegeben ist. Sie können den Speicherort der RAM-Disk angeben, wenn Sie den Informatica-Datenkatalogdienst konfigurieren. Der Katalogdienst ruft die HTTP-Prinzipale aus der HTTP-Keytab am Speicherort der RAM-Disk ab.

Die Vorteile bei Verwendung des Informatica-Datenkatalogdiensts sind:

- Die Speicherorte der RAM-Disk sind temporäre Speicherorte im Arbeitsspeicher, durch die Sicherheitsverstöße verhindert werden.
- Sie können Sicherheitsrisiken vermeiden, die mit der Verwendung einer HTTP-Keytab verbunden sind, da auf die im Speicherort der RAM-Disk gespeicherte Keytab nur von Informatica-Anwendungen zugegriffen werden kann.

- Sie können die manuellen Schritte vermeiden, zu denen das Kopieren der HTTP-Prinzipale von jedem Knoten und das Zusammenführen der Hostnamen-Keytabs und der HTTP-Keytab gehören.

Voraussetzungen

Stellen Sie sicher, dass die folgenden Voraussetzungen auf allen Cloudera-Hadoop-Clusterknoten erfüllt sind:

- Stellen Sie sicher, dass der Administrator des Cloudera Service and Configuration Manager (SCM) Eigentümer des Verzeichnisses ist, in dem Sie die HTTP-Keytab speichern. Mit dem Befehl `chown cloudera-scm:cloudera-scm <Verzeichnis>` können Sie die Eigentümerschaft des Verzeichnisses zuweisen. Alternativ können Sie sicherstellen, dass das Verzeichnis, in dem Sie die HTTP-Keytab für jeden Knoten speichern, über Lese-, Schreib- und Ausführungsberechtigungen verfügt.
- Der Informatica-Datenkatalogdienst verwendet auf jedem Knoten standardmäßig Port 8080. Wenn Sie diesen Port für den Dienst verwenden möchten, stellen Sie sicher, dass der Port auf jedem Knoten frei ist. Sie können den Port ändern, wenn Sie den CSD-basierten Informatica-Dienst erstellen oder aktivieren.
- Stellen Sie sicher, dass der Benutzer des Dienst-Clusters zur Cloudera SCM-Gruppe hinzugefügt wird. Verwenden Sie den Befehl `usermod -G cloudera-scm <SCN-Benutzer>`, um den Benutzer des Dienst-Clusters zur Cloudera SCM-Gruppe hinzuzufügen.

Erstellen des Informatica Custom Service-Deskriptordiensts

Sie können die Datei `INFORMATICA_DATA_CATALOG-1.0.jar` verwenden, um den Informatica-Datenkatalogdienst in einem Cloudera-Hadoop-Cluster zu erstellen. Kopieren Sie die JAR-Datei von `$INFA_HOME/services/CatalogService/ClouderaKeytabUtility/`.

Führen Sie die folgenden Schritte zum Erstellen des Informatica-Datenkatalogdiensts durch:

1. Kopieren Sie `INFORMATICA_DATA_CATALOG-1.0.jar` in das Verzeichnis `„/opt/cloudera/csd“` auf dem Computer, auf dem Sie Cloudera Service and Configuration Manager (SCM) installiert haben.
2. Starten Sie den Cloudera SCM-Server neu.
3. Öffnen Sie die Benutzeroberfläche von Cloudera SCM.
Hinweis: Wenn die Cloudera-Management-Dienste ausgeführt werden, starten Sie die Dienste neu.
4. Wenn Sie den Cluster erstellt haben, wählen Sie in der Benutzeroberfläche von Cloudera SCM die Option zum Hinzufügen des **Informatica-Datenkatalogdiensts**. Wenn Sie einen Cluster erstellen, wählen Sie bei der Auswahl der zu installierenden Dienste den **Informatica-Datenkatalogdienst** aus. Siehe folgendes Bild als Referenz:

Service Type	Description
ADLS Connector	The ADLS Connector service provides key management for accessing Azure Data Lake Stores from CDH services.
Accumulo	The Apache Accumulo sorted, distributed key/value store is a robust, scalable, high performance data storage and retrieval system. This service only works with releases based on Apache Accumulo 1.6 or later.
Echo	The echo service
Flume	Flume collects and aggregates data from almost any source into a persistent store such as HDFS.
HBase	Apache HBase provides random, real-time, read/write access to large data sets (requires HDFS and ZooKeeper).
HDFS	Apache Hadoop Distributed File System (HDFS) is the primary storage system used by Hadoop applications. HDFS creates multiple replicas of data blocks and distributes them on compute hosts throughout a cluster to enable reliable, extremely rapid computations.
Hive	Hive is a data warehouse system that offers a SQL-like language called HiveQL.
Hue	Hue is a graphical user interface to work with the Cloudera Distribution Including Apache Hadoop (requires HDFS, MapReduce, and Hive).
Impala	Impala provides a real-time SQL query interface for data stored in HDFS and HBase. Impala requires the Hive service and shares the Hive Metastore with Hue.
Informatica Data Catalog	Informatica Enterprise Data Catalog Service to get http keytabs

Back Continue

5. Wenn Sie den Dienst im Assistenten zum Hinzufügen von Diensten konfigurieren, wählen Sie die Knoten in dem Cluster aus, auf dem Cloudera NodeManager ausgeführt wird, wie in der folgenden Abbildung dargestellt:

cloudera MANAGER Support ▾ admin ▾

Add Informatica Data Catalog Service to Cluster 1

Customize Role Assignments for Informatica Data Catalog

You can customize the role assignments for your new service here, but note that if assignments are made incorrectly, such as assigning too many roles to a single host, performance will suffer.

You can also view the role assignments by host. View By Host

Informatica Server × 1 New

vats001.informatica.com ▾

Feedback

Back 1 2 3 4 5 Continue

6. Geben Sie den Port für den Dienst an. Der Standardwert ist 8080.
7. Geben Sie den Speicherort der RAM-Disk auf den Knoten an, auf denen Sie die HTTP-Keytab speichern möchten, wie in der folgenden Abbildung dargestellt:

Add Informatica Data Catalog Service to Cluster 1

Review Changes

Directory Directory	Informatica Server Default Group <input type="text"/> Missing required value: Directory	?
Webserver port Service_Port	Informatica Server Default Group <input type="text" value="8080"/>	?

Back 1 2 3 4 Continue

8. Klicken Sie auf **Fortfahren** und führen Sie den Assistenten zum Hinzufügen von Diensten aus, um den Informatica-Datenkatalogdienst hinzuzufügen.

Hinweis: Wenn Sie den Informatica-Datenkatalogdienst starten, kopiert der Dienst die HTTP-Keytab an den angegebenen Speicherort der RAM-Disk.

Häufig gestellte Fragen (FAQ)

Was sind die Voraussetzungen, um eine HTTP-Keytab neu zu generieren?

Führen Sie die folgenden Schritte aus, bevor Sie eine HTTP-Keytab neu generieren:

1. Stoppen Sie den Katalogdienst.
Cloudera Manager fordert Sie auf, alle Dienste zu stoppen, die HTTP-Keytabs benötigen. Die Dienste umfassen den NodeManager-Dienst, den ResourceManager-Dienst und den Informatica-Dienst.
2. Stoppen Sie die Dienste, die HTTP-Keytabs benötigen.
3. Generieren Sie die Benutzerprinzipale des Dienst-Clusternamens für alle Dienste, einschließlich des Katalogdiensts, neu.
4. Starten Sie die Dienste, die Sie gestoppt haben.

Wie richte ich eine RAM-Disk auf einem Knoten ein?

Fügen Sie den Eintrag `<RAM-Disk-Verzeichnis> tmpfs nodev,nosuid,noexec,nodiratime,size=<Größe der RAM-Disk> 0 0` für den Mount-Speicherort in die Datei `/etc/fstab` ein. Wenn Sie beispielsweise `/mnt/ramdiskdir` als RAM-Disk-Verzeichnis angeben und 512 MB als Größe der RAM-Disk konfigurieren möchten, fügen Sie folgenden Mount-Eintrag hinzu:
`tmpfs /mnt/ramdiskdir tmpfs nodev,nosuid,noexec,nodiratime,size=512M 0 0`

Hinweis: Wenn Sie den Computer neu starten, wird das RAM-Disk-Verzeichnis beibehalten, die Daten im RAM-Disk-Verzeichnis werden jedoch gelöscht.

Verwenden Sie den folgenden Befehl, wenn Sie eine RAM-Disk vorübergehend einrichten möchten: `mount -t tmpfs -o size=<Größe der RAM-Disk> tmpfs <RAM-Disk-Verzeichnis>`

Muss ich den Benutzer für den Dienst-Clusternamen zur Cloudera SCM-Gruppe hinzufügen?

Cloudera Manager führt den CSD-Dienst mit den Berechtigungen eines Cloudera SCM-Benutzers aus. Die Cloudera SCM-Benutzerberechtigungen werden zudem zum Generieren der spnego-Keytab verwendet. Ein Cloudera SCM-Benutzer verfügt möglicherweise nicht über ausreichend Berechtigungen, um einem

Benutzer des Dienst-Clusters die Eigentümerberechtigung für eine Keytab zu erteilen. Die für eine Keytab konfigurierten Standardberechtigungen sind `640`. Dadurch erhält nur der Eigentümer der Keytab Lese- und Schreibberechtigungen und die Gruppe Leseberechtigung. Um dem Benutzer des Dienst-Clusters eingeschränkten Zugriff ähnlich dem des Cloudera SCM-Benutzers zu gewähren, können Sie den Namen des Benutzers des Dienst-Clusters zur Cloudera SCM-Gruppe hinzufügen.

ANHANG F

Erstellen von benutzerdefinierten Benutzern und Benutzergruppen für Dienste, die in einem eingebetteten Cluster bereitgestellt werden

Dieser Anhang umfasst die folgenden Themen:

- [Übersicht, 197](#)
- [Voraussetzungen, 198](#)
- [Erstellen von benutzerdefinierten Benutzern und Benutzergruppen für Dienste, die in einem eingebetteten Cluster bereitgestellt werden, 198](#)

Übersicht

Sie können benutzerdefinierte Benutzernamen und Benutzergruppen für Dienste wie HDFS und YARN erstellen, wenn Sie Enterprise Data Catalog auf einem eingebetteten Hadoop-Cluster bereitstellen.

Ambari verwendet für Dienste standardmäßig Benutzernamen wie hdfs, zookeeper, yarn und postgres. Sie können benutzerdefinierte Benutzernamen und Benutzergruppen für Ambari konfigurieren, indem Sie benutzerdefinierte Eigenschaften im Informatica-Cluster-Dienst hinzufügen.

Hinweis: Fügen Sie alle benutzerdefinierten Eigenschaften hinzu, wenn Sie den Informatica-Cluster-Dienst erstellen.

Die Liste der benutzerdefinierten Eigenschaften, die Sie für Benutzernamen und Benutzergruppen konfigurieren können, lautet wie folgt:

Benutzername	Benutzerdefinierte Eigenschaft
hdfs	lcsCustomOptions.ihssecurity.hdfs.user
yarn	lcsCustomOptions.ihssecurity.yarn.user

Benutzername	Benutzerdefinierte Eigenschaft
mapred	lcsCustomOptions.ihssecurity.mapred.user
zookeeper	lcsCustomOptions.ihssecurity.zookeeper.user
ams	lcsCustomOptions.ihssecurity.ams.user
smoke	lcsCustomOptions.ihssecurity.smoke.user

Benutzergruppe	Benutzerdefinierte Eigenschaft
Proxybenutzer	lcsCustomOptions.ihssecurity.proxyuser.group
hadoop	lcsCustomOptions.ihssecurity.hadoop.group

Voraussetzungen

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind, bevor Sie benutzerdefinierte Benutzernamen oder Benutzergruppen für Dienste erstellen:

- Geben Sie benutzerdefinierte Eigenschaften für alle Benutzernamen und Benutzergruppen an.
- Bevor Sie den Informatica-Cluster-Dienst aktivieren, vergewissern Sie sich, dass alle benutzerdefinierten Benutzer und Benutzergruppen in LDAP vorhanden sind. Wenn Sie lokal verwaltete benutzerdefinierte Benutzer und Benutzergruppen verwenden möchten, vergewissern Sie sich, dass die benutzerdefinierten Benutzer und Benutzergruppen auf dem lokalen Computer vorhanden sind.
- Vergewissern Sie sich, dass Sie alle Aufgaben verwalten, die mit dem Erstellen und Verwalten der benutzerdefinierten Benutzer und Benutzergruppen verbunden sind. Zu den Aufgaben gehören das Hinzufügen benutzerdefinierter Benutzer in den erforderlichen Benutzergruppen und das Erstellen von Basisverzeichnissen.
- Stellen Sie sicher, dass Sie den Smoke-Benutzernamen in den folgenden Benutzergruppen angeben:
 - Proxybenutzer
 - hadoop

Erstellen von benutzerdefinierten Benutzern und Benutzergruppen für Dienste, die in einem eingebetteten Cluster bereitgestellt werden

Führen Sie die folgenden Schritte aus, um benutzerdefinierte Benutzernamen und Benutzergruppen zu konfigurieren:

1. Melden Sie sich bei Informatica Administrator an.

2. Führen Sie die Schritte zum Erstellen eines Informatica-Cluster-Diensts aus, wie im Abschnitt *Erstellen eines Informatica-Cluster-Diensts* aufgeführt.
3. Fügen Sie alle benutzerdefinierten Eigenschaften hinzu und geben Sie die benutzerdefinierten Benutzernamen und Benutzergruppen als Werte für die benutzerdefinierten Eigenschaften im Informatica-Cluster-Dienst an.
4. Klicken Sie auf **Fertig stellen**.

ANHANG G

Konfigurieren benutzerdefinierter Ports für Hadoop-Anwendungen

Dieser Anhang umfasst die folgenden Themen:

- [Übersicht, 200](#)
- [Konfigurieren benutzerdefinierter Ports für Hadoop-Anwendungen, 202](#)

Übersicht

Sie können benutzerdefinierte Ports für Hadoop-Anwendungen angeben, wenn Sie den Informatica-Cluster-Dienst erstellen oder ändern.

Auf Basis der Datengröße, die Sie in der Eigenschaft **Ladetyp** angeben, wenn Sie den Informatica-Cluster-Dienst erstellen, können Sie die Hadoop-Anwendungseigenschaften und die benutzerdefinierten Ports in der Datei `LowLoad.properties`, `MediumLoad.properties` oder `HighLoad.properties`, die sich im Verzeichnis `<INFA_HOME>/services/InfahadoopService/Binaries` befinden, hinzufügen. Sie können dann den Informatica-Cluster-Dienst aktivieren oder neu starten, um die benutzerdefinierten Portänderungen zu implementieren.

Hinweis: Achten Sie darauf, dass Sie keine weiteren Zeilen aus der Datei `<Ladetyp>.properties` entfernen. Der `Ladetyp` unter `<Load Type>` kann `LowLoad`, `MediumLoad` oder `HighLoad` sein.

Die Liste der benutzerdefinierten Ports, die Sie für Hadoop-Anwendungen konfigurieren können, lautet wie folgt:

Hadoop-Anwendungseigenschaft	Standardportwert
<code>zoo.cfg.clientPort</code>	2181
<code>yarn-site.yarn.resourcemanager.webapp.address</code>	8046
<code>yarn-site.yarn.resourcemanager.webapp.https.address</code>	8088
<code>yarn-site.yarn.resourcemanager.address</code>	8032
<code>yarn-site.yarn.resourcemanager.resource-tracker.address</code>	8025
<code>yarn-site.yarn.resourcemanager.scheduler.address</code>	8030

Hadoop-Anwendungseigenschaft	Standardportwert
yarn-site.yarn.resourcemanager.admin.address	8141
yarn-site.yarn.nodemanager.address	45454
yarn-site.yarn.nodemanager.webapp.address	8042
yarn-site.yarn.timeline-service.address	10200
yarn-site.yarn.timeline-service.webapp.address	8188
yarn-site.yarn.timeline-service.webapp.https.address	8190
hdfs-site.dfs.namenode.http.address	50070
hdfs-site.dfs.namenode.https.address	50470
hdfs-site.dfs.namenode.rpc.address	8020
hdfs-site.dfs.datanode.address	50010
hdfs-site.dfs.datanode.http.address	50075
hdfs-site.dfs.datanode.https.address	50475
hdfs-site.dfs.journalnode.rpc.address	8485
hdfs-site.dfs.journalnode.http.address	8480
hdfs-site.dfs.journalnode.https.address	8481
hdfs-site.dfs.datanode.ipc.address	8010
mapred-site.mapreduce.jobhistory.address	10020
mapred-site.mapreduce.jobhistory.webapp.address	19888

Hinweis: Konfigurieren Sie für einen eingebetteten Cluster, in dem Kerberos nicht aktiviert ist, die Ports im Bereich von 1024 bis 65535.

Konfigurieren von Anwendungsports für einen Kerberos-fähigen eingebetteten Cluster

Sie können benutzerdefinierte Ports für die folgenden Hadoop-Anwendungseigenschaften konfigurieren, wenn der eingebettete Cluster für Kerberos aktiviert ist:

- Stellen Sie sicher, dass Sie Werte im Bereich von 0 bis 1023 konfigurieren, wenn Sie benutzerdefinierte Werte für die folgenden Hadoop-Anwendungseigenschaften bereitstellen möchten:
 - `dfs.datanode.address`
 - `dfs.datanode.http.address`

Hinweis: Wenn der eingebettete Cluster nicht Kerberos-fähig ist, können Sie die Werte im Bereich von 0 bis 1023 für die folgenden Hadoop-Anwendungseigenschaften konfigurieren:

- `hdfs-site.dfs.datanode.address` Der Standardwert ist 1019.
- `hdfs-site.dfs.datanode.http.address` Der Standardwert ist 1022.

Konfigurieren benutzerdefinierter Ports für Hadoop-Anwendungen

Führen Sie die folgenden Schritte aus, um benutzerdefinierte Benutzernamen und Benutzergruppen zu konfigurieren:

1. Melden Sie sich bei Informatica Administrator an.
2. Öffnen Sie die Datei `<Ladety>.properties`, die sich in folgendem Verzeichnis befindet: `<INFA_HOME>/services/InfahadoopService/Binaries`
3. Fügen Sie den benutzerdefinierten Port für die Hadoop-Anwendung in folgendem Format hinzu: `<Eigenschaft>=${host}:<Port>` in der Datei `custom.properties.<Größe>`. Um beispielsweise einen benutzerdefinierten Port für `yarn-site.yarn.resource-manager.webapp.address` anzugeben, fügen Sie folgende Zeile in die Datei `yarn-site.yarn.resource-manager.webapp.address=${host}:<Benutzerdefinierte Portnummer>` ein. Ersetzen Sie `<Benutzerdefinierte Portnummer>` durch die benötigte Portnummer.
4. Speichern Sie die Datei `custom.properties.<Größe>`.
5. Klicken Sie auf **Fertig stellen**.
6. Deaktivieren und aktivieren Sie dann den Informatica-Cluster-Dienst, um die Änderungen zu implementieren.

Wenn Sie einen vorhandenen Informatica-Cluster-Dienst ändern, können Sie den Informatica-Cluster-Dienst neu starten, um die Änderungen zu implementieren. Wenn Sie den Dienst neu starten möchten, stellen Sie sicher, dass die Portnummern für die folgenden Hadoop-Anwendungseigenschaften mit den Portnummern übereinstimmen, die für die in der Spalte *Dependent Hadoop Application Property* aufgelisteten Eigenschaften konfiguriert sind:

Hadoop-Anwendungseigenschaft	Abhängige Hadoop-Anwendungseigenschaft
<code>yarn-site.yarn.log.server.url</code>	<code>mapred-site.mapreduce.jobhistory.webapp.address</code>
<code>yarn-site.yarn.log.server.web-service.url</code>	<code>yarn-site.yarn.timeline-service.webapp.address</code>
<code>hdfs-site.dfs.namenode.shared.edits.dir</code>	<code>hdfs-site.dfs.journalnode.rpc.address</code>

Wenn Sie beispielsweise die Portnummer 8189 für `mapred-site.mapreduce.jobhistory.webapp.address` konfiguriert haben, geben Sie die gleiche Portnummer für `yarn-site.yarn.log.server.url` an.

INDEX

A

- abhängige Dienste
 - Übersicht [145](#)
- AddLicense (infacmd)
 - Fehlerbehebung [172](#)
- Anwendungsdienste
 - Abhängigkeiten [145](#)
 - Benennungskonventionen [33](#)
 - Installationsanforderungen [32](#)
 - Ports [29](#)
 - Übersicht [22](#)
 - Voraussetzungen [143](#)
 - Vorbereitung zum Erstellen [137](#)
- Authentifizierung
 - Kerberos [64](#)

B

- Behebung von Fehlern beim Beitreten zu Domänen [171](#)
- Benutzerauthentifizierung
 - Übersicht [22](#)
- Benutzerkonten
 - Modellrepository [148](#)
- Berechnungsrolle
 - Knoten [20](#)
- Berechtigungen
 - Katalogdienst [134](#)

C

- catalina.out
 - Fehler bei der Installation beheben [169](#)
- Clients
 - Übersicht [24](#)
- Clusterverwaltung
 - Übersicht [60](#)
- Content-Management-Dienst
 - abhängiger Dienst [145](#)
 - erforderliche Datenbanken [28](#)
 - Übersicht [27](#)
 - zugeordnete Dienste [27](#)
- Content-Managementdienst
 - erstellen [160](#)
 - konfigurieren [160](#)

D

- Data Analyzer Repository
 - Sybase ASE-Datenbankanforderungen [42](#)
- Datenbankanforderungen
 - Datenobjekt-Cache [42](#)
 - Installationsanforderungen [31](#)

- Datenbankanforderungen (*Fortsetzung*)
 - Modellrepository [43](#)
 - Profiling-Warehouse [46](#)
 - Referenzdaten-Warehouse [47](#)
- Datenbankbenutzerkonten
 - Richtlinien für das Einrichten [39](#)
- Datenbanken
 - Data Analyzer Repository [39](#)
- Datenbankverbindungen
 - erstellen [138](#)
- Datenintegrationsdienst
 - abhängiger Dienst [145](#)
 - erstellen [150](#)
 - Konfiguration der Hostdatei [153](#)
 - konfigurieren [150](#)
 - nach dem Erstellen [153](#)
 - Übersicht [25](#)
 - zugeordnete Dienste [25](#)
- Datenobjekt-Cache
 - Datenbankanforderungen [42](#)
 - IBM DB2-Datenbankanforderungen [43](#)
 - Microsoft SQL Server-Datenbankanforderungen [43](#)
 - Oracle-Datenbankanforderungen [43](#)
- Debug-Protokolle
 - Beheben von Fehlern bei der Installation [169](#)
- Deinstallation
 - Regeln und Richtlinien [165](#)
- Dienste
 - Anwendungsdienste [22](#)
 - Dienstmanager [21](#)
- Dienstmanager
 - Übersicht [21](#)
- Dienstrolle
 - Knoten [20](#)
- Domänen
 - Anwendungsdienste [22](#)
 - Benennungskonventionen [33](#)
 - Benutzerauthentifizierung [22](#)
 - Dienstmanager [21](#)
 - Knoten [20](#)
 - konfigurieren [131](#)
 - planen [24](#)
 - Ports [29](#)
 - Sicherheit [23](#)
 - Übersicht [19](#)
- Domänen-Konfigurations-Repository
 - Microsoft SQL Server-Datenbankanforderungen [41](#)
- Domänenkonfigurations-Repository
 - Anforderungen [31](#)
 - Fehlerbehebung [170](#)
 - IBM DB2-Datenbankanforderungen [39, 44](#)
 - Oracle-Datenbankanforderungen [41](#)
 - Vorbereiten der Datenbanken [39](#)
- Domänenobjekte
 - Benennungskonventionen [33](#)

Domänensicherheit
Übersicht [23](#)

E

Eingebetteter Hadoop-Cluster
Vorbereiten [60](#)

Einzelknoten
Installation [19](#)

Enterprise Data Catalog
automatische Installation [108](#), [128](#)
Bereitstellung – Übersicht [49](#)
deinstallieren [166](#)
Dienste [15](#), [16](#)
Eingebettete Hadoop-Bereitstellung [49](#)
Installation [13](#)
Installation im Konsolenmodus [70](#)
Vorhandene Hadoop-Bereitstellung [63](#)

Enterprise Data Catalog-Dienste
Starten und Beenden unter Linux [185](#)

Enterprise Data Catalog-Server
deinstallieren [165](#)

F

Fehlerbehebung
Ausführen einer Ressource [171](#)
Beitreten zu Domänen [171](#)
Domänenkonfigurations-Repository [170](#)
Erstellen von Domänen [171](#)
Informatica-Dienste [171](#)
Lizenzen [172](#)
Pingen von Domänen [172](#)

G

Gateway-Knoten
Erstellen während der Installation [20](#)

Gebietsschema-Umgebungsvariablen
konfigurieren [132](#)

geräuschloser Modus
Enterprise Data Catalog [108](#)
Installation von Enterprise Data Catalog [128](#)

H

Hostdatei
Datenintegrationsdienst [153](#)

I

IBM DB2-Datenbankanforderungen
Datenobjekt-Cache [43](#)
Domänen-Repository [39](#), [44](#)
Modellrepository-Datenbank [39](#), [44](#)
Profiling-Warehouse [46](#)
Referenzdaten-Warehouse [48](#)

infacmd
Pingen von Objekten [172](#)

Informatica Administrator
anmelden [137](#)

Informatica-Cluster-Dienst
Arbeitsablauf [56](#)

Informatica-Cluster-Dienst (*Fortsetzung*)
Übersicht [27](#), [56](#)

Informatica-Clusterdienst
Erstellen [57](#)

Informatica-Dienste
Fehlerbehebung [171](#)

Installation
Prozess [14](#)

Installationsanforderungen
Anwendungsdienst-Anforderungen [32](#)
Datenbankanforderungen [31](#)
Festplattenspeicher [29](#)
Mindest-Systemanforderungen [28](#)
Portanforderungen [29](#)

Installationsprotokolle
Beschreibungen [169](#)

K

Katalogdienst
abhängiger Dienst [145](#)
Berechtigungen [134](#)
Erstellen [153](#)
Übersicht [26](#)
zugeordnete Dienste [26](#)

Kerberos-Authentifizierung
Vorhandener Cluster [64](#)

Knoten
Anwendungsdienste [22](#)
Benennungskonventionen [33](#)
Berechnungsrolle [20](#)
Dienstmanager [21](#)
Dienstrolle [20](#)
Fehlerbehebung [171](#)
gateways [20](#)
Rollen [20](#)
Übersicht [20](#)
worker [20](#)

Kompatibilität der Codepage
Anwendungsdienste [131](#)
Gebietsschema [131](#)

Konfiguration
Domänen [131](#)
Umgebungsvariablen [132](#), [133](#)
Umgebungsvariablen unter Linux [134](#)

Konsolenmodus
Installieren von Enterprise Data Catalog-Diensten [70](#)

L

LANG
Umgebungsvariablen [132](#)

LC_ALL
Umgebungsvariablen [132](#)

LC_CTYPE
Umgebungsvariablen [132](#)

Linux
Bibliothekspfade [134](#)
Installieren der Enterprise Data Catalog-Dienste im Konsolenmodus [70](#)
Starten und Beenden von Enterprise Data Catalog-Diensten [185](#)
Umgebungsvariablen [132](#)

Lizenzen
hinzufügen [172](#)
Übersicht [22](#)

Lizenzschlüssel
Übersicht [22](#)
localhost
Datenintegrationsdienst [153](#)

M

Mehrere Knoten
Installation [19](#)
Microsoft SQL Server-Datenbankanforderungen
Datenobjekt-Cache [43](#)
Domänen-Konfigurations-Repository [41](#)
Modellrepository [45](#)
Profiling-Warehouse [46](#)
Referenzdaten-Warehouse [48](#)
Mindest-Systemanforderungen
Knoten [32](#)
Modellrepository
Benutzer [148](#)
Datenbankanforderungen [43](#)
IBM DB2-Datenbankanforderungen [39, 44](#)
Microsoft SQL Server-Datenbankanforderungen [45](#)
Oracle-Datenbankanforderungen [45](#)
Modellrepository-Dienst
erforderliche Datenbanken [26](#)
Erstellen [146](#)
Konfigurieren [145](#)
nach dem Erstellen [148](#)
Übersicht [26](#)

N

node.log
Fehler bei der Installation beheben [169](#)

O

Oracle-Datenbankanforderungen
Datenobjekt-Cache [43](#)
Domänenkonfigurations-Repository [41](#)
Modellrepository [45](#)
Profiling-Warehouse [47](#)
Referenzdaten-Warehouse [48](#)

P

Ping (infacmd)
Fehlerbehebung [172](#)
Plattenspeicheranforderungen
Installationsanforderungen [29](#)
Portanforderungen
Installationsanforderungen [29](#)
Ports
Anforderungen [29](#)
Anwendungsdienste [29](#)
Domänen [29](#)
Profiling Warehouse
IBM DB2-Datenbankanforderungen [46](#)
Microsoft SQL Server-Datenbankanforderungen [46](#)
Profiling-Warehouse
Datenbankanforderungen [46](#)
Oracle-Datenbankanforderungen [47](#)
Protokolldateien
catalina.out [169](#)

Protokolldateien (*Fortsetzung*)
Debug-Protokolle [169](#)
Installation [168](#)
Installationsprotokolle [169](#)
node.log [169](#)
Typen [168](#)

R

Referenzdaten-Warehouse
Datenbankanforderungen [47](#)
IBM DB2-Datenbankanforderungen [48](#)
Microsoft SQL Server-Datenbankanforderungen [48](#)
Oracle-Datenbankanforderungen [48](#)
Repositorys
Vorbereiten der Datenbanken [38](#)

S

Service Manager
Protokolldateien [169](#)
Sicherheit
Datenspeicher [23](#)
Domänen [23](#)
Sicherheitsdomänen
SSL [64](#)
Sybase ASE-Datenbankanforderungen
Data Analyzer Repository [42](#)
Systemdienste
Übersicht [22](#)
Systemvoraussetzungen
Anwendungsdienste [32](#)
Mindest-Installationsanforderungen [28](#)
Minimal [28](#)

U

Umgebungsvariablen
Bibliothekspfade unter Linux [134](#)
Gebietsschema [132](#)
konfigurieren [132, 133](#)
konfigurieren unter Linux [134](#)
LANG [132](#)
LANG_C [132](#)
LC_ALL [132](#)
LC_CTYPE [132](#)
Linux [132](#)

V

Verbindungen
Eigenschaften für Oracle [141](#)
Erstellen von Datenbankverbindungen [138, 142](#)
IBM DB2-Eigenschaften [139](#)
Microsoft SQL Server-Eigenschaften [140](#)
Verschlüsselungsschlüssel
sicherer Datenspeicher [23](#)
Übersicht [23](#)
Voraussetzungen
Anwendungsdienste [143](#)
Vorbereitungen für Datenbanken
Repositorys [38](#)
Vorhandener Hadoop-Cluster
Vorbereiten [64](#)

W

Worker-Knoten

Erstellen während der Installation [20](#)