



Informatica®
10.5.9

Installation für PowerCenter und Data Quality

© Copyright Informatica LLC 1998, 2025

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

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

Gemäß Ihren Opt-out-Rechten überträgt die Software automatisch Informationen über die Computer- und Netzwerkumgebung, in der die Software bereitgestellt wird, sowie über die Datennutzung und Systemstatistiken der Bereitstellung an Informatica in den USA. Diese Übertragung gilt als Teil der Services/Dienste im Rahmen der Datenschutzrichtlinie von Informatica; die Verwendung und anderweitige Verarbeitung der Informationen durch Informatica erfolgen entsprechend der Datenschutzrichtlinie von Informatica, die hier zur Verfügung steht: <https://www.informatica.com/in/privacy-policy.html> Sie können die Sammlung von Nutzungsdaten im Administrator Tool deaktivieren.

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.

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 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.

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 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.

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

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

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 DITTER.

Teile dieser Software und/oder Dokumentationen unterliegen dem Urheberrecht Dritter. Die erforderlichen Hinweise auf Drittanbieter sind im Lieferumfang des Produkts enthalten.

Publikationsdatum: 2025-10-16

Inhalt

Einleitung	13
Informatica-Ressourcen.	13
Informatica Network.	13
Informatica-Wissensdatenbank.	13
Informatica-Dokumentation.	14
Informatica-Produktverfügbarkeitsmatrizen.	14
Informatica Velocity.	14
Informatica Marketplace.	14
Globaler Kundensupport von Informatica.	14
 Teil I: Erste Schritte der Installation.....	15
 Kapitel 1: Erste Schritte der Installation.	16
Checkliste für die ersten Schritte.	16
Installation – Übersicht.	16
Installation Prozess.	17
Planen der Installationsoption.	18
Planen der Installationskomponenten.	19
Knoten.	20
Dienstmanager.	20
Anwendungsdienste.	20
Datenbanken.	20
Benutzerauthentifizierung.	21
Sicherer Datenspeicher.	22
Domänensicherheit.	22
Informatica-Client-Tools.	23
 Teil II: Vor Beginn der Installation.....	24
 Kapitel 2: Vor der Installation von Diensten unter UNIX oder Linux.	25
VorbereitungenCheckliste.	25
Lesen der Versionshinweise.	26
Überprüfen der Systemvoraussetzungen.	26
Überprüfen von temporärem Speicherplatz und von Berechtigungen.	26
Überprüfen von Patch-Anforderungen unter UNIX oder Linux.	27
Überprüfen der Portanforderungen.	28
Überprüfen der Anforderungen an Verteilungspakete(Linux und UNIX).	30
Überprüfen des Grenzwerts für den Dateideskriptor.	30
Überprüfen der Hardwarevoraussetzungen für Anwendungsdienste.	31
Data Transformation-Dateien sichern.	33

Konfigurieren von POSIX Asynchronous I/O.	33
Überprüfen der Umgebungsvariablen.	34
Erstellen eines Systembenutzerkontos.	35
Einrichten einer Schlüsselspeicherdatei.	35
Installieren von Sprachenschriftarten unter UNIX oder Linux.	37
Herunterladen und Extrahieren der Installationsprogrammdateien.	37
Überprüfen der Codesignatur des Installationsprogramms.	38
Überprüfen der Prüfsumme des Installationspakets unter UNIX und Linux.	39
Überprüfen des Lizenzschlüssels.	39
Kapitel 3: Vor der Installation der Dienste unter Windows.	40
Vor der Installation der Dienste unter Windows - Übersicht.	40
Lesen der Versionshinweise.	40
Überprüfen der Systemvoraussetzungen.	41
Überprüfen von temporärem Speicherplatz und von Berechtigungen.	41
Überprüfen der Patchanforderungen.	42
Überprüfen der Portanforderungen.	42
Überprüfen der Anforderungen an Verteilungspakete (Windows).	43
Überprüfen der Hardwarevoraussetzungen für Anwendungsdienste.	44
Data Transformation-Dateien sichern.	45
Überprüfen der Umgebungsvariablen.	46
Erstellen eines Systembenutzerkontos.	46
Einrichten von Schlüsselspeicher- und Truststore-Dateien.	47
Herunterladen und Extrahieren der Installationsprogrammdateien.	49
Überprüfen der Codesignatur des Installationsprogramms.	49
Überprüfen der Prüfsumme des Installationspakets unter Windows.	50
Überprüfen des Lizenzschlüssels.	50
Kapitel 4: Vorbereiten von Anwendungsdiensten und Datenbanken.	51
Checkliste zur Vorbereitung der Anwendungsdienste.	51
Vorbereiten von Anwendungsdiensten und Datenbanken – Übersicht.	52
Einrichten von Datenbankbenutzerkonten.	52
Identifizieren von Anwendungsdiensten nach Produkt.	52
Datenbankanforderungen des Domänen-Konfigurations-Repositorys.	53
IBM DB2-Datenbankanforderungen.	54
Microsoft SQL Server-Datenbankanforderungen.	55
Microsoft Azure SQL-Datenbankanforderungen.	55
Oracle-Datenbankanforderungen.	55
PostgreSQL-Datenbankanforderungen.	56
Sybase – Datenbankanforderungen.	56
Analyst-Dienst.	58
Content-Management-Dienst.	58
Anforderungen des Referenzdaten-Warehouse.	59

Datenintegrationsdienst.	61
Anforderungen für Datenobjekt-Cache-Datenbank.	61
Profiling Warehouse-Anforderungen.	63
Anforderungen an Arbeitsablauf-Datenbanken.	65
Metadata Manager-Dienst.	68
Metadata Manager Repository-Datenbankanforderungen.	68
IBM DB2-Datenbankanforderungen.	69
Microsoft SQL Server-Datenbankanforderungen.	70
Oracle-Datenbankanforderungen.	71
Geteilte Domäne für Metadata Manager.	72
Modellrepository-Dienst.	73
Modellrepository – Datenbankanforderungen.	74
IBM DB2-Datenbankanforderungen.	74
Microsoft Azure SQL-Datenbankanforderungen.	75
Microsoft SQL Server-Datenbankanforderungen.	76
Oracle – Datenbankanforderungen.	76
PostgreSQL-Datenbankanforderungen.	77
Überwachen des Modellrepository-Diensts.	77
PowerCenter-Integrationsdienst.	78
PowerCenter-Repository-Dienst.	79
PowerCenter-Repository-Datenbankanforderungen.	79
IBM DB2-Datenbankanforderungen.	80
Microsoft SQL Server-Datenbankanforderungen.	80
Oracle-Datenbankanforderungen.	80
PostgreSQL-Datenbankanforderungen.	81
Sybase ASE-Datenbankanforderungen.	82
Suchdienst.	82
Konfigurieren nativer Konnektivität auf Dienstcomputern.	83
Install Database Client Software.	84
Konfigurieren von Umgebungsvariablen für Datenbank-Clients.	85
Kapitel 5: Vorbereiten der Kerberos-Authentifizierung.	88
Checkliste zur Vorbereitung der Kerberos-Authentifizierung	88
Vorbereiten der Kerberos-Authentifizierung – Übersicht.	89
Einrichten der Kerberos-Konfigurationsdatei.	89
Generieren des Namensformats für Dienstprinzipale und Keytab-Dateien.	91
Dienstprinzipalanforderungen auf der Knotenebene.	91
Dienstprinzipalanforderungen auf Prozessebene.	92
Ausführen des SPN-Formatgenerators	92
Überprüfen der SPN- und Keytab-Format-Textdatei.	94
Erstellen der Dienstprinzipalnamen und Keytab-Dateien.	96
Fehlerbehebung bei den Dienstprinzipalnamen und Keytab-Dateien.	96

Kapitel 6: Aufzeichnen von Informationen für Abfragen des Installationsprogramms. 99

Checkliste zum Sammeln der Informationen für Abfragen des Installationsprogramms.	99
Aufzeichnen von Informationen für Abfragen des Installationsprogramms – Übersicht.	100
Domäne.	101
Knoten.	102
Verteilungspakete.	102
Anwendungsdienste.	102
Datenbanken	103
Verbindungszeichenfolge für eine sichere Datenbank.	105
Sicherer Datenspeicher.	108
Kerberos.	108

Kapitel 7: Einführung in das Dienste-Installationsprogramm. 110

Aufgaben des Dienste-Installationsprogramms.	110
Sichere Dateien und Verzeichnisse.	110
Vorinstallations-Dienstprogramme.	111
Ausführen des Vorinstallations-Systemprüfungstools (i10Pi) im Konsolenmodus.	112
Ausführen des Vorinstallations-Systemprüfungstools (i10Pi) im Grafikmodus.	115
Ausführen des Vorinstallations-Systemprüfungstools (i10pi) im automatischen Modus.	121

Teil III: Ausführen des Dienste-Installationsprogramms. 122

Kapitel 8: Installation von Informatica-Diensten im Konsolenmodus. 123

Installation von Informatica-Diensten - Übersicht.	123
Erstellen einer Domäne.	123
Ausführen des Installationsprogramms.	124
Willkommen beim Informatica-Installationsprogramm.	124
Willkommen – Akzeptieren der allgemeinen Geschäftsbedingungen.	124
Komponentenauswahl.	124
Lizenz und Installationsverzeichnis.	125
Netzwerksicherheit – Dienstprinzipalebene.	126
Network Security - Kerberos Authentication.	126
Domänenauswahl.	127
Domänensicherheit – Sichere Kommunikation.	130
Domain Configuration Repository.	132
Domänensicherheit – Verschlüsselungsschlüssel.	137
Domänen- und Knotenkonfiguration.	138
Konfigurieren von Informatica-Anwendungsdiensten.	141
Konfigurieren der Modellrepository-Datenbank.	142
Datenintegrationsdienst.	146
Konfigurieren der Überwachungsmodellrepository-Datenbank.	148

Parameter und Datenbank des Content-Management-Diensts.	152
Profiling Warehouse Database.	155
PowerCenter-Repository-Dienst und PowerCenter-Integrationsdienst.	158
Anfügen einer Domäne.	159
Ausführen des Installationsprogramms.	159
Willkommen – Akzeptieren der allgemeinen Geschäftsbedingungen.	160
Komponentenauswahl.	160
Voraussetzungen für die Installation.	160
Lizenz und Installationsverzeichnis.	161
Dienstprinzipalebene.	161
Domänenauswahl.	162
Domänensicherheit – Sichere Kommunikation.	163
Domänenkonfiguration.	165
Domänensicherheit – Verschlüsselungsschlüssel.	165
Knotenkonfiguration der hinzuzufügenden Domäne.	166
Port-Konfiguration.	167
Konfigurieren der Modellrepository-Datenbank.	168
Datenintegrationsdienst.	172
PowerCenter-Repository-Dienst und PowerCenter-Integrationsdienst.	173

Kapitel 9: Installation von Informatica-Diensten im Grafikmodus. 175

Übersicht über die Installation der Dienste im Grafikmodus.	175
Erstellen einer Domäne.	175
Ausführen des Installationsprogramms.	175
Willkommen beim Informatica-Installationsprogramm.	176
Willkommen – Akzeptieren der allgemeinen Geschäftsbedingungen.	178
Lizenz und Installationsverzeichnis.	179
Netzwerksicherheit – Dienstprinzipalebene	182
Network Security - Kerberos Authentication.	184
Domänenauswahl.	186
Domänensicherheit – Sichere Kommunikation.	192
Domänenkonfigurations-Repository	194
Domänensicherheit – Verschlüsselungsschlüssel.	197
Domänen- und Knotenkonfiguration.	199
Port-Konfiguration.	202
Windows-Dienstkonfiguration.	204
Konfigurieren der Datenbank des Modellrepository-Diensts.	205
Konfigurieren der Datenbank des Überwachungsmodellrepository-Diensts.	211
Datenintegrationsdienst	214
Parameter und Datenbank des Content-Management-Diensts.	216
Profiling Warehouse Connection Database.	220
PowerCenter-Repository-Dienst und PowerCenter-Integrationsdienst	223
Beitreten zu einer Domäne.	224

Ausführen des Installationsprogramms.	224
Willkommen beim Informatica-Installationsprogramm	225
Willkommen – Akzeptieren der allgemeinen Geschäftsbedingungen	227
Lizenz und Installationsverzeichnis	228
Netzwerksicherheit – Dienstprinzipalebene	231
Network Security - Kerberos Authentication	233
Domänenauswahl	235
Domänensicherheit – Sichere Verbindung.	238
Domänenkonfiguration	240
Domänensicherheit – Verschlüsselungsschlüssel	241
Knotenkonfiguration der hinzuzufügenden Domäne.	242
Port-Konfiguration	244
Windows-Dienstkonfiguration.	246
Konfigurieren der Datenbank des Modellrepository-Diensts	247
Datenintegrationsdienst	253
PowerCenter-Repository-Dienst und PowerCenter-Integrationsdienst	255

Kapitel 10: Ausführen des automatischen Installationsprogramms. 257

Automatische Installation.	257
Konfigurieren der Eigenschaftendatei.	257
Ausführen des Installationsprogramms.	258
Verschlüsseln von Passwörtern in der Eigenschaftendatei.	259

Kapitel 11: Fehlerbehebung 260

Behebung von Problemen bei der Installation - Übersicht.	260
Fortsetzen eines fehlgeschlagenen Installationsprogrammprozesses.	260
Vor dem Fortsetzen des Installationsprogramms.	261
Fortsetzung des Installationsprogramms.	261
Fehlerbehebung bei Installationsprotokolldateien.	262
Debug-Protokolldateien.	262
Dateiinstallations-Protokolldatei.	262
Protokolldateien des Dienstmanagers.	263
Fehlerbehebung von Domänen und Knoten.	263
Erstellen des Domänenkonfigurations-Repository.	264
Erstellen oder Anfügen einer Domäne.	264
Starten von Informatica.	264
Pingen der Domäne.	265
Hinzufügen einer Lizenz.	265
Fehlerbehebung bei Informatica Developer.	265

Teil IV: Nach der Installation der Dienste.....	266
Kapitel 12: Durchführen der Domänenkonfiguration.	267
Checkliste zum Abschließen der Domänenkonfiguration.	267
Durchführen der Domänenkonfiguration - Übersicht.	268
Überprüfen der Gebietsschemaeinstellungen und der Codepage-Kompatibilität.	268
Konfigurieren der Gebietsschema-Umgebungsvariablen.	268
Konfigurieren von Umgebungsvariablen unter UNIX oder Linux.	269
Konfigurieren der Informatica-Umgebungsvariablen.	269
Konfigurieren von Bibliothekspfad-Umgebungsvariablen.	271
Konfigurieren der Kerberos-Umgebungsvariablen.	271
Kapitel 13: Vorbereiten zum Erstellen der Anwendungsdienste.	273
Checkliste zum Vorbereiten der Erstellung von Anwendungsdiensten.	273
Erstellen von Verzeichnissen für den Analyst-Dienst.	274
Erstellen eines Schlüsselspeichers für eine sichere Verbindung zu einem Web-Anwendungsdienst	274
Anmelden Sie bei Informatica Administrator.	275
Fehlerbehebung bei der Anmeldung bei Informatica Administrator.	276
Erstellen von Verbindungen.	276
Eigenschaften von IBM DB2-Verbindungen.	277
Verbindungseigenschaften der Microsoft Azure SQL-Datenbank.	278
Eigenschaften von Microsoft SQL Server-Verbindungen.	279
Eigenschaften für Oracle-Verbindungen.	280
Eigenschaften von PostgreSQL-Verbindungen.	281
Erstellen einer Verbindung.	282
Kapitel 14: Erstellen und Konfigurieren von Anwendungsdiensten.	283
Checkliste zum Erstellen und Konfigurieren von Anwendungsdiensten.	283
Erstellen und Konfigurieren von Anwendungsdiensten – Übersicht.	284
Erstellen und Konfigurieren des Modellrepository-Diensts.	284
Erstellen des Modellrepository-Dienstes.	284
Nach dem Erstellen des Modellrepository-Dienstes.	287
Erstellen und Konfigurieren des Datenintegrationsdiensts.	289
Erstellen des Datenintegrationsdiensts	289
Nach dem Erstellen des Datenintegrationsdienstes.	292
Erstellen und Konfigurieren des PowerCenter-Repository-Dienstes.	293
Erstellen des PowerCenter-Repository-Dienstes	293
Nach dem Erstellen des PowerCenter-Repository-Dienstes.	295
Erstellen und Konfigurieren des PowerCenter-Integrationsdienstes.	297
Erstellen des PowerCenter-Integrationsdienstes.	297
Nach dem Erstellen des PowerCenter-Integrationsdienstes.	299
Erstellen und Konfigurieren des Metadata Manager-Dienstes.	299

Erstellen des Metadata Manager-Dienstes.	299
Nach dem Erstellen des Metadata Manager-Dienstes.	304
Erstellen und Konfigurieren des Content-Management-Dienstes.	304
Erstellen des Content-Management-Dienstes.	304
Erstellen und Konfigurieren des Analyst-Dienstes.	306
Erstellen des Analyst-Dienstes.	306
Nach dem Erstellen des Analyst-Dienstes.	308
Erstellen und Konfigurieren des Suchdienstes.	308
Erstellen des Suchdienstes.	309

Teil V: Installation des Informatica-Client..... 311

Kapitel 15: Installieren der Clients..... 312

Installieren der Clients - Übersicht.	312
Vor dem Installieren.	313
Überprüfen der Prüfsumme des Installationspakets	313
Überprüfen der Systemvoraussetzungen.	313
Überprüfen von Drittanbieteranforderungen für Informatica Developer.	314
Überprüfen von Drittanbieteranforderungen für den PowerCenter Client.	314
Installieren der Clients.	314
Nach der Installation.	315
Installation von Sprachen.	315
Konfigurieren des Client für eine sichere Domäne.	316
Konfigurieren des Workspace-Verzeichnisses für das Developer-Tool.	317
Starten von PowerCenter Client.	318
Starten des Developer Tools.	318

Kapitel 16: Installation im automatischen Modus 320

Übersicht über die Installation im automatischen Modus.	320
Konfigurieren der Eigenschaftendatei.	320
Ausführen des automatischen Installationsprogramms.	321

Teil VI: Deinstallation..... 323

Kapitel 17: Deinstallation..... 324

Deinstallation von Informatica – Übersicht.	324
Regeln und Richtlinien für die Deinstallation.	324
Deinstallieren des Informatica-Servers im Konsolenmodus.	325
Deinstallieren des Informatica-Servers im automatischen Modus.	326
Deinstallieren des Informatica-Servers im Grafikmodus.	326
Deinstallation von Informatica-Clients.	327
Deinstallieren von Informatica-Clients im Grafikmodus.	327
Deinstallieren von Informatica-Clients im automatischen Modus.	327

Anhang A: Starten und Anhalten der Informatica-Dienste.....	329
Starten und Anhalten der Informatica-Dienste - Übersicht	329
Starten oder Beenden der Informatica-Dienste über die Konsole.	330
Beenden von Informatica in Informatica Administrator.	330
Starten oder Beenden von Informatica über die Systemsteuerung.	330
Starten oder Anhalten von Informatica über das Startmenü.	331
Starten bzw. Anhalten von Informatica über eine Eingabeaufforderung.	331
Regeln und Richtlinien zum Starten oder Beenden von Informatica.	331
 Anhang B: Verwalten von Verteilungspaketen.....	 333
Verwaltung von Verteilungspaketen – Übersicht.	333
Vorbereitungen.	333
Installieren oder Entfernen von Verteilungspaketen im Konsolenmodus.	334
Installieren oder Entfernen von Verteilungspaketen im automatischen Modus.	335
Nach der Installation.	336
 Anhang C: Verbinden mit Datenbanken unter UNIX oder Linux.....	 337
Verbinden mit Datenbanken unter UNIX oder Linux – Übersicht.	337
Herstellen einer Verbindung zu einer IBM DB2 Universal-Datenbank.	338
Konfigurieren von nativer Konnektivität.	338
Verbinden zu einer Informix-Datenbank.	340
Konfigurieren der ODBC-Konnektivität.	340
Herstellen einer Verbindung zu einer Microsoft SQL Server-Datenbank.	341
Konfigurieren der SSL-Authentifizierung über ODBC.	341
Konfigurieren von benutzerdefinierten Eigenschaften für Microsoft SQL Server.	342
Herstellen einer Verbindung zu einer Netezza-Datenbank.	342
Konfigurieren der ODBC-Konnektivität.	343
Herstellen einer Verbindung zu einer Oracle-Datenbank.	344
Konfigurieren der nativen Konnektivität.	345
Herstellen einer Verbindung zu einer PostgreSQL-Datenbank.	347
Konfigurieren von nativer Konnektivität.	347
Konfigurieren der ODBC-Konnektivität	349
Verbinden zu einer Sybase ASE-Datenbank.	351
Konfigurieren von nativer Konnektivität.	351
Herstellen einer Verbindung zu einer Teradata-Datenbank.	353
Konfigurieren der ODBC-Konnektivität.	354
Verbinden zu einer JDBC-Datenquelle.	356
Herstellen einer Verbindung zu einer ODBC-Datenquelle.	357
odbc.ini-Beispieldatei.	359
 Anhang D: Verbinden zu Datenbanken unter Windows.....	 366
Verbinden zu Datenbanken unter Windows - Übersicht.	366

Verbinden zu einer IBM DB2 Universal-Datenbank unter Windows.	367
Konfigurieren der nativen Konnektivität.	367
Herstellen einer Verbindung zu einer Informix-Datenbank unter Windows.	368
Konfigurieren der ODBC-Konnektivität.	368
Verbinden mit Microsoft Access und Microsoft Excel unter Windows.	368
Konfigurieren der ODBC-Konnektivität.	368
Verbinden zu einer Microsoft SQL Server-Datenbank Unter Windows.	369
Konfigurieren der nativen Konnektivität.	369
Konfigurieren von benutzerdefinierten Eigenschaften für Microsoft SQL Server.	370
Verbinden zu einer Netezza-Datenbank unter Windows.	371
Konfigurieren der ODBC-Konnektivität.	371
Herstellen einer Verbindung zu einer Oracle-Datenbank unter Windows.	371
Konfigurieren der nativen Konnektivität.	372
Herstellen einer Verbindung zu einer PostgreSQL-Datenbank.	373
Konfigurieren der nativen Konnektivität.	374
Konfigurieren der ODBC-Konnektivität	375
Verbinden zu einer Sybase ASE-Datenbank unter Windows.	375
Konfigurieren von nativer Konnektivität.	375
Herstellen einer Verbindung zu einer Teradata-Datenbank über Windows.	376
Konfigurieren der ODBC-Konnektivität.	377
 Anhang E: Aktualisieren des DynamicSections-Parameters einer DB2-Datenbank.	 378
DynamicSections-Parameter - Übersicht.	378
Einrichten des DynamicSections-Parameters.	378
Herunterladen und Installieren des Dienstprogramms DDconnect JDBC	379
Ausführen des Tests für das JDBC-Tool	379
 Index.	 380

Einleitung

Folgen Sie den Anweisungen in *Installation für PowerCenter und Data Quality*, um Informatica-Dienste und die PowerCenter- und Informatica Data Quality-Produkte zu installieren. Sie können Informatica-Dienste und -Clients auf einer oder mehreren Maschinen installieren. Das Handbuch umfasst erforderliche Aufgaben vor und nach der Installation und Schritte zum Installieren der Informatica-Dienste und -Clients für die Informatica-Domäne. Zu den erforderlichen vorbereitenden Aufgaben zählen das Planen der Umgebung, das Einrichten der Datenbanken und das Überprüfen der Systemvoraussetzungen. Zu den erforderlichen Aufgaben nach der Installation zählen zusätzliche Anwendungsdienste und das Konfigurieren der Umgebungsvariablen.

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 Network

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

Als Mitglied des Informatica Network 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 Network 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.

Für die Suche in 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>

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 ips@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 ein Global Support Center über das Informatica-Netzwerk oder telefonisch kontaktieren.

Um Online-Supportressourcen im Informatica Network zu finden, klicken Sie auf **Support kontaktieren** im Hilfemenü von Informatica Intelligent Cloud Services, um zur Seite **Cloud-Support** zu gelangen. Die Seite **Cloud-Support** enthält Informationen zum Systemstatus und Community-Diskussionen. Melden Sie sich bei Informatica Network an und klicken Sie auf **Benötigen Sie Hilfe**, um zusätzliche Ressourcen zu finden und den globalen Kundensupport von Informatica per E-Mail zu kontaktieren.

Die Telefonnummern für den globalen Kundensupport von Informatica (Informatica Global Customer Support) finden Sie auf der Informatica-Website unter <https://www.informatica.com/services-and-training/support-services/contact-us.html>.

Teil I: Erste Schritte der Installation

- [Erste Schritte der Installation, 16](#)

KAPITEL 1

Erste Schritte der Installation

Dieses Kapitel umfasst die folgenden Themen:

- [Checkliste für die ersten Schritte , 16](#)
- [Installation – Übersicht, 16](#)
- [Installation Prozess, 17](#)
- [Planen der Installationsoption, 18](#)
- [Planen der Installationskomponenten, 19](#)

Checkliste für die ersten Schritte

Dieses Kapitel enthält allgemeine Konzepte und Planungsinformationen im Zusammenhang mit der Installation. Verwenden Sie diese Checkliste zur Überwachung der vorbereitenden Aufgaben.

☐ Verständnis der allgemeinen Konzepte:

- Beschreibung und Prozess des Installationsprogramms.
- Terminologie und Komponenten der Informatica-Domäne.

☐ Allgemeine Planung:

- Installationsoptionen. Schauen Sie sich die Installationsoptionen an, um das Produkt und die Installationsoptionen kennenzulernen.
- Installationskomponenten. Lesen Sie die Beschreibung der Installationskomponenten und der Planungsnotizen.

Installation – Übersicht

Willkommen beim Informatica-Installationsprogramm für Informatica-Domänendienste und -Clients. Die Informatica-Domänendienste bestehen aus Kerndiensten zur Unterstützung der Domänen- und Anwendungsdienste. Die Informatica-Clients bestehen aus Thick-Client- und Webclient-Anwendungen.

Bei der Installation der Informatica-Dienste werden Sie aufgefordert, eine Domäne zu erstellen oder anzufügen. Die Domäne ist eine Zusammenstellung von Knoten, die die Computer darstellen, auf denen die Anwendungsdienste ausgeführt werden. Bei erstmaliger Ausführung des Installationsprogramms müssen Sie die Domäne erstellen. Bei Installation auf einem einzelnen Computer erstellen Sie die Informatica-Domäne und einen Gateway-Knoten auf diesem Computer. Bei Installation auf mehreren Computern erstellen Sie eine

Informatica-Domäne und einen Gateway-Knoten während der ersten Installation. Während der Installation auf den zusätzlichen Computern erstellen Sie Gateway- oder Worker-Knoten, die Sie an die Domäne anfügen.

Wenn Sie das Installationsprogramm ausführen, werden Dateien für Dienste installiert. Während des Installationsvorgangs können Sie optional Anwendungsdienste erstellen. Sie können Anwendungsdienste auch nach Abschluss der Installation manuell erstellen.

Wenn Sie andere Informatica-Produkte installiert haben, überprüfen Sie, ob die installierte Version mit der Version des zu installierenden Produkts kompatibel ist.

Installation Prozess

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

Der Installationsprozess variiert je nach den von Ihnen installierten Produkten. Der Installationsprozess umfasst die folgenden allgemeinen Aufgaben:

Ausführen der Vorinstallationsaufgaben.

1. Planen Sie die Informatica-Installation. Legen Sie die Produkte fest, die in Ihrer Umgebung ausgeführt werden sollen. Wenn Sie eine Domäne erstellen, überlegen Sie sich die Anzahl der Knoten in der Domäne, die auf jedem Knoten ausgeführten Anwendungsdienste, die Systemanforderungen und den von der Domäne verwendeten Typ der Benutzerauthentifizierung.
2. Bereiten Sie die für Repositories, Warehouses und Kataloge benötigten Datenbanken vor. Überprüfen Sie die Datenbankanforderungen und richten Sie die Datenbanken ein.
3. Richten Sie die Computer so ein, dass sie Systemanforderungen erfüllen, damit Sie die Informatica-Dienste erfolgreich installieren und ausführen können.
4. Ermitteln Sie die Sicherheitsanforderungen für die Domäne, Dienste und Datenbanken.

Führen Sie das Installationsprogramm aus.

Wenn Sie das Installationsprogramm ausführen, können Sie auf Basis Ihrer Anforderungen aus unterschiedlichen Optionen auswählen.

Schließen Sie die Konfiguration ab.

1. Überprüfen Sie die Codepage-Kompatibilität.
2. Konfigurieren Sie die Umgebungsvariablen.
3. Führen Sie die Aufgaben aus, die für den von der Domäne verwendeten Typ der Benutzerauthentifizierung erforderlich sind.
4. Optional können Sie die sichere Kommunikation für die Domäne konfigurieren.
5. Erstellen und konfigurieren Sie Anwendungsdienste.
6. Konfigurieren Sie die von den Anwendungsdiensten benötigten Verbindungen.
7. Erstellen Sie die von den Anwendungsdiensten benötigten Benutzer und Verbindungen.

Installieren Sie die Informatica-Client-Tools.

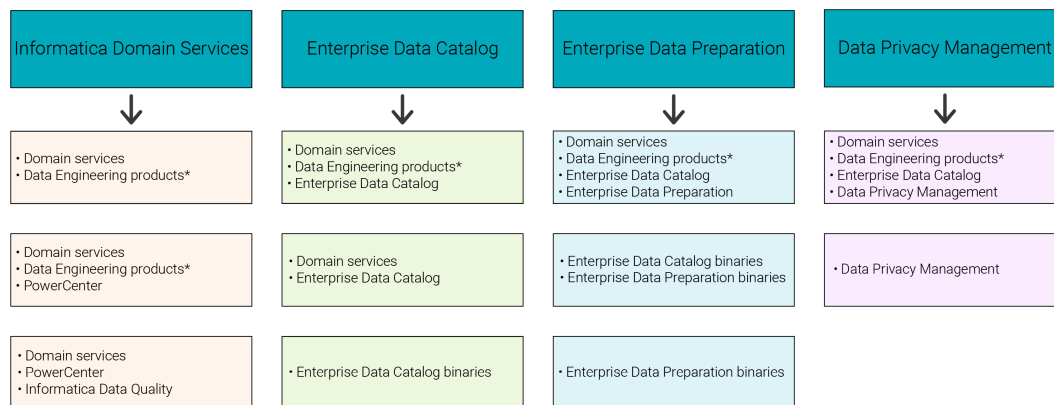
1. Überprüfen Sie die Anforderungen für Installation und Drittanbietersoftware für die Clients.
2. Verwenden Sie das Client-Installationsprogramm zum Installieren auf Windows-Computern.
3. Konfigurieren Sie erforderlichen Umgebungsvariablen und installieren Sie optional weitere Sprachen.

Planen der Installationsoption

Bevor Sie mit der Planung und Vorbereitung der Installation beginnen, bestimmen Sie den Typ der Installation, die Sie ausführen möchten.

Wenn Sie das Installationsprogramm ausführen, können Sie basierend auf dem Produkt oder den Produkten, die Sie installieren möchten, aus den Optionen im Begrüßungsfenster auswählen. Das Fenster „Komponenten“ wird basierend auf Ihrer Produktauswahl angezeigt, damit Sie Produktkomponenten auswählen können.

Die folgende Abbildung zeigt die Produkte, die Sie auf Grundlage der Installationsoptionen installieren können:



*Data Engineering products include Data Engineering Integration, Data Engineering Quality, and Data Engineering Streaming.

Betrachten Sie die verschiedenen Optionen, die beim Ausführen des Installationsprogramms verfügbar sind:

Informatica-Domänendienste

Um die Informatica-Domänendienste zu installieren, können Sie die Installationsoption 1 im Fenster „Komponenten“ auswählen, um Informatica-Domänendienste zu installieren und zu konfigurieren.

Installieren Sie die Informatica-Domänendienste über eine der folgenden Produktoptionen:

- Nur die Data Engineering-Produkte für Integration, Quality und Streaming
- Herkömmliche Produkte und die erwähnten Data Engineering-Produkte
- Nur herkömmliche Produkte wie PowerCenter und Informatica Data Quality

Wenn Sie Informatica-Domänendienste installieren, können Sie wählen, ob Sie eine Domäne erstellen oder eine Domäne anfügen möchten. Test Data Management ist mit herkömmlichen und Data Engineering-Produkten installiert.

Enterprise Data Catalog

Um Enterprise Data Catalog zu installieren, können Sie die Installationsoption 2 im Fenster „Komponenten“ auswählen, um Enterprise Data Catalog zu installieren und zu konfigurieren.

Wählen Sie bei der Installation von Enterprise Data Catalog eine der folgenden Optionen aus:

- Domänendienste, Data Engineering-Produkte und Enterprise Data Catalog
- Domänendienste und Enterprise Data Catalog.
- Nur Enterprise Data Catalog-Binärdateien in einer vorhandenen Domäne Nach der Installation der Binärdateien können Sie das Installationsprogramm erneut ausführen, um die Dienste zu konfigurieren.

Enterprise Data Preparation

Um Enterprise Data Preparation zu installieren, können Sie die Installationsoption 3 im Fenster „Komponenten“ auswählen, um Enterprise Data Preparation zu installieren und zu konfigurieren.

Wählen Sie bei der Installation von Enterprise Data Preparation eine der folgenden Optionen aus:

- Data Engineering-Produkte, Enterprise Data Catalog und Enterprise Data Preparation
- Enterprise Data Catalog- und Enterprise Data Preparation-Binärdateien in einer vorhandenen Domäne
Nach der Installation der Binärdateien können Sie das Installationsprogramm erneut ausführen, um die Dienste zu konfigurieren.
- Nur Enterprise Data Preparation-Binärdateien in einer vorhandenen Domäne mit Enterprise Data Catalog
Nach der Installation der Binärdateien können Sie das Installationsprogramm erneut ausführen, um die Dienste zu konfigurieren.

Data Privacy Management

Um Data Privacy Management zu installieren, können Sie die Installationsoption 4 im Fenster „Komponenten“ auswählen, um Data Privacy Management zu installieren und zu konfigurieren.

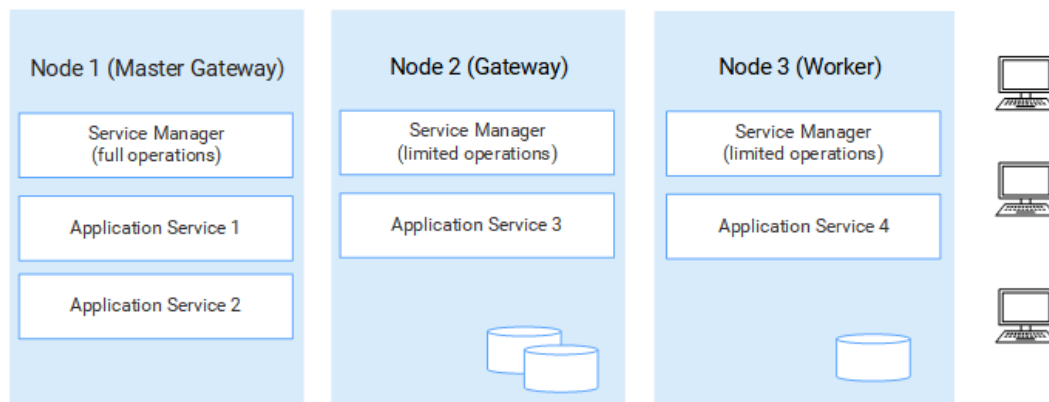
Wählen Sie bei der Installation von Data Privacy Management eine der folgenden Optionen aus:

- Data Engineering-Produkte, Enterprise Data Catalog und Data Privacy Management
- Data Privacy Management in einer vorhandenen Domäne mit Enterprise Data Catalog

Planen der Installationskomponenten

Eine Informatica-Domäne ist eine Zusammenstellung von Knoten und Diensten. Ein Knoten entspricht der logischen Darstellung eines einzelnen Computers in einer Domäne. Die Dienste beinhalten den Dienstmanager, der alle Domänenvorgänge verwaltet, und eine Reihe von Anwendungsdiensten, die serverbasierte Funktionen darstellen. Die Domäne und einige Dienste benötigen Datenbanken, in die sie Metadaten und Laufzeitergebnisse schreiben.

Die folgende Abbildung zeigt die allgemeine Architektur einer Domäne auf mehreren Knoten:



Knoten

Wenn Sie die Domänendienste zum ersten Mal installieren, erstellen Sie die Informatica-Domäne und einen Gateway-Knoten. Wenn Sie die Domänendienste auf anderen Computern installieren, erstellen Sie zusätzliche Knoten, die Sie der Domäne anfügen.

Die Domäne besitzt die folgenden Knotentypen:

- **Gateway-Knoten.** Ein Gateway-Knoten ist ein Knoten, den Sie konfigurieren, damit er als Gateway für die Domäne eingesetzt werden kann. Ein Gateway-Knoten kann Anwendungsdienste ausführen und als Master-Gateway-Knoten eingesetzt werden. Der Master-Gateway-Knoten ist der Eingangspunkt zur Domäne. Sie können mehr als einen Knoten als Gateway-Knoten konfigurieren, es fungiert aber immer nur jeweils ein Gateway-Knoten als Master-Gateway-Knoten.
- **Worker-Knoten.** Ein Worker-Knoten ist ein beliebiger Knoten, den Sie nicht als Gateway für die Domäne konfigurieren. Ein Worker-Knoten kann zwar Anwendungsdienste ausführen, aber nicht als Gateway dienen.

Beim Planen der Installation: Sie müssen die Anzahl und den Typ der Knoten planen, die Sie basierend auf Ihren Dienst- und Verarbeitungsanforderungen benötigen. Wenn Sie hohe Verfügbarkeit benötigen, sollten Sie mehr als einen Gateway-Knoten für Failover-Funktionalität erstellen.

Dienstmanager

Der Dienstmanager ist ein Dienst, der alle Domänenoperationen verwaltet. Der Dienstmanager wird auf jedem Knoten in der Domäne ausgeführt und führt Domänenfunktionen wie Authentifizierung, Protokollierung und Verwaltung von Anwendungsdiensten aus. Auf einem Gateway-Knoten führt der Dienstmanager mehr Aufgaben aus als auf einem Worker-Knoten.

Beim Planen der Installation: Beachten Sie, dass die Funktionalität des Dienstmanagers vom Knotentyp abhängig ist.

Anwendungsdienste

Anwendungsdienste stellen serverbasierte Funktionen dar. Ein Anwendungsdienst kann obligatorisch oder optional sein und benötigt unter Umständen Zugriff auf eine Datenbank.

Bei Ausführung des Installationsprogramms können Sie die Erstellung einiger Dienste festlegen. Nachdem Sie die Installation abgeschlossen haben, erstellen Sie andere Anwendungsdienste basierend auf dem Lizenzschlüssel, der für Ihr Unternehmen generiert wurde.

Beim Planen der Installation: 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.

Datenbanken

Einige Anwendungsdienste erfordern Datenbanken zum Speichern von Metadaten und zum Schreiben von Laufzeitergebnissen. Sie müssen Datenbanken für die Anwendungsdienste in der Domäne erstellen.

Sie können folgende Datenbanken erstellen:

Datenbank des Domänenkonfigurations-Repositorys

Das Domänenkonfigurations-Repository speichert Konfigurations- und Benutzerinformationen aus einer Domäne.

Referenzdaten-Warehouse-Datenbank

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

Datenobjekt-Cache-Datenbank

Der Datenobjekt-Cache speichert zwischengespeicherte logische Datenobjekte und virtuelle Tabellen für den Datenintegrationsdienst. Die Datenobjekt-Zwischenspeicherung aktiviert den Datenintegrationsdienst für den Zugriff auf vorgefertigte logische Datenobjekte und virtuelle Tabellen.

Profiling-Warehouse-Datenbank

Im Profiling-Warehouse werden Profiling- und Scorecard-Ergebnisse gespeichert. Sie benötigen ein Profiling-Warehouse, um Profilerstellung und Datenerkennung durchzuführen.

Arbeitsablauf-Datenbank

In der Arbeitsablauf-Datenbank werden Laufzeitmetadaten für Arbeitsabläufe mithilfe des Datenintegrationsdiensts gespeichert.

Datenbank des Metadata Manager-Repositorys

Das Metadata Manager-Repository ist ein zentraler Speicherort in einer relationalen Datenbank, der Metadaten aus verschiedenen Metadatenquellen speichert. Es speichert auch das Metadata Manager-Warehouse und die Modelle für die einzelnen Metadaten-Quellentypen.

Modellrepository-Datenbank

Das Modellrepository speichert Daten und Metadaten der Informatica-Dienste und -Clients. Informatica-Client-Tools wie das Analyst Tool und das Developer Tool speichern die Daten im Modellrepository.

Überwachungsmodellrepository-Datenbank

Das Überwachungsmodellrepository speichert Statistiken für Ad-hoc-Jobs, Anwendungen, logische Datenobjekte, SQL-Datendienste, Webdienste und Arbeitsabläufe, die von Informatica-Clients und Anwendungsdiensten erstellt wurden.

PowerCenter-Repository-Datenbank

Das PowerCenter-Repository speichert Daten und Metadaten der PowerCenter-Dienste und -Clients. Der PowerCenter-Repository-Dienst verwaltet das Repository und führt alle Metadaten-Transaktionen zwischen der Repository-Datenbank und Repository-Clients aus.

Beim Planen der Installation: Sie müssen die von den Anwendungsdiensten benötigten Datenbanken und Datenbankbenutzer erstellen.

Benutzerauthentifizierung

Wenn Sie das Installationsprogramm ausführen, können Sie auswählen, welche Authentifizierung für die Domäne verwendet werden soll.

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

- **Nativ.** Native Benutzerkonten werden in der Domäne gespeichert und können nur innerhalb der Domäne verwendet werden. Die native Authentifizierung ist der Standard.
- **LDAP.** LDAP-Benutzerkonten werden in einem LDAP-Verzeichnisdienst gespeichert und von Anwendungen innerhalb des Unternehmens gemeinsam verwendet. Sie können die LDAP-Authentifizierung konfigurieren, nachdem Sie das Installationsprogramm ausgeführt haben.

- SAML. SAML-Authentifizierung (Security Assertion Markup Language) können Sie für das Administrator Tool, das Analyst Tool und das Monitoring Tool konfigurieren. Sie können die SAML-Authentifizierung konfigurieren, nachdem Sie das Installationsprogramm ausgeführt haben.
- Kerberos. Kerberos-Benutzerkonten werden in einem LDAP-Verzeichnisdienst gespeichert und von Anwendungen innerhalb des Unternehmens gemeinsam verwendet. Wenn Sie die Kerberos-Authentifizierung während der Installation aktivieren, müssen Sie die Informatica-Domäne für die Arbeit mit dem Kerberos-Schlüsselverteilungszentrum (KDC) konfigurieren.

Beim Planen der Installation: Sie müssen den in der Domäne zu verwendenden Authentifizierungstyp planen. Wenn das Installationsprogramm die Kerberos-Authentifizierung konfigurieren soll, müssen Sie das Netzwerk vor der Installation vorbereiten. Sie können Kerberos auch nach der Installation konfigurieren. Beachten Sie, dass Sie SAML- und Kerberos-Authentifizierung nicht gleichzeitig konfigurieren können.

Sicherer Datenspeicher

Informatica verschlüsselt sensible Daten, bevor diese in den Informatica-Repositorys gespeichert werden.

Wenn Sie eine Domäne erstellen, müssen Sie das Verzeichnis des Verschlüsselungsschlüssels angeben. Das Installationsprogramm generiert eine Verschlüsselungsschlüsseldatei namens `siteKey` und speichert sie in einem Standardverzeichnis oder im von Ihnen angegebenen Verzeichnis. Alle Knoten in einer Domäne müssen denselben Verschlüsselungsschlüssel verwenden.

Wichtig: Das Installationsprogramm generiert auch einen eindeutigen Site-Schlüssel. Wenn Sie den Site-Schlüssel verlieren, können Sie ihn nicht erneut generieren. Speichern Sie unbedingt eine Kopie dieses Schlüssels und teilen Sie den eindeutigen Site-Schlüssel nicht mit anderen.

Domänensicherheit

Wenn Sie eine Domäne erstellen, können Sie Optionen zur Konfiguration der Sicherheit in der Domäne aktivieren.

Für die folgenden Domänenkomponenten können Sie sichere Kommunikation konfigurieren:

- Administrator Tool. Konfigurieren Sie eine sichere HTTPS-Verbindung für das Administrator Tool. Während der Installation können Sie die Schlüsselspeicherdatei für die HTTPS-Verbindung bereitstellen.
- Dienstmanager. Konfigurieren Sie eine sichere Verbindung zwischen dem Dienstmanager und anderen Domänendiensten. Während der Installation können Sie Schlüsselspeicherdateien und Truststore-Dateien bereitstellen, die die zu verwendenden SSL-Zertifikate enthalten.
- Domänenkonfigurations-Repository. Das Domänenkonfigurations-Repository können Sie mit dem SSL-Protokoll sichern. Während der Installation können Sie die Truststore-Datei bereitstellen, die das zu verwendende SSL-Zertifikat enthält.

Beim Planen der Installation: Legen Sie die Sicherheitsstufe fest, die Sie für die Domänenkomponenten konfigurieren möchten. Wenn Sie die Sicherheit für die Domäne konfigurieren, müssen Sie den Speicherort und das Passwort für die Schlüsselspeicher- und Truststore-Dateien kennen. Wenn Sie die Kerberos-Authentifizierung für die Informatica-Domäne verwenden, müssen Sie mit dem Kerberos-Administrator die Benutzer- und Dienstprinzipale einrichten, die für die Domäne erforderlich sind.

Informatica-Client-Tools

Verwenden Sie Informatica-Clients für den Zugriff auf die zugrunde liegende Informatica-Funktionalität in der Domäne. Die Clients senden Anfragen an den Dienstmanager und die Anwendungsdienste.

Die Informatica-Clients bestehen aus Thick-Client-Anwendungen und Thin- oder Web-Client-Anwendungen, die Sie für den Zugriff auf Dienste und Repositories in der Domäne verwenden.

In der folgenden Tabelle werden die Tools für PowerCenter beschrieben:

Informatica Client	Beschreibung
Informatica Developer (das Developer Tool)	Eine Thick-Client-Anwendung zum Erstellen und Ausführen von Datenobjekten, Mappings, Profilen und Arbeitsabläufen.
Informatica Administrator (das Administrator Tool)	Eine Webanwendung zur Verwaltung der Domänen- und Anwendungsdienste.
Informatica Analyst (das Analyst Tool)	Eine Webanwendung zur Analyse, Bereinigung, Integration und Standardisierung von Daten in einem Unternehmen.
PowerCenter-Client	Thick-Client-Anwendung zum Erstellen und Ausführen von Mappings, Sitzungen und Arbeitsabläufen.

Beim Planen der Installation: Legen Sie fest, wie viele Instanzen des PowerCenter Client und des Developer Tools Sie installieren möchten. Die Planung von Web-Client-Anwendungen ist nicht unbedingt erforderlich.

Teil II: Vor Beginn der Installation

Dieser Teil enthält die folgenden Kapitel:

- [Vor der Installation von Diensten unter UNIX oder Linux, 25](#)
- [Vor der Installation der Dienste unter Windows, 40](#)
- [Vorbereiten von Anwendungsdiensten und Datenbanken, 51](#)
- [Vorbereiten der Kerberos-Authentifizierung, 88](#)
- [Aufzeichnen von Informationen für Abfragen des Installationsprogramms, 99](#)
- [Einführung in das Dienste-Installationsprogramm, 110](#)

KAPITEL 2

Vor der Installation von Diensten unter UNIX oder Linux

Dieses Kapitel umfasst die folgenden Themen:

- [VorbereitungenCheckliste , 25](#)
- [Lesen der Versionshinweise, 26](#)
- [Überprüfen der Systemvoraussetzungen, 26](#)
- [Data Transformation-Dateien sichern, 33](#)
- [Konfigurieren von POSIX Asynchronous I/O, 33](#)
- [Überprüfen der Umgebungsvariablen, 34](#)
- [Erstellen eines Systembenutzerkontos, 35](#)
- [Einrichten einer Schlüsselspeicherdatei, 35](#)
- [Installieren von Sprachenschriftarten unter UNIX oder Linux, 37](#)
- [Herunterladen und Extrahieren der Installationsprogrammdateien, 37](#)
- [Überprüfen des Lizenzschlüssels, 39](#)

VorbereitungenCheckliste

In diesem Kapitel werden die vorbereitenden Aufgaben beschrieben, die Sie unbedingt ausführen müssen. Verwenden Sie diese Checkliste, um vorbereitende Aufgaben zu überwachen, bevor Sie die Dienste vorbereiten.

- ☐ Lesen Sie die Informatica-Versionshinweise, um aktuelle Informationen über den Installations- und Upgradeprozess zu erfahren.
- ☐ Überprüfen Sie die Systemvoraussetzungen:
 - Überprüfen Sie die Größenanforderungen abhängig von Ihren Verarbeitungs- und Parallelitätsanforderungen.
 - Überprüfen Sie die Patch-Anforderungen, um sicherzustellen, dass der Computer über die erforderlichen Betriebssystem-Patches und -Bibliotheken verfügt.
 - Stellen Sie sicher, dass die zu verwendenden Portnummern für die Anwendungsdienstprozesse auf den Computern verfügbar sind, auf denen Sie die Informatica-Dienste installieren.

- Überprüfen Sie die Verteilungsanforderungen, um die Informatica-Domäne in die Hadoop- oder Databricks-Umgebung zu integrieren.
- Stellen Sie sicher, dass das Betriebssystem den Grenzwert für den Dateideskriptor erfüllt.
- ☐ Sichern Sie die Data Transformation-Dateien, die in einer früheren Installation erstellt wurden.
- ☐ Prüfen Sie die Systemumgebungsvariablen.
- ☐ Erstellen Sie ein Systembenutzerkonto zur Ausführung des Installationsprogramms.
- ☐ Richten Sie Schlüsselspeicherdateien und Truststore-Dateien ein, wenn Sie für die Domäne eine sichere Kommunikation konfigurieren möchten, und richten Sie eine sichere Verbindung zu Webclientanwendungen ein.
- ☐ Extrahieren Sie die Dateien des Installationsprogramms.
 - Überprüfen Sie die Codesignatur des Installationsprogramms.
 - Überprüfen Sie die Integrität des Installationspakets mit der Prüfsumme.
- ☐ Überprüfen Sie den Lizenzschlüssel.

Lesen der Versionshinweise

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

Suchen Sie die Versionshinweise im Informatica-[documentation portal](#).

Überprüfen der Systemvoraussetzungen

Stellen Sie sicher, dass Ihre Umgebung die minimalen Systemanforderungen für Installation, temporären Festplattenspeicher, Portverfügbarkeit, Datenbanken und Anwendungsdiensthardware erfüllt.

Weitere Informationen zu Produktanforderungen und unterstützten Plattformen finden Sie in der [Product Availability Matrix](#).

Überprüfen von temporärem Speicherplatz und von Berechtigungen

Stellen Sie sicher, dass Ihre Umgebung die Mindestsystemanforderungen für den temporären Festplattenspeicher, Berechtigungen für die temporären Dateien und die Informatica-Client-Tools erfüllt.

Speicherplatz für die temporären Dateien

Das Installationsprogramm schreibt temporäre Dateien auf die Festplatte. Stellen Sie sicher, dass für die Installation 1 GB Speicherplatz auf dem Computer vorhanden ist. Wenn die Installation abgeschlossen ist, werden die temporären Dateien gelöscht und der Speicherplatz wird freigegeben.

In der folgenden Tabelle werden die Mindestanforderungen für Speicherplatz und Arbeitsspeicher für die Installation von PowerCenter- oder Data Engineering-Produkten beschrieben:

Optionen	Mindestanforderungen
Temporärer Speicherplatz zur Ausführung des Installationsprogramms	1 GB Speicherplatz
Installation mit Anwendungsdiensten für Data Engineering-Produkte	50 GB Speicherplatz, 8 GB RAM und 8 Kerne. Von den 50 GB werden 25 GB für die Produktinstallations-Binärdateien benötigt.
Installation mit Anwendungsdiensten für PowerCenter	50 GB Speicherplatz, 4 GB RAM und 6 Kerne. Von den 50 GB Speicherplatz werden 25 GB für die Produktinstallations-Binärdateien benötigt.

Berechtigungen für die temporären Dateien

Vergewissern Sie sich, dass Sie über Lese-, Schreib- und Ausführungsberechtigungen auf das `/tmp`-Verzeichnis verfügen.

Weitere Informationen zu Produktanforderungen und unterstützten Plattformen finden Sie in der [Product Availability Matrix](#).

Überprüfen von Patch-Anforderungen unter UNIX oder Linux

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

PowerCenter unter UNIX

In der folgenden Tabelle finden Sie eine Auflistung der Patches und Bibliotheken, die die Informatica-Dienste für PowerCenter unter UNIX benötigen:

Plattform	Compiler-Version	Betriebssystem	Betriebssystem-Patch
AIX	16	7.3 TL3	Betriebssystemebene: 7300-03 bos.adt.debug Version 7.3.3
AIX	16	7.2 TL5	Betriebssystemebene: 7200-05 bos.adt.debug Version 7.2.5.0

PowerCenter unter Linux

In der folgenden Tabelle finden Sie eine Auflistung der Patches und Bibliotheken, die die Informatica-Dienste für PowerCenter unter Linux benötigen:

Plattform	Betriebssystem	Betriebssystem-Patch
AWS Linux	Linux 2 - 20250417.01	Alle folgenden Pakete: <ul style="list-style-type: none">- e2fsprogs-libs-1.42.9-19.amzn2.x86_64- keyutils-libs-1.5.8-3.amzn2.0.2.x86_64- libsepol-2.5-10.amzn2.0.1.x86_64- libselineux-2.5-12.amzn2.0.2.x86_64
Ubuntu	22.04	Alle folgenden Pakete: <ul style="list-style-type: none">- e2fsprogs/focal, jetzt 1.46.5-2ubuntu1.1 amd64 [installiert]- libkeyutils1/focal, jetzt 1.6.1-2ubuntu3 amd64 [installiert, automatisch]- libselineux1/focal, jetzt 3.3-1build2 amd64 [installiert, automatisch]- libsepol1/focal, jetzt 2.7-1ubuntu0.1 amd64 [installiert, automatisch]
Ubuntu	24.04	Alle folgenden Pakete: <ul style="list-style-type: none">- e2fsprogs/focal, jetzt 1.47.0-2.4~exp1ubuntu4.1 amd64 [installiert]- libkeyutils1/focal, jetzt 1.47.0-2.4~exp1ubuntu4.1 amd64 [installiert, automatisch]- libselineux1/focal, jetzt 3.5-2ubuntu2.1 amd64 [installiert, automatisch]- libsepol2/noble, jetzt 3.5-2build1 amd64 [installiert, automatisch]
Linux-x64	Red Hat Enterprise Linux 7.3	Alle folgenden Pakete, in denen <version> eine beliebige Version des Pakets ist: <ul style="list-style-type: none">- e2fsprogs-libs-<version>.el7- keyutils-libs-<version>.el7- libselineux-<version>.el7- libsepol-<version>.el7
Linux-x64	Red Hat Enterprise Linux 8	Alle folgenden Pakete, in denen <version> eine beliebige Version des Pakets ist: <ul style="list-style-type: none">- e2fsprogs-libs-<Version>.el8- keyutils-libs-<Version>.el8- libselineux-<Version>.el8- libsepol-<Version>.el8
Linux-x64	Red Hat Enterprise Linux 9	Alle folgenden Pakete, in denen <version> eine beliebige Version des Pakets ist: <ul style="list-style-type: none">- e2fsprogs-libs-<version>.el9- keyutils-libs-<version>.el9- libselineux-<version>.el9- libsepol-<version>.el9
Linux-x64	SUSE Linux Enterprise Server 15	Service Pack 7

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 das Installationsprogramm ausführen.

Hinweis: Das Starten von Diensten und Knoten kann bei einem Portkonflikt fehlschlagen.

In der folgenden Tabelle werden die Portanforderungen für die Installation beschrieben:

Port	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. 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-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.
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 hoch sein wie die Zahl der Anwendungsdienstprozesse, die auf dem Knoten ausgeführt werden. Standard ist 6014 bis 6114. Der Dienstmanager weist dem Modellrepository-Dienst dynamisch Portnummern aus diesem Bereich zu.
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: <ul style="list-style-type: none"> - 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 Portkonflikte in der Domäne zu vermeiden.

Beachten Sie beim Festlegen der Portnummern die folgenden Richtlinien:

- Sie müssen für jede Domäne und jede Komponente in der Domäne eine eindeutige Portnummer angeben.
- Die Portnummer für die Domäne und die Domänenkomponenten darf sich nicht im Bereich der Portnummern befinden, die Sie für die Anwendungsdienstprozesse festgelegt.
- 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 Anforderungen an Verteilungspakete(Linux und UNIX)

Sie können Verteilungspakete von Drittanbietern verwenden, um die Informatica-Domäne in die Hadoop- oder Databricks-Umgebung zu integrieren.

Die Informatica-Domäne und der Client benötigen die Integrationspakete, um komplexe Dateien innerhalb der Informatica-Domäne zu verarbeiten oder eine Verbindung zu Hadoop oder Databricks herzustellen, wenn die Verarbeitung innerhalb der Informatica-Domäne stattfindet.

Wenn Sie ein Verteilungspaket benötigen, können Sie es jederzeit über das Installationsprogramm oder über Integration Package Manager (den Paketmanager) installieren.

Sie können das Cloudera CDP Private Cloud-Verteilungspaket verwenden, um komplexe Dateien innerhalb der Informatica-Domäne zu verarbeiten oder eine Verbindung zur Hadoop- oder Databricks-Umgebung herzustellen, die Verarbeitung aber innerhalb der Informatica-Domäne vorzunehmen. Je nach Ihren Anforderungen können Sie jedoch auch ein anderes Verteilungspaket verwenden.

Die folgenden Adapter erfordern Verteilungspakete für die Verarbeitung innerhalb der Informatica-Domäne:

- PowerExchange for Amazon S3
- PowerExchange for Google Cloud Storage
- PowerExchange for Google Cloud Storage for PowerCenter
- PowerExchange for Hadoop for PowerCenter
- PowerExchange for HBase
- PowerExchange for HDFS
- PowerExchange for Hive
- PowerExchange for JDBC V2
- PowerExchange for Kafka for PowerCenter
- PowerExchange for MapR-DB
- PowerExchange for Microsoft Azure Blob Storage
- PowerExchange for Microsoft Azure Data Lake Storage Gen1
- PowerExchange for Microsoft Azure Data Lake Storage Gen2

Überprüfen des Grenzwerts für den Dateideskriptor

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

Informatica-Dienstprozesse können eine hohe Anzahl an Dateien verwenden. Zur Vermeidung von Fehlern, die sich aus der hohen Anzahl an Dateien und Prozessen ergeben, können Sie Systemeinstellungen mithilfe des

Limit-Befehls ändern, wenn Sie eine C-Shell verwenden, oder mithilfe des Ulimit-Befehls, wenn Sie eine Bash-Shell verwenden.

Auflisten von Betriebssystemeinstellungen

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

Führen Sie in der C-Shell `limit` aus.

Führen Sie in der Bash-Shell `ulimit -a` aus.

Festlegen des Grenzwerts für den Dateideskriptor

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

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

Führen Sie in der C-Shell `limit -h filesize <wert>` aus.

Führen Sie in der Bash-Shell `ulimit -n <wert>` aus.

Festlegen von maximalen Benutzerprozessen

Informatica-Dienste verwenden zahlreiche Benutzerprozesse. Verwenden Sie den Befehl „ulimit -u“, um die Einstellung der maximalen Benutzerprozesse hoch genug für alle für die Blaze-Engine erforderlichen Prozesse einzustellen.

Um die maximalen Benutzerprozesse festzulegen, führen Sie den folgenden Befehl aus: Führen Sie den folgenden Befehl aus, um die Einstellung für maximale Benutzerprozesse festzulegen:

Führen Sie in der C-Shell `limit -u processes <wert>` aus.

Führen Sie in der Bash-Shell `ulimit -u <wert>` aus.

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"> - Analyst-Dienst - Content-Management-Dienst - Datenintegrationsdienst - Metadata Manager-Dienst - Modellrepository-Dienst - PowerCenter-Integrationsdienst - PowerCenter-Repository-Dienst - Suchdienst - Webdienst-Hub 	2 CPUs mit mehreren Cores	12 GB	20 GB
Ein Knoten führt die folgenden Dienste aus: <ul style="list-style-type: none"> - Analyst-Dienst - Content-Management-Dienst - Datenintegrationsdienst - Modellrepository-Dienst - Suchdienst 	2 CPUs mit mehreren Cores	12 GB	20 GB
Ein Knoten führt den folgenden Dienst aus: <ul style="list-style-type: none"> - Analyst-Dienst 	1 CPU mit mehreren Cores	4 GB	n/v
Ein Knoten führt den folgenden Dienst aus: <ul style="list-style-type: none"> - Suchdienst 	1 CPU mit mehreren Cores	4 GB	10 GB
Ein Knoten führt die folgenden Dienste aus: <ul style="list-style-type: none"> - Analyst-Dienst - Suchdienst 	1 CPU mit mehreren Cores	4 GB	10 GB
Ein Knoten führt die folgenden Dienste aus: <ul style="list-style-type: none"> - Metadata Manager-Dienst - PowerCenter-Integrationsdienst - PowerCenter-Repository-Dienst 	2 CPUs mit mehreren Cores	8 GB	10 GB
Ein Knoten führt die folgenden Dienste aus: <ul style="list-style-type: none"> - Metadata Manager-Dienst - PowerCenter-Integrationsdienst - PowerCenter-Repository-Dienst 	2 CPUs mit mehreren Cores	8 GB	10 GB
Ein Knoten führt die folgenden Dienste aus: <ul style="list-style-type: none"> - PowerCenter-Integrationsdienst - PowerCenter-Repository-Dienst 	1 CPU mit mehreren Cores	4 GB	10 GB
Ein Knoten führt die folgenden Dienste aus: <ul style="list-style-type: none"> - Datenintegrationsdienst - Modellrepository-Dienst 	1 CPU mit mehreren Cores	4 GB	10 GB
Ein Knoten führt die folgenden Dienste aus: <ul style="list-style-type: none"> - Datenintegrationsdienst - Content-Management-Dienst 	1 CPU mit mehreren Cores	4 GB	10 GB
Ein Knoten führt den folgenden Dienst aus: <ul style="list-style-type: none"> - Metadata Manager-Dienst 	1 CPU mit mehreren Cores	4 GB	10 GB

Dienste	Prozessor	Speicherkapazität	Festplattenspeicher
Ein Knoten führt die folgende Dienstkomponente aus: - Metadata Manager-Agent	1 CPU mit mehreren Cores	4 GB	400 MB
Ein Knoten führt den folgenden Dienst aus: - Webdienst-Hub	1 CPU mit mehreren Cores	4 GB	5 GB

Data Transformation-Dateien sichern

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

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

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

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

Konfigurieren von POSIX Asynchronous I/O

Machen Sie POSIX Asynchronous I/O bei der Installation von Informatica auf IBM AIX auf allen Konten verfügbar, auf denen Sie einen PowerCenter Integration Service ausführen möchten. Wenn POSIX Asynchronous I/O nicht verfügbar ist, kann ein auf einem IBM AIX-Rechner ausgeführter PowerCenter Integration Service möglicherweise nicht gestartet werden.

Hinweis: Ab Version 10.5.7 wird die Unterstützung für AIX-Installationsprogramme zurückgestellt und ist nicht verfügbar.

Überprüfen der Umgebungsvariablen

Konfigurieren Sie Umgebungsvariablen für die Informatica-Installation.

In der folgenden Tabelle werden die zu überprüfenden Umgebungsvariablen beschrieben:

Variable	Beschreibung
IATEMPDIR	<p>Der Speicherort der während der Installation erstellten temporären Dateien. Informatica benötigt 1 GB Speicherplatz auf der Festplatte für temporäre Dateien.</p> <p>Konfigurieren Sie die Umgebungsvariable, wenn keine temporären Dateien im Verzeichnis <code>/tmp</code> erstellt werden sollen.</p> <p>Wenn Sie das Standardverzeichnis <code>/tmp</code> ändern möchten, müssen Sie die Umgebungsvariablen IATEMPDIR und _JAVA_OPTIONS auf das neue Verzeichnis festlegen.</p> <p>Legen Sie die Variable beispielsweise so fest, dass „IATEMPDIR=/home/user“ exportiert wird.</p> <p>Hinweis: Heben Sie die Festlegung der Variablen IATEMPDIR nach der Installation auf.</p>
_JAVA_OPTIONS	<p>Konfigurieren Sie die Umgebungsvariable, um das temporäre Verzeichnis zu ändern.</p> <p>Wenn Sie das Standardverzeichnis <code>/tmp</code> ändern möchten, müssen Sie die Umgebungsvariablen IATEMPDIR und _JAVA_OPTIONS auf das neue Verzeichnis festlegen.</p> <p>Legen Sie die Variable beispielsweise so fest, dass <code>_JAVA_OPTIONS=-Djava.io.tmpdir=/home/user</code> exportiert wird.</p> <p>Hinweis: Heben Sie die Festlegung der Variablen _JAVA_OPTIONS nach der Installation auf.</p>
LANG und LC_ALL	<p>Ändern Sie das Gebietsschema, um die korrekte Zeichenkodierung für die Terminalsitzung festzulegen. Legen Sie zum Beispiel die Kodierung auf <code>Latin1</code> oder <code>ISO-8859-1</code> für Französisch, <code>EUC-JP</code> oder <code>UMSCHALT JIS</code> für Japanisch oder <code>UTF-8</code> für Chinesisch oder Koreanisch fest. Die Zeichenkodierung legt die Arten von Zeichen fest, die auf dem UNIX-Terminal angezeigt werden.</p>
DISPLAY	<p>Setzen Sie die DISPLAY-Umgebung zurück, bevor Sie das Installationsprogramm ausführen. Die Installation schlägt möglicherweise fehl, wenn die DISPLAY-Umgebungsvariable einen Wert aufweist.</p>
SKIP_VENDOR_CHECK	<p>Konfigurieren Sie die Umgebungsvariable, um die sudo-Eingabeaufforderung aus dem Installationsprogramm unter Linux oder AIX zu entfernen.</p> <p>Legen Sie die Umgebungsvariable auf „true“ fest, um die sudo-Eingabeaufforderung aus der Informatica-Serverinstallation unter Linux oder AIX zu entfernen.</p> <p>Hinweis: Wenn Sie keine sudo-Berechtigungen haben, legen Sie die Umgebungsvariable auf „true“ fest, bevor Sie das Installationsprogramm ausführen. Wenn Sie über sudo-Berechtigungen verfügen, müssen Sie die Umgebungsvariable nicht festlegen.</p>

Hinweis: Stellen Sie sicher, dass das Flag NOEXEC nicht für das Dateisystem festgelegt ist, das auf dem Verzeichnis `/tmp` gemountet ist. Ab Version 10.5.7 wird die Unterstützung für AIX-Installationsprogramme zurückgestellt und ist nicht verfügbar.

Erstellen eines Systembenutzerkontos

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

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

Vergewissern Sie sich, dass das Benutzerkonto, mit dem der Informatica-Dienst installiert wird, keine Berechtigungen für den Zugriff auf vertrauliche Dateien auf dem Computer hat, auf dem Sie die Informatica-Dienste installieren.

Einrichten einer Schlüsselspeicherdatei

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

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

keytool

Mithilfe von keytool können Sie ein SSL-Zertifikat oder einen CSR (Certificate Signing Request) sowie Schlüsselspeicherdateien und Truststore-Dateien im JKS-Format verwenden erstellen.

OpenSSL

Sie können OpenSSL zum Erstellen eines SSL-Zertifikats oder CSR verwenden sowie einen Schlüsselspeicher im JKS-Format in das PEM-Format konvertieren.

Weitere Informationen zu OpenSSL finden Sie in der Dokumentation auf der folgenden Website:

<https://www.openssl.org/docs/>

Um ein höheres Sicherheitsniveau zu erreichen, senden Sie Ihre CSR an eine Zertifizierungsstelle, um ein signiertes Zertifikat zu erhalten.

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

Sichere Kommunikation innerhalb der Informatica-Domäne

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

Sie haben eine Zertifikatssignieranfrage und einen privaten Schlüssel erstellt.

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

Beachten Sie, dass für die RSA-Verschlüsselung mehr als 512 Bit erforderlich sind.

Sie haben ein signiertes SSL-Zertifikat.

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

Sie haben das Zertifikat in Schlüsselspeicher importiert.

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

Die Schlüsselspeicherdateien müssen die Root- und SSL-Zwischenzertifikate enthalten.

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

Sie haben das Zertifikat in Truststores importiert.

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

Die Truststore-Dateien müssen die Root-, Zwischen- und Endbenutzer-SSL-Zertifikate enthalten.

Die Schlüsselspeicherdateien und Truststore-Dateien befinden sich im richtigen Verzeichnis.

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

Der für das Administrator Tool verwendete Schlüsselspeichertyp bestimmt die Schlüsselspeichertypen für den Content-Management-Dienst.

Bei Verwendung des standardmäßigen Schlüsselspeicherzertifikats für das Administrator Tool können Sie entweder das standardmäßige oder ein benutzerdefiniertes Schlüsselspeicherzertifikat für den Content-Management-Dienst verwenden.

Bei Verwendung eines benutzerdefinierten Schlüsselspeicherzertifikats für das Administrator Tool müssen Sie ein benutzerdefiniertes Schlüsselspeicherzertifikat für den Content-Management-Dienst verwenden.

Weitere Informationen zum Erstellen eines benutzerdefinierten Schlüsselspeichers und Truststores finden Sie unter

[Informatica How-To Library article "How to Create Keystore and Truststore Files for Secure Communication in the Informatica Domain"](#).

Sichere Verbindung zum Administrator-Tool

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

Sie haben eine Zertifikatssignieranfrage und einen privaten Schlüssel erstellt.

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

Beachten Sie, dass für die RSA-Verschlüsselung mehr als 512 Bit erforderlich sind.

Sie haben ein signiertes SSL-Zertifikat.

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

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

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

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

Der Schlüsselspeicher befindet sich im richtigen Verzeichnis.

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

Installieren von Sprachenschriftarten unter UNIX oder Linux

Ab Version 10.5.7 verwenden Informatica-Server- und Clientanwendungen Version 11 des Azul Java Development Kit (JDK). Azul Zulu bündelt die physischen Schriftarten, die im JDK 11 enthalten sind, nicht. Bevor Sie die Domäne aktualisieren, stellen Sie sicher, dass die Sprachenschriftarten auf dem Linux-Computer installiert sind, auf dem der Knoten gehostet wird. Laden Sie die Sprachenschriftarten herunter und installieren Sie sie auf der Root-Ebene mit den Benutzeranmeldeinformationen für `sudo`.

Um die auf den Linux-Computern installierten Schriftarten zu überprüfen, führen Sie die Befehle `fc-match` und `fc-list` aus.

Um ein bestimmtes fontconfig-Paket zu installieren, führen Sie den folgenden Befehl basierend auf der Linux-Distribution aus:

- **Red Hat Enterprise Linux (RHEL) oder CentOS Stream**

```
sudo yum install fontconfig dejavu-sans-fonts dejavu-serif-fonts
```

Der Befehl installiert das fontconfig-Paket und die DejaVu-Schriftfamilien sans und serif auf einem Linux-System mit dem yum-Paketmanager.

- **SUSE Linux Enterprise (SLES)**

```
sudo zypper install dejavu-fonts fontconfig
```

Der Befehl installiert die DejaVu-Schriftfamilie und die fontconfig-Bibliothek auf einem Linux-System mit dem zypper-Paketmanager.

Herunterladen und Extrahieren der Installationsprogrammdateien

Die Installationsdateien werden als komprimierte Dateien verteilt. Sie können die Informatica-Installationsdatei und die Verteilungspakete über den FTP-Link abrufen, der in Ihrer Erfüllung-E-Mail enthalten ist.

Laden Sie die Informatica-TAR-Installationsdatei und die ZIP-Dateien des erforderlichen Verteilungspakets von der Informatica Electronic Software-Download-Site herunter. Sie können sie in ein lokales Verzeichnis oder ein freigegebenes Netzlaufwerk herunterladen, das Ihrem Computer zugeordnet ist.

Um andere komprimierte Dateien und Dienstprogramme herunterzuladen, stellen Sie eine Versandanfrage an den globalen Kundensupport von Informatica.

Extrahieren Sie die Dateien des Installationsprogramms in ein Verzeichnis auf Ihrem Computer. Der Benutzer, der das Installationsprogramm ausführt, muss über Lese- und Schreibberechtigungen für das Verzeichnis der Installationsdateien sowie über Ausführungsberechtigungen für die ausführbare Datei verfügen.

Hinweis: Stellen Sie sicher, dass Sie die Installationsdateien in ein lokales Verzeichnis extrahieren, da Sie das Installationsprogramm nicht aus einer zugeordneten Datei ausführen können.

Kopieren Sie die ZIP-Dateien der Verteilungspakete an den folgenden Speicherort: `<Informatica-Installationsprogrammdateien>/source`

Hinweis: Das Installationsprogramm schlägt fehl, wenn die ZIP-Dateien für Verteilungspakete nicht im Quellverzeichnis verfügbar sind.

Überprüfen der Codesignatur des Installationsprogramms

Sie können die Signatur des Informatica-Softwarecodes überprüfen.

Informatica verwendet eine zertifikatsbasierte digitale Signatur, um den Informatica-Softwarecode zu signieren. Die Codesignatur hilft, die Authentizität des Codes zu überprüfen, und stellt sicher, dass der Code nicht geändert oder beschädigt wird, nachdem Informatica den Code signiert hat. Sie können festlegen, ob Sie der Software vertrauen, basierend darauf, ob die Codesignatur vorhanden ist oder nicht.

Sie können ein Codesignaturzertifikat anfordern, das Informationen, mit denen Informatica LLC vollständig identifiziert wird, und die Zertifizierungsstelle enthält, die das Zertifikat ausstellt. Das digitale Zertifikat bindet die Identität von Informatica an einen öffentlichen Schlüssel und an einen privaten Schlüssel.

Die digitale Signierung von Software beginnt mit der Erstellung eines kryptografischen Hash-Werts oder eines Digests. Der Digest hat eine Eins-zu-Eins-Entsprechung mit den Originaldaten. Verwenden Sie den Digest, da es keine Hinweise zur Wiederherstellung der Originaldaten gibt und schon eine kleine Änderung der Originaldaten zu einer Änderung des Hash-Werts führt. Informatica verwendet seinen privaten Schlüssel zum Signieren des Digests oder erzeugt eine Signatur in Form einer Bitfolge. Gute Algorithmen für digitale Signaturen ermöglichen es einem Benutzer mit dem öffentlichen Schlüssel, den Ersteller der Signatur zu verifizieren.

So überprüfen Sie, ob der signierte Code authentisch ist

Nachdem Informatica das Softwarepaket signiert hat, können Sie sich an den globalen Kundensupport von Informatica wenden, um auf das Codesignaturzertifikat zuzugreifen. Informatica liefert das Installationsprogramm zusammen mit der Signaturdatei aus, die den Hash der Binärdatei des Installationsprogramms enthält, die mit dem privaten Schlüssel von Informatica verschlüsselt ist. Sie können die Integrität digital signierter Binärdateien mit allen verfügbaren Tools verifizieren, z. B. mit OpenSSL.

Wenn Sie beispielsweise die Paketauthentifizierung überprüfen und die Codesicherheit bestätigen müssen, geben Sie die folgenden OpenSSL-Befehle ein:

```
openssl base64 -d -in $signature -out /tmp/sign.sha256
openssl dgst -sha256 -verify <(openssl x509 -in <cert> -pubkey -noout) -signature /tmp/
sign.sha256 <file>
```

Wobei `<Signatur>` die Datei ist, die die Signatur in Base64 enthält, `<Zertifikat>` das Codesignaturzertifikat ist, und `<Datei>` die zu verifizierende Datei ist.

Basierend auf dem Überprüfungsprozess zeigt OpenSSL eine Erfolgs- oder Fehlermeldung an, um zu bestätigen, ob der Installationsprogrammcode echt ist oder nicht. Beachten Sie, dass die Überprüfung für das Installationsprogramm etwa zwei Minuten dauern kann.

Überprüfen der Prüfsumme des Installationspakets unter UNIX und Linux

Bevor Sie das Installationsprogramm für Dienste ausführen, überprüfen Sie die Integrität des Installationspakets mit dem Befehl „cksum“. Mit dem Befehl „cksum“ wird der Prüfsummenwert für die Installationsprogramme berechnet.

Vergleichen Sie die Prüfsumme für die spezifischen Installationsdateien mit der Prüfsumme der Installationsdateien, die von der Informatica Electronic Software-Download-Site heruntergeladen wurden.

In der folgenden Tabelle werden die Prüfsumme und Dateigröße des Installationsprogramms der Informatica-Dienste für UNIX und Linux aufgelistet:

Datei	Prüfsummenwert	Dateigröße
informatica_1059_server_linux-x64.tar	1877917307	16460503040 Byte
informatica_1059_server_aix-ppc64.tar	2768966257	12369950720 Byte

Ein Prüfsummenkonflikt kann auftreten, wenn es während des Downloads aufgrund von Netzwerkproblemen zu Datenfehlern kommt oder wenn Daten in der Datei auf der Festplatte beschädigt werden. Weitere Informationen zu Prüfsummenfehlern finden Sie unter

[HOW TO: Identify file errors after downloading Informatica installation files.](#)

Überprüfen des Lizenzschlüssels

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

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

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

KAPITEL 3

Vor der Installation der Dienste unter Windows

Dieses Kapitel umfasst die folgenden Themen:

- [Vor der Installation der Dienste unter Windows - Übersicht, 40](#)
- [Lesen der Versionshinweise, 40](#)
- [Überprüfen der Systemvoraussetzungen, 41](#)
- [Data Transformation-Dateien sichern, 45](#)
- [Überprüfen der Umgebungsvariablen, 46](#)
- [Erstellen eines Systembenutzerkontos, 46](#)
- [Einrichten von Schlüsselspeicher- und Truststore-Dateien, 47](#)
- [Herunterladen und Extrahieren der Installationsprogrammdateien, 49](#)
- [Überprüfen des Lizenzschlüssels, 50](#)

Vor der Installation der Dienste unter Windows - Übersicht

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

Lesen der Versionshinweise

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

Suchen Sie die Versionshinweise im Informatica-[documentation portal](#).

Überprüfen der Systemvoraussetzungen

Stellen Sie sicher, dass Ihre Umgebung die minimalen Systemanforderungen für Installation, temporären Festplattenspeicher, Portverfügbarkeit, Datenbanken und Anwendungsdiensthardware erfüllt.

Weitere Informationen zu Produktanforderungen und unterstützten Plattformen finden Sie in der [Product Availability Matrix](#).

Überprüfen von temporärem Speicherplatz und von Berechtigungen

Stellen Sie sicher, dass Ihre Umgebung die Mindestsystemanforderungen für den temporären Festplattenspeicher, Berechtigungen für die temporären Dateien und die Informatica-Client-Tools erfüllt.

Speicherplatz für die temporären Dateien

Das Installationsprogramm schreibt temporäre Dateien auf die Festplatte. Stellen Sie sicher, dass für die Installation 1 GB Speicherplatz auf dem Computer vorhanden ist. Wenn die Installation abgeschlossen ist, werden die temporären Dateien gelöscht und der Speicherplatz wird freigegeben.

In der folgenden Tabelle werden die Mindestanforderungen für Speicherplatz und Arbeitsspeicher für die Installation von PowerCenter- oder Data Engineering-Produkten beschrieben:

Optionen	Mindestanforderungen
Temporärer Speicherplatz zur Ausführung des Installationsprogramms	1 GB Speicherplatz
Installation mit Anwendungsdiensten für Data Engineering-Produkte	50 GB Speicherplatz, 8 GB RAM und 8 Kerne. Von den 50 GB werden 25 GB für die Produktinstallations-Binärdateien benötigt.
Installation mit Anwendungsdiensten für PowerCenter	50 GB Speicherplatz, 4 GB RAM und 6 Kerne. Von den 50 GB Speicherplatz werden 25 GB für die Produktinstallations-Binärdateien benötigt.

Berechtigungen für die temporären Dateien

Vergewissern Sie sich, dass Sie über Lese-, Schreib- und Ausführungsberechtigungen auf das `/tmp`-Verzeichnis verfügen.

Weitere Informationen zu Produktanforderungen und unterstützten Plattformen finden Sie in der [Product Availability Matrix](#).

Überprüfen der Patchanforderungen

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

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

Plattform	Betriebssystem	Betriebssystem-Patch
Windows 2019	2019 64 Bit	Nicht erforderlich
Windows 2022	2022 64 Bit	Nicht erforderlich
Windows 2025	2025 64 Bit	Nicht erforderlich

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 das Installationsprogramm ausführen.

Hinweis: Das Starten von Diensten und Knoten kann bei einem Portkonflikt fehlschlagen.

In der folgenden Tabelle werden die Portanforderungen für die Installation beschrieben:

Port	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. 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-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.

Port	Beschreibung
Höchste Portnummer	Höchste Portnummer des dynamischen Portnummernbereichs, die den Anwendungsdienstprozessen, die auf diesem Knoten laufen, zugewiesen werden kann. Standardwert ist 6114.
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 hoch sein wie die Zahl der Anwendungsdienstprozesse, die auf dem Knoten ausgeführt werden. Standard ist 6014 bis 6114. Der Dienstmanager weist dem Modellrepository-Dienst dynamisch Portnummern aus diesem Bereich zu.
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: <ul style="list-style-type: none"> - 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 Portkonflikte in der Domäne zu vermeiden.

Beachten Sie beim Festlegen der Portnummern die folgenden Richtlinien:

- Sie müssen für jede Domäne und jede Komponente in der Domäne eine eindeutige 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 Anforderungen an Verteilungspakete (Windows)

Die Informatica-Domäne und der Client benötigen die Integrationspakete, um komplexe Dateien innerhalb der Informatica-Domäne zu verarbeiten oder eine Verbindung zu Hadoop oder Databricks herzustellen, wenn die Verarbeitung innerhalb der Informatica-Domäne stattfindet.

Wenn Sie ein Verteilungspaket benötigen, können Sie es jederzeit über das Installationsprogramm oder über Integration Package Manager (den Paketmanager) installieren.

Sie können das Cloudera CDP Private Cloud-Verteilungspaket verwenden, um komplexe Dateien innerhalb der Informatica-Domäne zu verarbeiten oder eine Verbindung zur Hadoop- oder Databricks-Umgebung herzustellen, die Verarbeitung aber innerhalb der Informatica-Domäne vorzunehmen. Je nach Ihren Anforderungen können Sie jedoch auch ein anderes Verteilungspaket verwenden.

Die folgenden Adapter erfordern Verteilungspakete für die Verarbeitung innerhalb der Informatica-Domäne:

- PowerExchange for Amazon S3
- PowerExchange for Google Cloud Storage

- PowerExchange for Google Cloud Storage for PowerCenter
- PowerExchange for Kafka for PowerCenter
- PowerExchange for Microsoft Azure Blob Storage
- PowerExchange for Microsoft Azure Data Lake Storage Gen1
- PowerExchange for Microsoft Azure Data Lake Storage Gen2

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"> - Analyst-Dienst - Content-Management-Dienst - Datenintegrationsdienst - Metadata Manager-Dienst - Modellrepository-Dienst - PowerCenter-Integrationsdienst - PowerCenter-Repository-Dienst - Suchdienst - Webdienst-Hub 	2 CPUs mit mehreren Cores	12 GB	20 GB
Ein Knoten führt die folgenden Dienste aus: <ul style="list-style-type: none"> - Analyst-Dienst - Content-Management-Dienst - Datenintegrationsdienst - Modellrepository-Dienst - Suchdienst 	2 CPUs mit mehreren Cores	12 GB	20 GB
Ein Knoten führt den folgenden Dienst aus: <ul style="list-style-type: none"> - Analyst-Dienst 	1 CPU mit mehreren Cores	4 GB	n/v
Ein Knoten führt den folgenden Dienst aus: <ul style="list-style-type: none"> - Suchdienst 	1 CPU mit mehreren Cores	4 GB	10 GB
Ein Knoten führt die folgenden Dienste aus: <ul style="list-style-type: none"> - Analyst-Dienst - Suchdienst 	1 CPU mit mehreren Cores	4 GB	10 GB

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

Data Transformation-Dateien sichern

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

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

Datei oder Verzeichnis	Standardspeicherort
Repository	<Informatica-Installationsverzeichnis>\DataTransformation\ServiceDB
Custom Global Components-Verzeichnis (TGP-Dateien)	<Informatica-Installationsverzeichnis>\DataTransformation\autoInclude\user

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

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

Überprüfen der Umgebungsvariablen

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

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

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

Erstellen eines Systembenutzerkontos

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

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

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

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

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

Einrichten von Schlüsselspeicher- und Truststore-Dateien

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

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

Keytool

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

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

OpenSSL

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

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

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

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

Sichere Kommunikation innerhalb der Informatica-Domäne

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

Sie haben eine Zertifikatssignieranfrage und einen privaten Schlüssel erstellt.

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

Beachten Sie, dass für die RSA-Verschlüsselung mehr als 512 Bit erforderlich sind.

Sie haben ein signiertes SSL-Zertifikat.

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

Sie haben das Zertifikat in Schlüsselspeicher importiert.

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

Die Schlüsselspeicherdateien müssen die Root- und SSL-Zwischenzertifikate enthalten.

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

Sie haben das Zertifikat in Truststores importiert.

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

Die Truststore-Dateien müssen die Root-, Zwischen- und Endbenutzer-SSL-Zertifikate enthalten.

Die Schlüsselspeicher und Truststores befinden sich im richtigen Verzeichnis.

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

Sichere Verbindung zum Administrator Tool

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

Sie haben eine Zertifikatssignieranfrage und einen privaten Schlüssel erstellt.

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

Beachten Sie, dass für die RSA-Verschlüsselung mehr als 512 Bit erforderlich sind.

Sie haben ein signiertes SSL-Zertifikat.

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

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

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

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

Der Schlüsselspeicher befindet sich im richtigen Verzeichnis.

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

Herunterladen und Extrahieren der Installationsprogrammdateien

Die Installationsdateien werden als komprimierte Dateien verteilt. Sie können die Informatica-Installationsdatei und die Verteilungspakete über den FTP-Link abrufen, der in Ihrer Erfüllungs-E-Mail enthalten ist.

Laden Sie die Informatica-TAR-Installationsdatei und die ZIP-Dateien des erforderlichen Verteilungspakets von der Informatica Electronic Software-Download-Site herunter. Sie können sie in ein lokales Verzeichnis oder ein freigegebenes Netzlaufwerk herunterladen, das Ihrem Computer zugeordnet ist.

Um andere komprimierte Dateien und Dienstprogramme herunterzuladen, stellen Sie eine Versandanfrage an den globalen Kundensupport von Informatica.

Extrahieren Sie die Dateien des Installationsprogramms in ein Verzeichnis auf Ihrem Computer. Der Benutzer, der das Installationsprogramm ausführt, muss über Lese- und Schreibberechtigungen für das Verzeichnis der Installationsdateien sowie über Ausführungsberechtigungen für die ausführbare Datei verfügen.

Hinweis: Stellen Sie sicher, dass Sie die Installationsdateien in ein lokales Verzeichnis extrahieren, da Sie das Installationsprogramm nicht aus einer zugeordneten Datei ausführen können.

Kopieren Sie die ZIP-Dateien der Verteilungspakete an den folgenden Speicherort: <Informatica-Installationsprogrammdateien>/source

Hinweis: Das Installationsprogramm schlägt fehl, wenn die ZIP-Dateien für Verteilungspakete nicht im Quellverzeichnis verfügbar sind.

Überprüfen der Codesignatur des Installationsprogramms

Sie können die Signatur des Informatica-Softwarecodes überprüfen.

Informatica verwendet eine zertifikatsbasierte digitale Signatur, um den Informatica-Softwarecode zu signieren. Die Codesignatur hilft, die Authentizität des Codes zu überprüfen, und stellt sicher, dass der Code nicht geändert oder beschädigt wird, nachdem Informatica den Code signiert hat. Sie können festlegen, ob Sie der Software vertrauen, basierend darauf, ob die Codesignatur vorhanden ist oder nicht.

Sie können ein Codesignaturzertifikat anfordern, das Informationen, mit denen Informatica LLC vollständig identifiziert wird, und die Zertifizierungsstelle enthält, die das Zertifikat ausstellt. Das digitale Zertifikat bindet die Identität von Informatica an einen öffentlichen Schlüssel und an einen privaten Schlüssel.

Die digitale Signierung von Software beginnt mit der Erstellung eines kryptografischen Hash-Werts oder eines Digests. Der Digest hat eine Eins-zu-Eins-Entsprechung mit den Originaldaten. Verwenden Sie den Digest, da es keine Hinweise zur Wiederherstellung der Originaldaten gibt und schon eine kleine Änderung der Originaldaten zu einer Änderung des Hash-Werts führt. Informatica verwendet seinen privaten Schlüssel zum Signieren des Digests oder erzeugt eine Signatur in Form einer Bitfolge. Gute Algorithmen für digitale Signaturen ermöglichen es einem Benutzer mit dem öffentlichen Schlüssel, den Ersteller der Signatur zu verifizieren.

So überprüfen Sie, ob der signierte Code authentisch ist

Nachdem Informatica das Softwarepaket signiert hat, können Sie sich an den globalen Kundensupport von Informatica wenden, um auf das Codesignaturzertifikat zuzugreifen. Informatica liefert das Installationsprogramm zusammen mit der Signaturdatei aus, die den Hash der Binärdatei des Installationsprogramms enthält, die mit dem privaten Schlüssel von Informatica verschlüsselt ist. Sie können die Integrität digital signierter Binärdateien mit allen verfügbaren Tools verifizieren, z. B. mit OpenSSL.

Wenn Sie beispielsweise die Paketauthentifizierung überprüfen und die Codesicherheit bestätigen müssen, geben Sie die folgenden OpenSSL-Befehle ein:

```
openssl base64 -d -in $signature -out /tmp/sign.sha256
openssl dgst -sha256 -verify <(openssl x509 -in <cert> -pubkey -noout) -signature /tmp/
sign.sha256 <file>
```

Wobei <Signatur> die Datei ist, die die Signatur in Base64 enthält, <Zertifikat> das Codesignaturzertifikat ist, und <Datei> die zu verifizierende Datei ist.

Basierend auf dem Überprüfungsprozess zeigt OpenSSL eine Erfolgs- oder Fehlermeldung an, um zu bestätigen, ob der Installationsprogrammcode echt ist oder nicht. Beachten Sie, dass die Überprüfung für das Installationsprogramm etwa zwei Minuten dauern kann.

Überprüfen der Prüfsumme des Installationspakets unter Windows

Überprüfen Sie vor der Ausführung des Installationsprogramms für die Dienste mit dem Befehl „cksum“ die Integrität des Installationspakets. Mit dem Befehl „cksum“ wird der Prüfsummenwert für das Installationsprogramm berechnet.

Vergleichen Sie die Prüfsumme für die spezifischen Installationsdateien mit der Prüfsumme der Installationsdateien, die von der Informatica Electronic Software-Download-Site heruntergeladen wurden.

In der folgenden Tabelle werden die Prüfsumme und die Dateigröße für Informatica-Dienste unter Windows aufgelistet:

Datei	Prüfsummenwert	Dateigröße
informatica_1059_server_winem-64t.zip	713085966	12339017941 Byte

Zu einer nicht übereinstimmenden Prüfsumme kann es kommen, wenn während des Downloads aufgrund von Netzwerkproblemen Datenfehler auftreten oder wenn Daten in der Datei auf der Festplatte beschädigt werden. Weitere Informationen zu Prüfsummenfehlern finden Sie unter [HOW TO: Identify file errors after downloading Informatica installation files](#).

Überprüfen des Lizenzschlüssels

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

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

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

KAPITEL 4

Vorbereiten von Anwendungsdiensten und Datenbanken

Dieses Kapitel umfasst die folgenden Themen:

- [Checkliste zur Vorbereitung der Anwendungsdienste , 51](#)
- [Vorbereiten von Anwendungsdiensten und Datenbanken – Übersicht, 52](#)
- [Einrichten von Datenbankbenutzerkonten, 52](#)
- [Identifizieren von Anwendungsdiensten nach Produkt, 52](#)
- [Datenbankanforderungen des Domänen-Konfigurations-Repositorys, 53](#)
- [Analyst-Dienst , 58](#)
- [Content-Management-Dienst, 58](#)
- [Datenintegrationsdienst, 61](#)
- [Metadata Manager-Dienst, 68](#)
- [Modellrepository-Dienst, 73](#)
- [Überwachen des Modellrepository-Diensts, 77](#)
- [PowerCenter-Integrationsdienst, 78](#)
- [PowerCenter-Repository-Dienst, 79](#)
- [Suchdienst, 82](#)
- [Konfigurieren nativer Konnektivität auf Dienstcomputern, 83](#)

Checkliste zur Vorbereitung der Anwendungsdienste

Dieses Kapitel enthält Informationen zu Anwendungsdiensten und Datenbanken für die Informatica-Umgebung. Verwenden Sie diese Checkliste, um die Dienstplanungs- und Datenbankvorbereitung zu überwachen.

- ☐ Identifizierung der in Ihrer Umgebung benötigten Anwendungsdienste.
- ☐ Identifizierung der vom Installationsprogramm zu erstellenden Anwendungsdienste.

☐ Vorbereitung der Datenbanken für die Dienste:

- Erstellen Sie die Datenbank.
- Erstellen Sie einen Benutzer für die Datenbank.
- Erstellen Sie Umgebungsvariablen.
- Konfigurieren Sie die Konnektivität.

Vorbereiten von Anwendungsdiensten und Datenbanken – Übersicht

Wenn Sie die Anwendungsdienste planen, müssen Sie die zugeordneten Dienste berücksichtigen, die eine Verbindung zum Anwendungsdienst herstellen. Sie müssen auch die relationalen Datenbanken planen, die der Anwendungsdienst benötigt.

Das Installationsprogramm fragt Sie, ob Sie während der Installation optional einige Dienste erstellen möchten. Einige Diensteigenschaften erfordern Datenbankinformationen. Wenn das Installationsprogramm einen Dienst erstellen soll, für den eine Datenbank erforderlich ist, müssen Sie die Datenbank vorbereiten, bevor Sie das Installationsprogramm ausführen. Um die Datenbanken vorzubereiten, überprüfen Sie die Datenbankanforderungen, richten Sie die Datenbank ein und richten Sie ein Benutzerkonto ein. Die Datenbankanforderungen hängen von den Anwendungsdiensten ab, die Sie erstellen möchten.

Wenn Sie während der Installation keine Dienste erstellen, können Sie sie nach der Installation manuell erstellen.

Einrichten von Datenbankbenutzerkonten

Richten Sie ein Datenbank- und Benutzerkonto für die Repository-Datenbanken ein.

Verwenden Sie die folgenden Regeln und Richtlinien, wenn Sie die Benutzerkonten einrichten:

- 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.

Identifizieren von Anwendungsdiensten nach Produkt

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

Die folgende Tabelle listet die Anwendungsdienste auf, die von PowerCenter- und Informatica Data Quality-Produkten verwendet werden:

Produkt	Anwendungsdienste
PowerCenter	<ul style="list-style-type: none"> - Analyst-Dienst - Content-Management-Dienst * - Datenintegrationsdienst * - Metadata Manager-Dienst - Modellrepository-Dienst * - Überwachungsmodellrepository-Dienst * - PowerCenter-Integrationsdienst * - PowerCenter-Repository-Dienst * - Suchdienst - Webdienst-Hub-Dienst
Informatica Data Quality	<ul style="list-style-type: none"> - Analyst-Dienst - Content-Management-Dienst * - Datenintegrationsdienst * - Metadata Manager-Dienst - Modellrepository-Dienst * - Überwachungsmodellrepository-Dienst * - PowerCenter-Integrationsdienst * - PowerCenter-Repository-Dienst * - Suchdienst
<p><i>* Diese Dienste können Sie bei der Installation des Produkts erstellen. Beachten Sie, dass Dienste je nach Ihrer Produktedition variieren können.</i></p>	

Datenbankanforderungen des Domänen-Konfigurations-Repositorys

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

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

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

Das Domänen-Konfigurations-Repository unterstützt die folgenden Datenbanktypen:

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL-Datenbank
- Oracle
- PostgreSQL

- Sybase ASE

Zulassen von 200 MB Speicherplatz für die Datenbank.

IBM DB2-Datenbankanforderungen

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

- Wenn sich das Repository in einer IBM DB2-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

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

Microsoft SQL Server-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository die folgenden Anleitungen:

- 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.

Microsoft Azure SQL-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository die folgenden Anleitungen:

- 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.

PostgreSQL-Datenbankanforderungen

Beachten Sie beim Einrichten der Datenbank in PostgreSQL die folgenden Richtlinien:

- Stellen Sie sicher, dass das Datenbankbenutzerkonto über die Berechtigungen CONNECT, CREATE TABLE und CREATE VIEW verfügt.
- Geben Sie den Namen des Datenbankschemas an, wenn Sie PostgreSQL als Datenbank verwenden.
- Stellen Sie sicher, dass PostgreSQL über ausreichend Festplattenspeicher für die Datendateien verfügt. Standardmäßig befinden sich die Datendateien an dem folgenden Speicherort:

`<PostgreSQL-Installationsverzeichnis>/data`

- Legen Sie die Konfigurationsparameter in der Datenbank fest.

In der folgenden Tabelle sind die Mindestwerte und empfohlenen Werte für die Konfigurationsparameter aufgeführt:

Parameter	Mindestwert	Empfohlener Wert
max_connections	200	4000
shared_buffers	2 GB	16 GB
max_locks_per_transaction	1024	1024
max_wal_size	1 GB	8 GB
checkpoint_timeout	5 Minuten	30 Minuten

Sybase – Datenbankanforderungen

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

- Stellen Sie die Seitengröße des Datenbankservers auf 16 K oder höher ein. Sie müssen die Seitengröße auf 16 K einstellen, da Sie diese Konfiguration nur ein einziges Mal vornehmen und sie später nicht mehr ändern können.
- Konfigurieren Sie die Datenbanksperreffunktion als Sperrung auf Zeilenebene.
 In der folgenden Tabelle wird beschrieben, wie Sie die Datenbanksperreffunktion konfigurieren müssen:

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

- Legen Sie die Sybase-Datenbankoption „ddl in tran“ auf TRUE fest.
- Legen Sie „allow nulls by default“ auf TRUE fest.

- Aktivieren Sie die Sybase-Datenbankoption (ON) und wählen Sie into/bulkcopy/pllsort.
- Aktivieren Sie die select-Berechtigung für die sysobjects-Systemtabelle.
- Erstellen Sie das folgende Anmeldeskript zum Deaktivieren der Standard-VARCHAR-Kürzung:

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

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

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

Datenbankkonfiguration	Sybase-Systemprozedur	Wert
Maximale Gesamtmenge an physischem Speicher	sp_configure "max memory"	2097151
Cache-Größe der Prozedur	sp_configure "procedure cache size"	500000
Anzahl geöffneter Objekte	sp_configure "number of open objects"	5000
Anzahl geöffneter Indizes	sp_configure "number of open indexes"	5000
Anzahl geöffneter Partitionen	sp_configure "number of open partitions"	5000
Heap-Speicher pro Benutzer	sp_configure "heap memory per user"	49152
Anzahl Sperren	sp_configure "number of locks"	100000

Analyst-Dienst

Der Analyst-Dienst führt das Analyst Tool aus. Er verwaltet die Verbindungen zwischen Dienstkomponenten und den Benutzern, die Zugriff auf das Analyst-Tool haben. Wenn Sie den Dienst erstellen, müssen Sie ihm andere Anwendungsdienste zuordnen.

In der folgenden Tabelle sind einige Abhängigkeiten im Zusammenhang mit dem Analyst-Dienst zusammengefasst:

Abhängigkeit	Zusammenfassung
Produkte	Die folgenden Produkte verwenden den Analyst-Dienst: <ul style="list-style-type: none">- Data Engineering Integration- Data Engineering Quality- Data Engineering Streaming- Enterprise Data Catalog- Informatica Data Quality- PowerCenter- Test Data Management
Dienste	Der Analyst-Dienst muss folgenden Diensten direkt zugeordnet werden: <ul style="list-style-type: none">- Datenintegrationsdienst- Modellrepository-Dienst
Datenbanken	Der Analyst-Dienst ist keinen Datenbanken zugeordnet.
Installationsprogramm	Sie können den Analyst-Dienst nicht während der Installation erstellen.

Content-Management-Dienst

Der Content-Management-Dienst verwaltet Referenzdaten für Datendomänen, die Referenztabelle verwenden. Er nutzt den Datenintegrationsdienst zum Ausführen von Mappings, die Daten zwischen Referenztabelle und externen Datenquellen übertragen. Wenn Sie den Dienst erstellen, müssen Sie ihm andere Anwendungsdienste zuordnen.

In der folgenden Tabelle werden die Abhängigkeiten für Produkte, Dienste und Datenbanken zusammengefasst, die dem Content-Management-Dienst zugeordnet sind:

Abhängigkeit	Zusammenfassung
Produkte	Die folgenden Produkte verwenden den Content-Management-Dienst: <ul style="list-style-type: none">- Data Engineering Quality- Data Privacy Management- Enterprise Data Catalog- Enterprise Data Preparation- Informatica Data Quality- Test Data Management
Dienste	Der Content-Management-Dienst muss folgenden Diensten direkt zugeordnet werden: <ul style="list-style-type: none">- Modellrepository-Dienst- Datenintegrationsdienst

Abhängigkeit	Zusammenfassung
Datenbanken	Der Content-Management-Dienst verwendet die folgende Datenbank: - Referenzdaten-Warehouse. Speichert die Datenwerte für die Referenztabelleobjekte, 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.
Installationsprogramm	Sie können den Content-Management-Dienst bei Ausführung des Installationsprogramms erstellen. Hinweis: Sie müssen den Content-Management-Dienst auf demselben Knoten wie den Datenintegrationsdienst erstellen.

Anforderungen des Referenzdaten-Warehouse

Das Referenzdaten-Warehouse speichert die Datenwerte für die Referenztabelleobjekte, 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
- PostgreSQL mit einem JDBC-Treiber

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.DBTAUTH 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 Azure SQL-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository die folgenden Anleitungen:

- 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.

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.

PostgreSQL-Datenbankanforderungen

Beachten Sie beim Einrichten der Datenbank in PostgreSQL die folgenden Richtlinien:

- Verwenden Sie eine JDBC-Verbindung, um eine Verbindung zur PostgreSQL-Datenbank herzustellen.

Informatica installiert einen DataDirect JDBC-Treiber für PostgreSQL, mit dem Sie eine Verbindung zur Datenbank herstellen können. Suchen Sie den Treiber im Installationsverzeichnis `clients/DeveloperClient/infacmd` und kopieren Sie den Treiber in das Verzeichnis `clients/externaljdbcjars`.

- Geben Sie den Schemanamen der Datenbank an. Lassen Sie den Schemanamen nicht leer.

Wenn die Datenbank den standardmäßigen PostgreSQL-Schemanamen von `public` verwendet, können Sie `public` als Schemanamen verwenden.

- Stellen Sie sicher, dass der Datenbankbenutzer über die Berechtigungen CONNECT und CREATE TABLE verfügt.

Datenintegrationsdienst

Der Datenintegrationsdienst empfängt Anfragen von Informatica-Client-Tools zur Ausführung von Integrations-, Profil- und Datenvorbereitungsjobs. Er schreibt Ergebnisse in verschiedene Datenbanken sowie Laufzeitmetadaten in das Modellrepository. Wenn Sie den Dienst erstellen, müssen Sie ihn einem anderen Anwendungsdienst zuordnen.

In der folgenden Tabelle werden die Abhängigkeiten für Produkte, Dienste und Datenbanken zusammengefasst, die dem Datenintegrationsdienst zugeordnet sind.

Abhängigkeit	Zusammenfassung
Produkte	Die folgenden Produkte verwenden den Datenintegrationsdienst: <ul style="list-style-type: none"> - Data Engineering Integration - Data Engineering Quality - Data Engineering Streaming - Data Privacy Management - Enterprise Data Catalog - Enterprise Data Preparation - Informatica Data Quality - PowerCenter - Test Data Management
Dienste	Der Datenintegrationsdienst muss den folgenden Diensten direkt zugeordnet werden: <ul style="list-style-type: none"> - Modellrepository-Dienst
Datenbanken	Der Datenintegrationsdienst verwendet die folgenden Datenbanken: <ul style="list-style-type: none"> - Datenobjekt-Cache. Speichert zwischengespeicherte logische Datenobjekte und virtuelle Tabellen. - Profiling-Warehouse. Speichert Profiling-Informationen wie Profil- und Scorecard-Ergebnisse. - Arbeitsablauf-Datenbank. Speichert Laufzeitmetadaten für Arbeitsabläufe.
Installationsprogramm	Sie können den Datenintegrationsdienst bei Ausführung des Installationsprogramms erstellen.

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.

Microsoft Azure SQL-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.

Profiling Warehouse-Anforderungen

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

Das Profiling-Warehouse unterstützt die folgenden Datenbanktypen:

- IBM DB2 UDB
- Microsoft SQL Server
- Oracle
- PostgreSQL

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 als Profiling-Warehouse-Verbindung für die Datenbanktypen IBM DB2 UDB, Microsoft SQL Server und Oracle 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 die folgenden Parameter auf die von Informatica empfohlenen Werte fest:

Parameter	Empfohlener Wert
open_cursors	4000
Sitzungen	1000 Sie können den folgenden Ausdruck verwenden, um den Standardwert für die Sitzung zu bestimmen: $(1.5 * PROCESSES) + 22$ Hinweis: Wenn der Sitzungswert niedriger als der Standardwert ist, verwendet die Oracle-Datenbank den Standardsitzungswert.
Prozesse	1000

PostgreSQL-Anforderungen (Referenzdaten-Datenbank)

Beachten Sie beim Einrichten der Datenbank in PostgreSQL die folgenden Richtlinien:

- Verwenden Sie eine JDBC-Verbindung, um eine Verbindung zur PostgreSQL-Datenbank herzustellen.
Hinweis: Die JDBC V2-Verbindung ist nicht anwendbar.
Informatica installiert einen DataDirect JDBC-Treiber für PostgreSQL, mit dem Sie eine Verbindung zur Datenbank herstellen können. Suchen Sie den Treiber im Installationsverzeichnis `clients/DeveloperClient/infacmd` und kopieren Sie den Treiber in das Verzeichnis `clients/externaljdbcjars`.
- Standardmäßig verwendet PostgreSQL `public` als Schema. Wenn Sie beabsichtigen, ein anderes Schema als "public" zu verwenden, stellen Sie sicher, dass Sie das neue Schema als Standardschema der Datenbank festlegen.
- Stellen Sie sicher, dass der Datenbankbenutzer über die Berechtigungen `CONNECT` und `CREATE TABLE` verfügt.

Anforderungen an Arbeitsablauf-Datenbanken

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

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

Die Arbeitsablauf-Datenbank unterstützt die folgenden Datenbanktypen:

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL-Datenbank
- Oracle
- PostgreSQL

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.
- Legen Sie die Verbindungspooling-Parameter fest.

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

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

Microsoft Azure SQL-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository die folgenden Anleitungen:

- 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.

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.
- Legen Sie die Verbindungspooling-Parameter fest.

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

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

Oracle-Datenbankanforderungen

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

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

ALTER TABLE

ALTER VIEW

CREATE SEQUENCE

CREATE SESSION

CREATE SYNONYM

CREATE TABLE

CREATE VIEW

DROP TABLE

DROP VIEW

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

- Legen Sie die Verbindungspooling-Parameter fest.

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

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

PostgreSQL-Datenbankanforderungen

Beachten Sie beim Einrichten der Datenbank in PostgreSQL die folgenden Richtlinien:

- Verwenden Sie eine JDBC-Verbindung, um eine Verbindung zur PostgreSQL-Datenbank herzustellen.
- Stellen Sie sicher, dass das Datenbankbenutzerkonto über die Berechtigungen CONNECT, CREATE TABLE und CREATE VIEW verfügt.
- Geben Sie den Namen des Datenbankschemas an, wenn Sie PostgreSQL als Datenbank verwenden.
- Stellen Sie sicher, dass PostgreSQL über ausreichend Festplattenspeicher für die Datendateien verfügt. Standardmäßig befinden sich die Datendateien an dem folgenden Speicherort:

`<PostgreSQL-Installationsverzeichnis>/data`

- Legen Sie die Konfigurationsparameter in der Datenbank fest.

In der folgenden Tabelle sind die Mindestwerte und empfohlenen Werte für die Konfigurationsparameter aufgeführt:

Parameter	Mindestwert	Empfohlener Wert
max_connections	200	4000
shared_buffers	2 GB	16 GB
max_locks_per_transaction	1024	1024
max_wal_size	1 GB	8 GB
checkpoint_timeout	5 Minuten	30 Minuten

Metadata Manager-Dienst

Der Metadata Manager-Dienst führt den Metadata Manager-Webclient in der Informatica-Domäne aus. Der Metadata Manager-Dienst verwaltet die Verbindungen zwischen Dienstkomponenten und den Benutzern, die Zugriff auf Metadata Manager haben.

In der folgenden Tabelle werden die Abhängigkeiten für Produkte, Dienste und Datenbanken zusammengefasst, die dem Metadata Manager-Dienst zugeordnet sind:

Abhängigkeit	Zusammenfassung
Produkte	Die folgenden Produkte verwenden den Metadata Manager-Dienst: <ul style="list-style-type: none">- Informatica Data Quality- PowerCenter
Dienste	Der Metadata Manager-Dienst muss folgenden Diensten direkt zugeordnet werden: <ul style="list-style-type: none">- PowerCenter-Integrationsdienst- PowerCenter-Repository-Dienst
Datenbanken	Der Metadata Manager-Dienst verwendet die folgende Datenbank: <ul style="list-style-type: none">- Metadata Manager-Repository. Speichert das Metadata Manager-Warehouse und Metadatenmodelle.
Installationsprogramm	Sie können den Metadata Manager-Dienst nicht bei Ausführung des Installationsprogramms erstellen. Sie müssen den Dienst nach Abschluss der Installation erstellen.

Metadata Manager Repository-Datenbankanforderungen

Das Metadata Manager-Repository ist ein zentraler Speicherort in einer relationalen Datenbank, der Metadaten aus verschiedenen Metadatenquellen speichert. Es speichert auch das Metadata Manager-Warehouse und die Modelle für die einzelnen Metadaten-Quellentypen. Jede Metadata Manager-Anwendung ist für die Ausführung mit einem Metadata Manager-Repository konfiguriert.

Das Metadata Manager-Repository unterstützt die folgenden Datenbanktypen:

- IBM DB2 UDB
- Microsoft SQL Server
- Oracle

Zulassen von 1 GB Speicherplatz für die Datenbank.

IBM DB2-Datenbankanforderungen

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

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

```
ALTER TABLE
CREATE FUNCTION
CREATE INDEX
CREATE PROCEDURE
CREATE TABLE
CREATE VIEW
DROP PROCEDURE
DROP TABLE
INSERT INTO
```

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

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

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

```
CREATE Bufferpool RBF IMMEDIATE SIZE 1000 PAGESIZE 32 K EXTENDED STORAGE ;
CREATE Bufferpool STBF IMMEDIATE SIZE 2000 PAGESIZE 32 K EXTENDED STORAGE ;
CREATE REGULAR TABLESPACE REGTS32 PAGESIZE 32 K MANAGED BY SYSTEM USING
('C:\DB2\NODE0000\reg32' ) EXTENTSIZE 16 OVERHEAD 10.5 PREFETCHSIZE 16 TRANSFERRATE
0.33 BUFFERPOOL RBF;
CREATE SYSTEM TEMPORARY TABLESPACE TEMP32 PAGESIZE 32 K MANAGED BY SYSTEM USING
('C:\DB2\NODE0000\temp32' ) EXTENTSIZE 16 OVERHEAD 10.5 PREFETCHSIZE 16 TRANSFERRATE
0.33 BUFFERPOOL STBF;
GRANT USE OF TABLESPACE REGTS32 TO USER <USERNAME>;
UPDATE DB CFG FOR <DB NAME> USING APP CTL HEAP SZ 16384
UPDATE DB CFG FOR <DB NAME> USING APPLHEAPSZ 16384
UPDATE DBM CFG USING QUERY HEAP SZ 8000
UPDATE DB CFG FOR <DB NAME> USING LOGPRIMARY 100
UPDATE DB CFG FOR <DB NAME> USING LOGFILSIZ 2000
UPDATE DB CFG FOR <DB NAME> USING LOCKLIST 1000
UPDATE DB CFG FOR <DB NAME> USING DBHEAP 2400
"FORCE APPLICATIONS ALL"
DB2STOP
DB2START
```

- Legen Sie die Sperrparameter fest, damit es beim Laden von Metadaten in das Metadata Manager-Repository in IBM DB2 nicht zu Deadlocks kommt.

In der folgenden Tabelle werden die Sperrparameter aufgelistet, die Sie konfigurieren können:

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

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

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

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

Microsoft SQL Server-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository die folgenden Anleitungen:

- Das Datenbankbenutzerkonto, das das Repository erstellt, muss über Berechtigungen zur Durchführung der folgenden Vorgänge verfügen:
 - ALTER TABLE
 - CREATE CLUSTERED INDEX
 - CREATE INDEX
 - CREATE PROCEDURE
 - CREATE TABLE
 - CREATE VIEW
 - DROP PROCEDURE
 - DROP TABLE
 - INSERT INTO
- Wenn im Repository Metadaten in einer Multibyte-Sprache gespeichert werden müssen, stellen Sie die Datenbank-Sortierreihenfolge bei der Installation von Microsoft SQL Server auf diese Multibyte-Sprache ein. Wenn im Repository beispielsweise Metadaten in Japanisch gespeichert werden müssen, setzen Sie bei der Installation von Microsoft SQL Server die Sortierreihenfolge der Datenbank auf eine japanische Sortierreihenfolge. Diese Konfiguration wird nur einmal vorgenommen und kann danach nicht mehr geändert werden.

Oracle-Datenbankanforderungen

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

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

ALTER TABLE
CREATE CLUSTER
CREATE INDEX
CREATE OR REPLACE FORCE VIEW
CREATE OR REPLACE PROCEDURE
CREATE OR REPLACE VIEW
CREATE SESSION
CREATE TABLE
DROP TABLE
INSERT INTO TABLE

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

<Temporärer Tablespace>

Größe auf mindestens 2 GB ändern.

CURSOR_SHARING

Auf FORCE festlegen.

MEMORY_TARGET

Mindestens auf 4 GB festlegen.

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

MEMORY_MAX_TARGET

Einen größeren Wert als die MEMORY_TARGET-Größe festlegen.

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

OPEN_CURSORS

Auf „3000 gemeinsam genutzt“ festlegen.

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

UNDO_MANAGEMENT

Auf AUTO festlegen.

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

Geteilte Domäne für Metadata Manager

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

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

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

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

Überlegungen zu geteilten Domänen

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

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

Sie sollten jedoch folgende Aspekte beachten:

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

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

Unter Umständen treten Lizenzprobleme auf.

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

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

Sie benötigen zusätzliche Datenbankschemas und Benutzerkonten.

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

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

Sie benötigen zusätzlichen Arbeits- und Festplattenspeicher.

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

Es gibt Beschränkungen bei der Produktversion.

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

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

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

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

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

Modellrepository-Dienst

Der Modellrepository-Dienst verwaltet das Modellrepository. Er empfängt Anfragen von Informatica-Clients und -Anwendungsdiensten zur Speicherung von bzw. zum Zugriff auf Metadaten im Modellrepository.

In der folgenden Tabelle werden die Abhängigkeiten für Produkte, Dienste und Datenbanken zusammengefasst, die dem Modellrepository-Dienst zugeordnet sind:

Abhängigkeit	Zusammenfassung
Produkte	Die folgenden Produkte verwenden den Modellrepository-Dienst: <ul style="list-style-type: none">- Data Engineering Integration- Data Engineering Quality- Data Engineering Streaming- Data Privacy Management- Enterprise Data Catalog- Enterprise Data Preparation- Informatica Data Quality- PowerCenter- Test Data Management
Dienste	Der Modellrepository-Dienst erfordert keine Zuordnung zu einem anderen Anwendungsdienst.

Abhängigkeit	Zusammenfassung
Datenbanken	Der Modellrepository-Dienst verwendet die folgende Datenbank: - Modellrepository. Speichert von Informatica-Clients und -Anwendungsdiensten erstellte Metadaten.
Installationsprogramm	Sie können den Modellrepository-Dienst bei Ausführung des Installationsprogramms erstellen.

Modellrepository – Datenbankanforderungen

Informatica-Dienste und Clients speichern Daten und Metadaten im Modellrepository. Konfigurieren Sie ein Überwachungsmodellrepository, um Statistiken für Ad-hoc-Jobs, Anwendungen, logische Datenobjekte, SQL-Datendienste, Webdienste und Arbeitsabläufe zu speichern. Richten Sie vor der Erstellung des Modellrepository-Diensts eine Datenbank und ein Datenbankbenutzerkonto für das Modellrepository ein. Es wird empfohlen, für das Modellrepository und das Überwachungsmodellrepository verschiedene Datenbankkonfigurationen zu verwenden.

Das Modellrepository unterstützt die folgenden Datenbanktypen:

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL-Datenbank
- Oracle
- PostgreSQL

Wenn Sie Microsoft SQL Server konfigurieren, können Sie die Microsoft Azure SQL-Datenbank als Modellrepository konfigurieren.

Wenn Sie die Windows NT-Anmeldeinformationen für die Modellrepository-Datenbank in Microsoft SQL Server angeben, müssen Sie auch die Syntax der Verbindungszeichenfolge bereitstellen, um die Authentifizierungsmethode als NTLM einzuschließen.

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

Weitere Informationen zur Konfiguration 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:

- Geben Sie den Tablespace-Namen an, wenn Sie IBM DB2 als Modellrepository-Datenbank verwenden.
- 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

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

Microsoft Azure SQL-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository die folgenden Anleitungen:

- 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.

Hinweis: Die Richtlinien zum Einrichten des Repositorys für Azure SQL Database mit Active Directory-Authentifizierung sind dieselben.

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.

Hinweis: Die Richtlinien zum Einrichten der Repositorys für Microsoft Azure SQL Database und Azure SQL Database mit Active Directory-Authentifizierung sind dieselben.

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.
- Sie können die Verbindung zwischen der Informatica-Domäne, dem Modellrepository-Dienst oder PowerCenter-Repository-Dienst und Oracle RAC konfigurieren. Oracle Real Application Clusters (RAC) ermöglicht eine hohe Verfügbarkeit von Datenbankanwendungen. Die Informatica-Domäne, der Modellrepository-Dienst und der PowerCenter-Repository-Dienst sind für alle CRUD-Vorgänge stabil gegenüber einem Failover von Oracle RAC-Datenbanken.
Sie können keine Administratorvorgänge mit Oracle RAC-Datenbank-Failover für die Informatica-Domäne und den Modellrepository-Dienst ausführen.

PostgreSQL-Datenbankanforderungen

Beachten Sie beim Einrichten der Datenbank in PostgreSQL die folgenden Richtlinien:

- Stellen Sie sicher, dass das Datenbankbenutzerkonto über die Berechtigungen CONNECT, CREATE TABLE und CREATE VIEW verfügt.
- Geben Sie den Namen des Datenbankschemas an, wenn Sie PostgreSQL als Datenbank verwenden.
- Stellen Sie sicher, dass PostgreSQL über ausreichend Festplattenspeicher für die Datendateien verfügt. Standardmäßig befinden sich die Datendateien an dem folgenden Speicherort:

`<PostgreSQL-Installationsverzeichnis>/data`

- Legen Sie die Konfigurationsparameter in der Datenbank fest.

In der folgenden Tabelle sind die Mindestwerte und empfohlenen Werte für die Konfigurationsparameter aufgeführt:

Parameter	Mindestwert	Empfohlener Wert
max_connections	200	4000
shared_buffers	2 GB	16 GB
max_locks_per_transaction	1024	1024
max_wal_size	1 GB	8 GB
checkpoint_timeout	5 Minuten	30 Minuten

Überwachen des Modellrepository-Diensts

Der Überwachungsmodellrepository-Dienst ist ein Modellrepository-Dienst, der Statistiken für Jobs des Datenintegrationsdiensts überwacht. Sie konfigurieren den Überwachungsmodellrepository-Dienst in den Domäneneigenschaften.

Hinweis: Wenn Sie Überwachungsstatistiken generieren möchten, müssen Sie einen dedizierten Modellrepository-Dienst für die Überwachung erstellen. Sie können Laufzeitüberwachungsstatistiken nicht im selben Repository speichern, in dem Sie Objektmetadaten speichern.

In der folgenden Tabelle werden die Abhängigkeiten für Produkte, Dienste und Datenbanken zusammengefasst, die dem Überwachungsmodellrepository-Dienst zugeordnet sind:

Abhängigkeit	Zusammenfassung
Produkte	Die folgenden Produkte verwenden den Überwachungsmodellrepository-Dienst: <ul style="list-style-type: none"> - Data Engineering Integration - Data Engineering Quality - Data Engineering Streaming - Data Privacy Management - Enterprise Data Catalog - Enterprise Data Preparation - Informatica Data Quality - PowerCenter - Test Data Management
Dienste	Der Überwachungsmodellrepository-Dienst erfordert keine Zuordnung zu einem anderen Anwendungsdienst.
Datenbanken	Der Überwachungsmodellrepository-Dienst verwendet die folgende Datenbank: <ul style="list-style-type: none"> - Modellrepository. Speichert Laufzeitüberwachungsstatistiken, die Sie im Administrator Tool anzeigen können.
Installationsprogramm	Sie können den Überwachungsmodellrepository-Dienst bei Ausführung des Installationsprogramms erstellen.

PowerCenter-Integrationsdienst

Der PowerCenter-Integrationsdienst erhält Anfragen von PowerCenter-Client Tools, um Datenintegrationsaufgaben auszuführen. Er schreibt Ergebnisse in verschiedene Datenbanken sowie Laufzeitmetadaten in das PowerCenter-Repository. Wenn Sie den Dienst erstellen, müssen Sie ihn einem anderen Anwendungsdienst zuordnen.

In der folgenden Tabelle werden die Abhängigkeiten für Produkte, Dienste und Datenbanken zusammengefasst, die dem PowerCenter-Integrationsdienst zugeordnet sind.

Abhängigkeit	Zusammenfassung
Produkte	Die folgenden Produkte verwenden den PowerCenter-Integrationsdienst: <ul style="list-style-type: none"> - PowerCenter - Informatica Data Quality - Test Data Management
Dienste	Der PowerCenter-Integrationsdienst muss dem folgenden Dienst direkt zugeordnet werden: <ul style="list-style-type: none"> - PowerCenter Repository Service
Datenbanken	Dem PowerCenter-Integrationsdienst ist keine Datenbank zugeordnet.
Installationsprogramm	Sie können den PowerCenter-Integrationsdienst bei Ausführung des Installationsprogramms erstellen.

PowerCenter-Repository-Dienst

Der PowerCenter-Repository-Dienst verwaltet das PowerCenter-Repository. Er empfängt Anfragen von Informatica-Clients und -Anwendungsdiensten, um Metadaten im PowerCenter-Repository zu speichern oder auf diese zuzugreifen.

In der folgenden Tabelle werden die Abhängigkeiten für Produkte, Dienste und Datenbanken zusammengefasst, die dem PowerCenter-Repository-Dienst zugeordnet sind:

Abhängigkeit	Zusammenfassung
Produkte	Die folgenden Produkte verwenden den PowerCenter-Repository-Dienst: <ul style="list-style-type: none">- PowerCenter- Informatica Data Quality- Test Data Management
Dienste	Der PowerCenter-Repository-Dienst erfordert keine Zuordnung zu einem anderen Anwendungsdienst.
Datenbanken	Der PowerCenter-Repository-Dienst verwendet die folgende Datenbank: <ul style="list-style-type: none">- PowerCenter-Repository Speichert von Informatica-Clients und -Anwendungsdiensten erstellte Metadaten.
Installationsprogramm	Sie können den PowerCenter-Repository-Dienst bei Ausführung des Installationsprogramms erstellen.

PowerCenter-Repository-Datenbankanforderungen

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

Das PowerCenter-Repository unterstützt die folgenden Datenbanktypen:

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL-Datenbank
- Oracle
- PostgreSQL

Hinweis: Um den PowerCenter-Repository-Dienst mit dem 10.5.9-Installationsprogramm zu erstellen, können Sie die Oracle-, Microsoft SQL Server- oder PostgreSQL-Datenbank verwenden. Wenn Sie den PowerCenter-Repository-Dienst auf einer der anderen Datenbanken installieren möchten, erstellen Sie den Dienst mit der erforderlichen Datenbank, nachdem Sie das Installationsprogramm ausgeführt haben.

Zulassen von 35 MB Speicherplatz für die Datenbank.

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

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

IBM DB2-Datenbankanforderungen

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

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

Legen Sie den Einzelknoten-Tabellenbereich-Namen beim Erstellen, Kopieren oder Wiederherstellen eines Repository fest. Wenn Sie keinen Tabellenbereich-Namen angeben, verwendet DB2 den Standard-Tabellenbereich.

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

Microsoft SQL Server-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository die folgenden Anleitungen:

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

Oracle-Datenbankanforderungen

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

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

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

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

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

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

```
CREATE SEQUENCE  
CREATE SESSION  
CREATE SYNONYM  
CREATE TABLE  
CREATE VIEW
```

- Informatica bietet keine Unterstützung für öffentliche Oracle-Synonyme für Repository-Tabellen. Stellen Sie sicher, dass für keine der Tabellen in der Datenbank öffentliche Synonyme erstellt wurden.
- Sie können Oracle Real Application Cluster (RAC) konfigurieren, um eine Verbindung mit einem Oracle-Dienst anzugeben, der mit Lastverteilung und hoher Verfügbarkeit aktiviert ist. Der PowerCenter Repository-Dienst ist gegenüber dem Datenbank-Failover im Oracle RAC-Setup stabil.

PostgreSQL-Datenbankanforderungen

Beachten Sie beim Einrichten der Datenbank in PostgreSQL die folgenden Richtlinien:

Berechtigungen

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

Festplattenspeicher

Stellen Sie sicher, dass PostgreSQL über ausreichend Festplattenspeicher für die Datendateien verfügt. Standardmäßig befinden sich die Datendateien an dem folgenden Speicherort:

<PostgreSQL-Installationsverzeichnis>/data

Konfigurationsparameter

Legen Sie die Konfigurationsparameter in der Datenbank fest.

In der folgenden Tabelle sind die Mindestwerte und empfohlenen Werte für die Konfigurationsparameter aufgeführt:

Parameter	Mindestwert	Empfohlener Wert
max_connections	200	4000
shared_buffers	2 GB	16 GB
max_locks_per_transaction	1024	4000
max_wal_size	1 GB	8 GB
checkpoint_timeout	5 Minuten	30 Minuten

Konfigurieren von PostgreSQL für das PowerCenter-Repository

Um eine PostgreSQL-Datenbank für das PowerCenter-Repository zu konfigurieren, legen Sie Werte für den PostgreSQL-Datenbankhost, -Port und -Dienstnamen für die Datei "pg_service.conf" im folgenden Format fest:

```
[PCRS_DB_SERVICE_NAME]
host=Database host IP
port=Database port
dbname=PowerCenter repository database service name
```

Stellen Sie sicher, dass die Einträge für [PCRS_DB_SERVICE_NAME] mit den Informationen für den PowerCenter-Repository-Dienst übereinstimmen. Um eine sichere Verbindung zu PostgreSQL für das PowerCenter-Repository herzustellen, legen Sie die Sicherheitseigenschaft zusammen mit den übrigen erforderlichen Datenbankeigenschaften in der pg_service.conf-Datei im folgenden Format fest:

sslmode=require Legen Sie die Umgebungsvariable PGSERVICEFILE auf den Speicherort der Datei pg_service.conf fest. Die Datei pg_service.conf enthält die Verbindungsparameter für die PostgreSQL-Datenbankverbindung im Informatica-Installationsverzeichnis. Legen Sie die Variable beispielsweise wie folgt fest:

Bei Verwendung einer Bourne-Shell:

```
$ export PGSERVICEFILE; PGSERVICEFILE=<pg_service.conf file
directory>/pg_service.conf
```

Bei Verwendung einer C-Shell:

```
$ setenv PGSERVICEFILE <pg_service.conf file  
directory>/pg_service.conf
```

Sybase ASE-Datenbankanforderungen

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

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

In der folgenden Tabelle sind die Konfigurationsanforderungen für den Speicher und die empfohlenen Baseline-Werte aufgeführt:

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

Suchdienst

Der Suchdienst verwaltet Suchvorgänge im Analyst Tool und gibt Suchergebnisse aus dem Modellrepository zurück. Wenn Sie den Dienst erstellen, müssen Sie ihn einem anderen Anwendungsdienst zuordnen.

In der folgenden Tabelle werden die Abhängigkeiten für Produkte, Dienste und Datenbanken zusammengefasst, die dem Suchdienst zugeordnet sind:

Abhängigkeit	Zusammenfassung
Produkte	Die folgenden Produkte verwenden den Suchdienst: <ul style="list-style-type: none">- Data Engineering Integration- Data Engineering Quality- Data Engineering Streaming- Enterprise Data Catalog- Enterprise Data Preparation- Informatica Data Quality- PowerCenter
Dienste	Der Suchdienst muss dem folgenden Dienst direkt zugeordnet werden: <ul style="list-style-type: none">- Modellrepository-Dienst

Abhängigkeit	Zusammenfassung
Datenbanken	Der Suchdienst ist keiner Datenbank zugeordnet.
Installationsprogramm	Sie können den Suchdienst nicht bei Ausführung des Installationsprogramms erstellen.

Konfigurieren nativer Konnektivität auf Dienstcomputern

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

Native Treiber werden mit dem Datenbankserver und der Clientsoftware geliefert. Konfigurieren Sie die Konnektivität auf den Computern, die auf die Datenbanken zugreifen müssen. Um die Kompatibilität zwischen dem Anwendungsdienst und der Datenbank zu gewährleisten, installieren Sie eine Client-Software, die mit der Datenbankversion kompatibel ist, und verwenden Sie die entsprechenden Bibliotheken des Datenbank-Client.

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

Datenintegrationsdienst

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

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

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

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

PowerCenter-Repository-Dienst

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

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

PowerCenter-Integrationsdienst

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

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

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

Install Database Client Software

You must install the database clients on the required machines based on the types of databases that the application services access.

To ensure compatibility between the application service and the database, use the appropriate database client libraries and install a client software that is compatible with the database version.

Install the following database client software based on the type of database that the application service accesses:

IBM DB2 Client Application Enabler (CAE)

Configure connectivity on the required machines by logging in to the machine as the user who starts Informatica services.

Microsoft SQL ServerNative Client

Download the latest client from the official Microsoft website.

Oracle client

Install compatible versions of the Oracle client and Oracle database server. You must also install the same version of the Oracle client on all machines that require it. To verify compatibility, contact Oracle.

Sybase Open Client (OCS)

Install an Open Client version that is compatible with the Sybase ASE database server. You must also install the same version of Open Client on the machines hosting the Sybase ASE database and Informatica. To verify compatibility, contact Sybase.

PostgreSQL client (psql)

Install and run the PostgreSQL interactive terminal program called psql, which allows you to interactively enter, edit, and run SQL commands.

psql is a terminal-based front-end to PostgreSQL. You can type in queries interactively, issue the queries to PostgreSQL, and check the query results. Or, the input can be from a file or from command line arguments.

You can install psql client application for PostgreSQL to work only on Linux or Windows.

Install and run the required software dependency packages to build PostgreSQL, such as GCC compiler package, readline and readline-devel packages, and zlib-devel compression library package. After you install the packages from the GNU Readline library, psql remembers each command you type, and you can use arrow keys to recall and edit previous commands.

You can also run the required library files with the yum install commands.

PostgreSQL on Windows

On Windows, download the psql client from the following link:

<https://www.enterprisedb.com/downloads/postgres-postgresql-downloads>

You must verify that PostgreSQL libraries are present in the following directories on Windows:

- Installation directory: C:\Program Files\PostgreSQL\<version>
- Command line tools installation directory: C:\Program Files\PostgreSQL\<version>
- pgAdmin4 installation directory: C:\Program Files\PostgreSQL\<version>\pgAdmin 4

PostgreSQL on Linux

On Linux, you also need to install the required postgresql libraries, <postgresql-package>-<version>-<release>.<distribution>.<architecture> and <postgresql-package>-<version>-<release>.<os>.<architecture>. For example: postgresql14-14.9-1PGDG.rhel7.x86_64 and postgresql14-libs-14.9-1PGDG.rhel7.x86_64.

For more information about the psql client, please refer to the official PSQL documentation.

Konfigurieren von Umgebungsvariablen für Datenbank-Clients

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

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

Oracle-Datenbank

In der folgenden Tabelle werden die Datenbank-Umgebungsvariablen aufgelistet, die Sie für die Oracle-Datenbank mit `sqlplus` als Datenbankdienstprogramm festlegen müssen:

Umgebungsvariable	Wert
ORACLE_HOME	<Client InstallDatabasePath>
PATH	<DatabasePath>/bin und USER_INSTALL_DIR/server/bin:\$PATH
LD_LIBRARY_PATH	\$ORACLE_HOME/lib und USER_INSTALL_DIR/server/bin:\$LD_LIBRARY_PATH
TNS_ADMIN	Auf den Speicherort der Datei "tnsnames.ora" festlegen: \$ORACLE_HOME/network/admin
INFA_TRUSTSTORE	Für die SSL-Standarddomäne hinzufügen zu: USER_INSTALL_DIR/services/shared/security Für benutzerdefinierte SSL-Domäne auf INFA_TRUSTSTORE und INFA_TRUSTSTORE_PASSWORD festlegen

IBM DB2-Datenbank

In der folgenden Tabelle werden die Datenbank-Umgebungsvariablen aufgelistet, die Sie für die IBM DB2-Datenbank mit `db2connect` als Datenbankdienstprogramm festlegen müssen:

Umgebungsvariable	Wert
DB2DIR	<database path>
DB2INSTANCE	<DB2InstanceName>
PATH	<database path>/bin

Sybase ASE-Datenbank

In der folgenden Tabelle werden die Datenbank-Umgebungsvariablen aufgelistet, die Sie für die Sybase ASE-Datenbank mit `isql` als Datenbankdienstprogramm festlegen müssen:

Umgebungsvariable	Wert
SYBASE15	<<database path>/sybase<version> >
SYBASE_ASE	\${SYBASE15}/ASE-<version>
SYBASE_OCS	\${SYBASE15}/OCS-<version>
PATH	\${SYBASE_ASE}/bin:\${SYBASE_OCS}/bin:\$PATH

PostgreSQL-Datenbank

In der folgenden Tabelle werden die Datenbank-Umgebungsvariablen aufgelistet, die Sie für die PostgreSQL-Datenbank festlegen müssen:

Umgebungsvariable	Wert
PGSERVICEFILE	Auf den Speicherort der pg_service.conf-Datei festlegen: <pg_service.conf-Dateiverzeichnis>/pg_service.conf
PGHOME	/usr/pgsql-10
PATH	\$PGHOME:\${PATH}
LD_LIBRARY_PATH	\$PGHOME/lib:\${LD_LIBRARY_PATH}
INFA_TRUSTSTORE	Für die SSL-Standarddomäne hinzufügen zu: <InstallationDirectory>/services/shared/security Für benutzerdefinierte SSL-Domäne auf INFA_TRUSTSTORE und INFA_TRUSTSTORE_PASSWORD festlegen
POSTGRES_ODBC	Legen Sie den Wert für die PostgreSQL-ODBC-Verbindung auf 1 fest. Sie können diesen Wert für alle Repositories in der Domäne oder für jedes PostgreSQL-Repository festlegen, das eine ODBC-Verbindung verwendet.

Microsoft SQL Server-Datenbank

In der folgenden Tabelle werden die Datenbank-Umgebungsvariablen aufgelistet, die Sie für die Microsoft SQL Server-Datenbank festlegen müssen:

Umgebungsvariable	Wert
ODBCHOME	USER_INSTALL_DIR/ODBC7.1
ODBCINI	\$ODBCHOME/odbc.ini
ODBCINST	\$ODBCHOME/odbcinst.ini
PATH	/opt/mssql-tools/bin:\$PATH\$PATHUSER_INSTALL_DIR/ODBC7.1:\$PATHUSER_INSTALL_DIR/server/bin:\$PATH

Umgebungsvariable	Wert
LD_LIBRARY_PATH	<i>\$ODBCHOME/lib</i>
INFA_TRUSTSTORE	<i>USER_INSTALL_DIR/server/bin:\$LD_LIBRARY_PATH</i> Für die SSL-Standarddomäne hinzufügen zu: USER_INSTALL_DIR/services/shared/security Für benutzerdefinierte SSL-Domäne auf INFA_TRUSTSTORE und INFA_TRUSTSTORE_PASSWORD festlegen

KAPITEL 5

Vorbereiten der Kerberos-Authentifizierung

Dieses Kapitel umfasst die folgenden Themen:

- [Checkliste zur Vorbereitung der Kerberos-Authentifizierung , 88](#)
- [Vorbereiten der Kerberos-Authentifizierung – Übersicht, 89](#)
- [Einrichten der Kerberos-Konfigurationsdatei, 89](#)
- [Generieren des Namensformats für Dienstprinzipale und Keytab-Dateien, 91](#)
- [Überprüfen der SPN- und Keytab-Format-Textdatei, 94](#)
- [Erstellen der Dienstprinzipalnamen und Keytab-Dateien, 96](#)

Checkliste zur Vorbereitung der Kerberos-Authentifizierung

Dieses Kapitel enthält Aufgaben, die auszuführen sind, wenn das Installationsprogramm während der Installation Kerberos aktivieren soll. Verwenden Sie diese Checkliste, um die zur Vorbereitung der Kerberos-Authentifizierung erforderlichen Aufgaben zu überwachen.

- ☐ Einrichten der Kerberos-Konfigurationsdatei.
- ☐ Generieren des Namensformats für Dienstprinzipal- und Keytab-Dateien.
- ☐ Überprüfen des SPN und der Keytab-Format-Textdatei.
- ☐ Erstellen der SPNs und Keytab-Dateien.

Vorbereiten der Kerberos-Authentifizierung – Übersicht

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

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

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

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

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

Einrichten der Kerberos-Konfigurationsdatei

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

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

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

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

Parameter	Wert
default_realm	Der Name des Dienstbereichs für die Informatica-Domäne. Wenn Sie die Domäne in eine nicht native Umgebung integrieren, legen Sie die Eigenschaft default_realm so fest, dass sie mit der Eigenschaft default_realm des Clusters übereinstimmt.
forwardable	Ermöglicht es einem Dienst, Client-Benutzeranmeldedaten an einen anderen Dienst zu delegieren. Legen Sie diesen Parameter auf TRUE fest. Für die Informatica-Domäne müssen Anwendungsdienste die Client-Benutzeranmeldedaten bei anderen Diensten authentifizieren.
default_tkt_enctypes	Verschlüsselungstypen für den Sitzungsschlüssel in Ticket-Granting-Tickets (TGT). Legen Sie diesen Parameter nur fest, wenn Sitzungsschlüssel spezifische Verschlüsselungstypen verwenden müssen.
udp_preference_limit	Legt das Protokoll fest, das Kerberos beim Senden einer Meldung an den KDC verwendet. Legen Sie „udp_preference_limit = 1“ fest, damit immer TCP verwendet wird. Die Informatica-Domäne unterstützt nur das TCP-Protokoll. Wenn udp_preference_limit auf einen anderen Wert festgelegt wurde, wird die Informatica-Domäne eventuell unerwartet heruntergefahren.

- Schließen Sie im Abschnitt *Bereiche* die Portnummer in die Adresse des KDC ein (getrennt durch einen Doppelpunkt).

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

kdc = kerberos.example.com:88
- Speichern Sie die Datei krb5.conf.
- Speichern Sie die Datei krb5.conf in einem Verzeichnis, das auf dem Rechner zugänglich ist, wenn Sie die Informatica-Dienste installieren möchten.

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

```
[libdefaults]
default_realm = AFNIKRB.AFNIDEV.COM
forwardable = true
udp_preference_limit = 1

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

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

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

Generieren des Namensformats für Dienstprinzipale und Keytab-Dateien

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

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

Knotenebene

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

Prozessebene

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

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

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

Dienstprinzipalanforderungen auf der Knotenebene

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

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

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

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

Knotenprozess

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

HTTP-Prozesse in der Domäne

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

Dienstprinzipalanforderungen auf Prozessebene

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

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

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

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

Knotenprozess

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

Informatica Administrator-Dienst

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

HTTP-Prozesse in der Domäne

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

Dienstprozess

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

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

Ausführen des SPN-Formatgenerators

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

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

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

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

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

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

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

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

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

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

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

8. Geben Sie „2“ zum Beenden der Eingabeaufforderung **Dienst hinzufügen?** oder **Knoten hinzufügen?** ein.

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

9. Drücken Sie zum Beenden des SPN-Formatgenerators die Eingabetaste.

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

Überprüfen der SPN- und Keytab-Format-Textdatei

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

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

Die Textdatei enthält die folgenden Informationen:

Entitätsname

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

SPN

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

Ein SPN kann eines der folgenden Formate aufweisen:

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

Keytab-Dateiname

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

Die Keytab-Dateinamen verwenden die folgenden Formate:

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

Schlüsseltabellentyp

Der Typ der Schlüsseltabelle. Folgende Schlüsseltabellentypen sind möglich:

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

Dienstprinzipale auf der Knotenebene

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

```

ENTITY_NAME      SPN                                KEY_TAB_NAME
KEY_TAB_TYPE
Node01            isp/Node01/Infadomain@MY.SVCREALM.COM    Node01.keytab
NODE_SPN
Node01            HTTP/NodeHost01.enterprise.com@MY.SVCREALM.COM    webapp_http.keytab
NODE_HTTP_SPN
Node02            isp/Node02/Infadomain@MY.SVCREALM.COM    Node02.keytab
NODE_SPN
Node02            HTTP/NodeHost02.enterprise.com@MY.SVCREALM.COM    webapp_http.keytab
NODE_HTTP_SPN
Node03            isp/Node03/Infadomain@MY.SVCREALM.COM    Node03.keytab
NODE_SPN
Node03            HTTP/NodeHost03.enterprise.com@MY.SVCREALM.COM    webapp_http.keytab
NODE_HTTP_SPN

```

Dienstprinzipale auf der Prozessebene

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

```

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

```

```
Service200:Node02 Service200/Node02/Infadomain@MY.SVCREALM.COM
Service200.keytab SERVICE_PROCESS_SPN
```

Erstellen der Dienstprinzipalnamen und Keytab-Dateien

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

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

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

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

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

Aktivieren Sie die Delegation in Microsoft Active Directory.

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

Delegierte Authentifizierung tritt ein, wenn ein Benutzer mit einem Dienst authentifiziert wird und dieser Dienst die Anmeldedaten des authentifizierten Benutzers zum Herstellen einer Verbindung zu einem anderen Dienst verwendet. Da Dienste in der Informatica-Domäne eine Verbindung zu anderen Diensten herstellen müssen, um einen Vorgang abzuschließen, muss für die Informatica-Domäne die Delegierungsoption in Microsoft Active Directory aktiviert sein.

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

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

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

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

Fehlerbehebung bei den Dienstprinzipalnamen und Keytab-Dateien

Mit Kerberos-Dienstprogrammen können Sie überprüfen, ob die vom Kerberos-Administrator erstellten Dienstprinzipal- und Keytab-Dateinamen mit den von Ihnen angeforderten Dienstprinzipal- und Keytab-

Dateienamen übereinstimmen. Mit den Dienstprogrammen können Sie außerdem den Status des Kerberos-Schlüsselverteilungszentrums (KDC) ermitteln.

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

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

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

klist

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

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

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

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

kinit

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

```
kinit <user_account>
```

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

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

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

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

setspn

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

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

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

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

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

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

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

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

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

Existing SPN found!
```

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

```
setspn -X
```

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

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

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

kdestroy

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

KAPITEL 6

Aufzeichnen von Informationen für Abfragen des Installationsprogramms

Dieses Kapitel umfasst die folgenden Themen:

- [Checkliste zum Sammeln der Informationen für Abfragen des Installationsprogramms, 99](#)
- [Aufzeichnen von Informationen für Abfragen des Installationsprogramms – Übersicht, 100](#)
- [Domäne, 101](#)
- [Knoten, 102](#)
- [Verteilungspakete, 102](#)
- [Anwendungsdienste, 102](#)
- [Datenbanken , 103](#)
- [Verbindungszeichenfolge für eine sichere Datenbank, 105](#)
- [Sicherer Datenspeicher, 108](#)
- [Kerberos, 108](#)

Checkliste zum Sammeln der Informationen für Abfragen des Installationsprogramms

Dieses Kapitel beschreibt die Informationen, die Sie bei Ausführung des Installationsprogramms eingeben müssen. Zeichnen Sie anhand der folgenden Checkliste die erforderlichen Informationen auf, bevor Sie das Installationsprogramm ausführen:

- ☐ Die Namen der zu erstellenden Knoten sowie der Dienste, die auf dem jeweiligen Knoten erstellt werden sollen.
- ☐ Grundlegende Datenbankinformationen für jede Datenbank, die einem von Ihnen erstellten Dienst zugeordnet ist.
- ☐ Mit einer gesicherten Domänenkonfigurations-Repository- und Modellrepository-Datenbank: JDBC-Verbindungszeichenfolge mit den erforderlichen Sicherheitsparametern.
- ☐ Notieren Sie den Site-Schlüssel für das Installationsprogramm.

- ☐ Wenn beim Ausführen des Installationsprogramms Kerberos-Authentifizierung aktiviert werden soll: Kerberos-Informationen für jeden Knoten in der Domäne.

Aufzeichnen von Informationen für Abfragen des Installationsprogramms – Übersicht

Wenn Sie die Informatica-Dienste installieren, benötigen Sie Informationen über die Domäne, Knoten, Anwendungsdienste, Datenbanken und Verteilungspakete für die Umgebung.

Dieser Abschnitt enthält die Informationen, die bei Ausführung des Installationsprogramms angegeben werden müssen. Informatica empfiehlt, die Informationen für Abfragen des Installationsprogramms aufzuzeichnen, bevor Sie den Installationsvorgang starten. Sie können z. B. eine Textdatei mit Informationen erstellen, um sie in das Installationsprogramm zu kopieren.

Benennungskonventionen für Datenobjekte

Sie können die Namen von Domänen, Knoten und Anwendungsdiensten nicht ändern. Verwenden Sie Namen, die auch dann weiter zweckmäßig sind, wenn Sie einen Knoten auf einen anderen Computer migrieren oder wenn Sie weitere Knoten und Dienste an die Domäne anfügen. Verwenden Sie zudem Namen, aus denen hervorgeht, wie das Domänenobjekt verwendet wird. Benennungskonventionen finden Sie in den entsprechenden Themen.

Domäne

Wenn Sie eine Domäne erstellen, müssen Sie einen Domänennamen und einen Gateway-Knotennamen angeben.

In der folgenden Tabelle werden die Domäneninformationen beschrieben, die Sie während des Installationsvorgangs eingeben müssen:

Domäneninformationen	Beschreibung
Domänename	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: ` % * + ; " ? , < > \ / Ziehen Sie eine der folgenden Benennungskonventionen in Betracht: DMN, DOM, DOMAIN, _<ORG>_<ENV>
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. Ziehen Sie die folgende Benennungskonvention in Betracht: Knoten<Knoten-Nr.>_<ORG>_<optionale Unterscheidung>_<ENV>

Knoten

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

In der folgenden Tabelle werden die Knoteninformationen beschrieben, die Sie eingeben müssen, wenn Sie eine Domäne anfügen:

Knoteninformationen	Beschreibung
Hostname des Knotens	<p>Vollqualifizierter Hostname des Computers, auf dem Knoten erstellt werden sollen. Wenn der Computer nur einen Netzwerknamen aufweist, verwenden Sie den Standardhostnamen. Der Hostname des Knotens darf keine Unterstriche (_) enthalten.</p> <p>Wenn der Rechner mehrere Netzwerknamen aufweist, können Sie den Standard-Hostnamen ändern und einen alternativen Netzwerknamen verwenden. Wenn der Computer nur einen Netzwerknamen aufweist, verwenden Sie den Standardhostnamen.</p> <p>Hinweis: Verwenden Sie nicht localhost. Der Hostname muss den Computer eindeutig kennzeichnen.</p>
Knotenname	<p>Name der Knoten, die Sie auf diesem Computer erstellen möchten. Der Knotenname ist nicht mit dem Hostnamen des Computers identisch.</p> <p>Ziehen Sie die folgende Benennungskonvention in Betracht: Knoten<Knoten-Nr.>_<ORG>_<optionale Unterscheidung>_<ENV></p>

Verteilungspakete

Wenn Sie ein Verteilungspaket über das Installationsprogramm installieren, notieren Sie sich das heruntergeladene Verteilungspaket.

Anwendungsdienste

Zeichnen Sie die Namen der Anwendungsdienste sowie die Knoten auf, auf denen Sie sie erstellen möchten.

In der folgenden Tabelle sind die Anwendungsdienste aufgeführt, die Sie bei Ausführung des Installationsprogramms erstellen können:

Anwendungsdienst	Namenskonvention
Katalogdienst	CS_<ORG>_<ENV>
Content-Management	CMS_<ORG>_<ENV>
Datenintegrationsdienst	DIS_<ORG>_<ENV>
Data Privacy Management-Dienst	DPM_<ORG>_<ENV>

Anwendungsdienst	Namenskonvention
Interaktiver Datenvorbereitungsdienst	DPS_<ORG>_<ENV>
Enterprise Data Preparation	EDLS_<ORG>_<ENV>
Metadaten-Zugriffsdienst	MAS_<ORG>_<ENV>
Informatica-Cluster-Dienst	ICS_<ORG>_<ENV>
Modellrepository-Dienst	MRS_<ORG>_<ENV>
Überwachungsmodellrepository-Dienst	mMRS_<ORG>_<ENV>
PowerCenter-Repository-Dienst	PCRS, RS_<ORG>_<ENV>
PowerCenter-Integrationsdienst	PCIS, IS_<ORG>_<ENV>

Weitere Informationen über alle Konventionen zur Benennung von Diensten finden Sie im folgenden Artikel über die schnelle Anwendung von optimalen Vorgehensweisen in Informatica auf Informatica Network:

[Velocity Naming Conventions](#)

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

Datenbanken

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

Domäne

In der folgenden Tabelle werden die Informationen beschrieben, die Sie während des Installationsvorgangs eingeben müssen:

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

Content-Managementdienst

In der folgenden Tabelle werden die Informationen beschrieben, die Sie während des Installationsvorgangs eingeben müssen:

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

Datenintegrationsdienst

In der folgenden Tabelle werden die Informationen beschrieben, die Sie während des Installationsvorgangs eingeben müssen:

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

Modellrepository-Dienst

In der folgenden Tabelle werden die Informationen beschrieben, die Sie während des Installationsvorgangs eingeben müssen:

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

PowerCenter-Repository-Dienst

In der folgenden Tabelle werden die Informationen beschrieben, die Sie während des Installationsvorgangs eingeben müssen:

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

Verbindungszeichenfolge für eine sichere Datenbank

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

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

Sie können eine sichere Verbindung für die folgenden Datenbanken konfigurieren:

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL-Datenbank
- PostgreSQL
- Azure PostgreSQL
- Oracle

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

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

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

Parameter	Beschreibung
EncryptionMethod	Obligatorisch. Gibt an, ob Daten bei der Netzwerkübertragung verschlüsselt werden. Dieser Parameter muss auf <code>SSL</code> festgelegt werden.
ValidateServerCertificate	Optional. Gibt an, ob Informatica das Zertifikat validiert, das vom Datenbankserver gesendet wird. Wenn dieser Parameter auf "True" gesetzt wird, validiert Informatica das vom Datenbankserver gesendete Zertifikat. Wenn Sie den Parameter <code>HostNameInCertificate</code> angeben, validiert Informatica auch den Hostnamen im Zertifikat. Wenn dieser Parameter auf „false“ festgelegt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat nicht. Informatica ignoriert alle Truststore-Informationen, die Sie angeben.
HostNameInCertificate	Optional. Hostname des Computers, auf dem die gesicherte Datenbank gehostet wird. Wenn Sie einen Hostnamen angeben, validiert Informatica den Hostnamen in der Verbindungszeichenfolge mit dem Hostnamen im SSL-Zertifikat. Wenn SSL-Verschlüsselung und Validierung aktiviert sind und diese Eigenschaft nicht angegeben wurde, verwendet der Treiber den in der Verbindungs-URL oder der Datenquelle der Verbindung angegebenen Servernamen, um das Zertifikat zu validieren.
cryptoProtocolVersion	Obligatorisch. Gibt das Kryptografieprotokoll an, das für die Verbindung mit einer gesicherten 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> festlegen.

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

IBM DB2

```
jdbc:Informatica:db2://
<hostname>:<portnummer>;DatabaseName=<datenbankname>;EncryptionMethod=SSL;HostNameInCertificate=<datenbankhostname>;ValidateServerCertificate=<true oder false>
```

Oracle

```
jdbc:Informatica:oracle://
<hostname>:<portnummer>;ServiceName=<dienstname>;EncryptionMethod=SSL;HostNameInCertificate=<datenbankhostname>;ValidateServerCertificate=<true oder false>
```

Verwenden Sie die folgende Verbindungszeichenfolge, um eine Verbindung zur Oracle-Datenbank über den Oracle Connection Manager herzustellen:

```
jdbc:Informatica:oracle:TNSNamesFile=<vollqualifizierter Pfad zur Datei
tnsnames.ora>;TNSServerName=<TNS-Servername>;
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://
<hostname>:<portnummer>;SelectMethod=cursor;DatabaseName=<datenbankname>;EncryptionMethod=SSL;HostNameInCertificate=<datenbankhostname>;ValidateServerCertificate=<true oder false>
```

Microsoft SQL Server mit Windows NT-Anmeldeinformationen

Wenn Sie die Windows NT-Anmeldeinformationen für die Modellrepository-Datenbank in Microsoft SQL Server angegeben haben, schließen Sie die Authentifizierungsmethode mithilfe der Syntax der Verbindungszeichenfolge als NTLM ein.

Microsoft SQL Server, der die Standardinstanz mit Windows NT-Anmeldeinformationen verwendet:

```
"jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft SQL Server, der eine benannte Instanz mit Windows NT-Anmeldeinformationen verwendet:

```
"jdbc:informatica:sqlserver://<host name>\<named instance name>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft Azure SQL

```
jdbc:Informatica:sqlserver://  
<hostname>:<portnummer>;SelectMethod=cursor;DatabaseName=<datenbankname>;SnapshotSerializ  
able=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServe  
rCertificate=false
```

PostgreSQL

```
jdbc:Informatica:postgresql://  
<hostname>:<portnummer>;DatabaseName=<datenbankname>;EncryptionMethod=SSL;HostNameInCerti  
ficate=<datenbankhostname>;ValidateServerCertificate=<true oder false>
```

Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database  
name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLSv1.2;
```

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

Sicherer Datenspeicher

Wenn Sie die Informatica-Dienste installieren, müssen Sie den vom Installationsprogramm generierten Site-Schlüssel sichern und sicherstellen, dass Sie den Site-Schlüssel speichern. Wenn Sie den Site-Schlüssel verlieren, können Sie ihn nicht erneut generieren.

Zeichnen Sie in der folgenden Tabelle die Informationen auf, die Sie zur Konfiguration von sicherem Datenspeicher benötigen:

Eigenschaft	Beschreibung
Verzeichnis des Verschlüsselungsschlüssels	Verzeichnis, in dem der Verschlüsselungsschlüssel für die Domäne gespeichert werden soll. Standardmäßig wird der Verschlüsselungsschlüssel im folgenden Verzeichnis erstellt: <Informatica-Installationsverzeichnis>/isp/config/keys.
Geben Sie an, ob Sie den vom Installationsprogramm generierten Site-Schlüssel sichern möchten oder nicht.	<p>Geben Sie an, ob Sie den vom Installationsprogramm generierten Site-Schlüssel sichern möchten oder nicht.</p> <ul style="list-style-type: none">- Wählen Sie 1 für Nein. Wenn Sie Nein wählen, wird das Installationsprogramm beendet.- Wählen Sie 2 für JA. Wenn Sie Ja wählen, stimmen Sie zu, die Datei manuell zu sichern. <p>Ein eindeutiger Site-Schlüssel wird generiert. Wenn Sie den Site-Schlüssel verlieren, können Sie ihn nicht erneut generieren. Speichern Sie unbedingt eine Kopie dieses Schlüssels und teilen Sie den eindeutigen Site-Schlüssel nicht mit anderen.</p>

Kerberos

Wenn Sie die Informatica-Anwendungsdienste installieren, können Sie in der Informatica-Domäne Optionen aktivieren, um die Sicherheit von Domäne, Diensten und Datenbanken zu konfigurieren.

Wenn Sie die Kerberos-Authentifizierung aktivieren möchten, ohne die Standarddatei zu verwenden, müssen Sie Informationen wie Schlüsselspeicherverzeichnisse und Truststore-Verzeichnisse bereitstellen. Jeder Knoten muss einen Schlüsselspeicher und einen Truststore enthalten, der von allen Diensten auf diesem Knoten verwendet wird.

In der folgenden Tabelle werden Sicherheitsinformationen beschrieben, die während der Installation angegeben werden:

Sicherheitsinformationen	Beschreibung
Dienstbereichsname	Name des Kerberos-Bereichs, zu dem die Informatica-Domänendienste gehören. Der Bereichsname muss aus Großbuchstaben bestehen. Die Namen des Dienst- und Benutzerbereichs müssen übereinstimmen.
Benutzerbereichsname	Name des Kerberos-Bereichs, zu dem die Informatica-Domänenbenutzer gehören. Der Bereichsname muss aus Großbuchstaben bestehen. Die Namen des Dienst- und Benutzerbereichs müssen übereinstimmen.

Sicherheitsinformationen	Beschreibung
Speicherort der Kerberos-Konfigurationsdatei	Verzeichnis, in dem die Kerberos-Konfigurationsdatei namens <i>krb5.conf</i> gespeichert ist. Für Informatica müssen in der Konfigurationsdatei bestimmte Eigenschaften eingerichtet werden. Wenn Sie nicht über die Berechtigung zum Kopieren oder Aktualisieren der Kerberos-Konfigurationsdatei verfügen, müssen Sie unter Umständen den Kerberos-Administrator bitten, die Datei zu aktualisieren.
Schlüsselspeicherdatei-Verzeichnis	Verzeichnis, das die Schlüsselspeicherdateien enthält. Das Verzeichnis muss Dateien mit der Bezeichnung "infa_keystore.jks" und "infa_keystore.pem" enthalten.
Schlüsselspeicherpasswort	Ein Klartext-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.

KAPITEL 7

Einführung in das Dienste-Installationsprogramm

Dieses Kapitel umfasst die folgenden Themen:

- [Aufgaben des Dienste-Installationsprogramms, 110](#)
- [Sichere Dateien und Verzeichnisse, 110](#)
- [Vorinstallations-Dienstprogramme, 111](#)
- [Ausführen des Vorinstallations-Systemprüfungstools \(i10Pi\) im Konsolenmodus, 112](#)
- [Ausführen des Vorinstallations-Systemprüfungstools \(i10Pi\) im Grafikmodus, 115](#)
- [Ausführen des Vorinstallations-Systemprüfungstools \(i10pi\) im automatischen Modus, 121](#)

Aufgaben des Dienste-Installationsprogramms

Das Installationsprogramm führt die Installationsaufgaben für die zu installierenden Produkte aus.

Das Installationsprogramm kann die folgenden Aufgaben ausführen:

1. Validierung und Systemüberprüfung vor der Installation.
2. Erstellen einer Domäne oder Hinzufügen eines Knotens zu einer vorhandenen Domäne.
3. Installation von Binärdateien zur Unterstützung von Diensten.
4. Erstellen von Anwendungsdiensten.
5. Konfiguration der Sicherheit zwischen Domäne und Diensten.
6. Starten der erstellten Domänen- und Anwendungsdienste.
7. Schreiben von Meldungen in die Protokolldatei.

Sichere Dateien und Verzeichnisse

Wenn Sie Informatica installieren oder aktualisieren, erstellt das Installationsprogramm Verzeichnisse zum Speichern von Informatica-Dateien, die eingeschränkten Zugriff benötigen, wie z. B. die

Verschlüsselungsschlüsseldatei der Domäne und die Datei „nodemeta.xml“. Das Installationsprogramm weist verschiedene Berechtigungen für die Verzeichnisse und Dateien in den Verzeichnissen zu.

Standardmäßig erstellt das Installationsprogramm die folgenden Verzeichnisse im Informatica-Installationsverzeichnis:

<Informatica-Installationsverzeichnis>/isp/config

Enthält die Datei nodemeta.xml. Enthält außerdem das Verzeichnis „/keys“, in dem die Verschlüsselungsschlüsseldatei gespeichert ist. Wenn Sie die Domäne konfigurieren, um die Kerberos-Authentifizierung zu verwenden, enthält das Verzeichnis „/keys“ auch die Kerberos-Keytab-Dateien. Sie können ein anderes Verzeichnis festlegen, in dem die Dateien gespeichert werden sollen. Das Installationsprogramm weist dieselben Berechtigungen für das angegebene Verzeichnis wie das Standardverzeichnis zu.

<Informatica-Installationsverzeichnis>/services/shared/security

Wenn Sie die sichere Kommunikation für die Domäne aktivieren, enthält das Verzeichnis /secret den Schlüsselspeicher und die Truststore-Dateien für die standardmäßigen SSL-Zertifikate.

Zum Gewährleisten der Sicherheit der Verzeichnisse und Dateien beschränkt das Installationsprogramm den Zugriff auf die Verzeichnisse und die Dateien in den Verzeichnissen. Das Installationsprogramm weist der Gruppe und dem Benutzerkonto, die als Eigentümer der Verzeichnisse und Dateien fungieren, bestimmte Berechtigungen zu.

Weitere Informationen über die den Verzeichnissen und Dateien zugewiesenen Berechtigungen finden Sie im Informatica-Sicherheitshandbuch.

Vorinstallations-Dienstprogramme

Informatica stellt Dienstprogramme bereit, um die Installation der Informatica-Dienste zu vereinfachen. Sie können das Informatica-Installationsprogramm zum Ausführen von Dienstprogrammen verwenden.

Führen Sie die folgenden Dienstprogramme vor der Installation von Informatica-Diensten aus:

Vorinstallations-Systemprüfungstool (i10Pi)

Das Vorinstallations-Systemprüfungstool (i10Pi) überprüft, ob ein Computer die Systemanforderungen für die Informatica-Installation erfüllt. Informatica empfiehlt die Überprüfung der Mindestsystemanforderungen vor Beginn der Installation. Wenn Sie das Systemprüfungstool vor der Installation ausführen, legt das Installationsprogramm die Werte für bestimmte Felder (beispielsweise die Datenbankverbindung und die Domänenportnummern) basierend auf den während der Systemüberprüfung eingegebenen Daten fest.

Kerberos SPN-Formatgenerator von Informatica

Der Kerberos SPN-Formatgenerator von Informatica generiert eine Liste von Kerberos-SPNs (Dienstprinzipalnamen) und Keytab-Dateinamen im von Informatica benötigten Format. Wenn Sie Informatica in einem Netzwerk mit Kerberos-Authentifizierung installieren, führen Sie das Dienstprogramm aus, um Dienstprinzipalnamen und Keytab-Dateinamen im Informatica-Format zu generieren. Bitten Sie anschließend den Kerberos-Administrator, die SPNs zur Kerberos-Prinzipaldatenbank hinzuzufügen und die Keytab-Dateien zu erstellen. Beginnen Sie erst dann mit der Installation.

Ausführen des Vorinstallations-Systemprüfungstools (i10Pi) im Konsolenmodus

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

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

1. Melden Sie sich mit einem Systembenutzerkonto am Computer an.

2. Schließen Sie alle anderen Anwendungen.

3. Führen Sie die Installationsdatei über eine Shell-Befehlszeile aus.

Der Installer zeigt die Nachricht an, um sicherzustellen, dass die Gebietsschema-Umgebungsvariablen gesetzt sind.

4. Wurden die Umgebungsvariablen nicht eingestellt, drücken Sie **n**, um den Installer zu beenden. Stellen Sie sie anschließend entsprechend den Anforderungen ein.

Wenn die Umgebungsvariablen eingestellt sind, drücken Sie **y**, um fortzufahren.

5. Drücken Sie **1**, um die Installation oder das Upgrade von Informatica durchzuführen.

6. Drücken Sie **1**, um das Vorinstallations-Systemprüfungstool (i10Pi) auszuführen, mit dem sichergestellt wird, dass der Computer die Systemanforderungen für die Installation oder das Upgrade erfüllt.

7. Klicken Sie unter **Willkommen** im Vorinstallations-Systemprüfungstool (i10Pi) auf **Weiter**.

Der Abschnitt **Systeminformationen** wird angezeigt.

8. Geben Sie den absoluten Pfad für das Installationsverzeichnis ein.

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

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

9. Drücken Sie die **Eingabetaste**.

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

11. Drücken Sie die **Eingabetaste**.

Der Abschnitt **Datenbank- und Verbindungsinformationen** wird angezeigt.

12. Um die JDBC-Verbindungsdaten mithilfe einer benutzerdefinierten JDBC-Verbindungszeichenfolge einzugeben, drücken Sie **1**. Um die JDBC-Verbindungsdaten mithilfe der JDBC-URL-Daten einzugeben, drücken Sie **2**.

Zum Herstellen einer Verbindung zu einer sicheren Datenbank müssen Sie die JDBC-Verbindung mithilfe einer benutzerdefinierten JDBC-Verbindungszeichenfolge eingeben.

13. Geben Sie die JDBC-Verbindungsdaten ein.

- Um die Verbindungsdaten mithilfe einer benutzerdefinierten JDBC-Verbindungszeichenfolge einzugeben, geben Sie die Verbindungszeichenfolge ein und legen Sie die Verbindungsparameter fest.

Verwenden Sie die folgende Syntax in der JDBC-Verbindungszeichenfolge:

IBM DB2

```
jdbc:Informatica:db2://<hostname>:<portnummer>;DatabaseName=
```

Oracle

```
jdbc:Informatica:oracle://<hostname>:<portnummer>;ServiceName=
```

Verwenden Sie die folgende Verbindungszeichenfolge, um eine Verbindung zur Oracle-Datenbank über den Oracle Connection Manager herzustellen:

```
jdbc:Informatica:oracle:TNSNamesFile=<vollqualifizierter Pfad zur Datei  
tnsnames.ora>;TNSServerName=<TNS-Name>;
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://  
<hostname>:<portnummer>;SelectMethod=cursor;DatabaseName=
```

Microsoft SQL Server mit Windows NT-Anmeldeinformationen

Wenn Sie die Windows NT-Anmeldeinformationen für die Modellrepository-Datenbank in Microsoft SQL Server angegeben haben, schließen Sie die Authentifizierungsmethode mithilfe der Syntax der Verbindungszeichenfolge als NTLM ein.

Microsoft SQL Server, der die Standardinstanz mit Windows NT-Anmeldeinformationen verwendet:

```
"jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database  
name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft SQL Server, der eine benannte Instanz mit Windows NT-Anmeldeinformationen verwendet:

```
"jdbc:informatica:sqlserver://<host name>\<named instance  
name>;DatabaseName=<database  
name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft Azure SQL

```
jdbc:Informatica:sqlserver://  
<hostname>:<portnummer>;SelectMethod=cursor;DatabaseName=<datenbankname>;SnapshotS  
erializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net  
;ValidateServerCertificate=false
```

Azure SQL-Datenbank mit Active Directory-Authentifizierung

```
jdbc:informatica: sqlserver://  
<Hostname>:<Portnummer>;database=<Datenbankname>;encrypt=true;AuthenticationMethod  
=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertificate=*.data  
base.windows.net;loginTimeout=<Sekunden>
```

PostgreSQL

```
jdbc:Informatica:postgresql://<hostname>:<portnummer>;DatabaseName=
```

Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database  
name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TL  
Sv1.2;
```

Sybase

`jdbc:Informatica:sybase://<Hostname>:<Portnummer>;DatabaseName=`

Stellen Sie sicher, dass die Verbindungszeichenfolge alle vom Datenbanksystem benötigten Verbindungsparameter enthält.

- Um die Verbindungsdaten mithilfe der JDBC-URL-Daten einzugeben, legen Sie die JDBC-URL-Eigenschaften fest.
In der folgenden Tabelle werden die Verbindungsinformationen beschrieben:

Eingabeaufforderung	Beschreibung
Datenbanktyp	Der Datenbanktyp für das Domänen-Konfigurations-Repository. Treffen Sie eine Auswahl aus den folgenden Datenbanktypen: <ul style="list-style-type: none">- 1 – Oracle- 2 – Microsoft SQL Server- 3 – IBM DB2- 4 – Sybase ASE- 5 – PostgreSQL
Datenbankbenutzer-ID	Benutzer-ID des Datenbankbenutzerkontos für das Domänen-Konfigurations-Repository.
Passwort des Datenbankbenutzers	Das Passwort für das Datenbankbenutzerkonto.
Datenbank-Hostname	Hostname für den Datenbankserver.
Datenbank-Portnummer	Portnummer der Datenbank.
Datenbankdienstname	Dienstname für Oracle- und IBM DB2-Datenbanken oder Datenbankname für PostgreSQL, Microsoft SQL Server und Sybase ASE.

- Wenn Sie eine Verbindung zu einer sicheren Datenbank herstellen möchten, wählen Sie **1** aus, um eine benutzerdefinierte Zeichenfolge zu verwenden und die Verbindungszeichenfolge einzugeben. Neben den Verbindungsparametern müssen die Sicherheitsparameter berücksichtigt werden. Informationen zu den Sicherheitsparametern, die in die JDBC-Verbindung für eine sichere Datenbank aufgenommen werden müssen, finden Sie unter [“Verbindungszeichenfolge für eine sichere Datenbank” auf Seite 105](#).

Das Tool prüft die Einstellungen der Festplatte, die Verfügbarkeit der Ports und die Konfiguration der Datenbank. Nach abgeschlossener Systemprüfung werden im Abschnitt **Systemprüfungsübersicht** die Ergebnisse der Systemprüfung angezeigt.

14. Kontrollieren Sie die Ergebnisse der Systemprüfung.

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

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

Die Ergebnisse der Systemüberprüfung werden in der folgenden Datei gespeichert: ...<Informatica-Installationsverzeichnis>/Server/I10PI/I10PI/en/I10PI_summary.txt

15. Drücken Sie die **Eingabetaste**, um das Vorinstallations-Systemprüfungstool (i10Pi) zu schließen.

Sie können sofort mit der Installation oder dem Upgrade der Informatica-Dienste fortfahren oder die Systemprüfung beenden und zu einem späteren Zeitpunkt mit der Installation oder dem Upgrade fortfahren. Wenn Sie sofort mit der Installation oder dem Upgrade fortfahren, müssen Sie das Installationsprogramm nicht erneut starten.

16. Um die Installation fortzusetzen oder unmittelbar ein Upgrade durchzuführen, drücken Sie **y**.
Um die Systemprüfung zu beenden und die Installation bzw. das Upgrade zu einem späteren Zeitpunkt fortzusetzen, drücken Sie **n**.

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

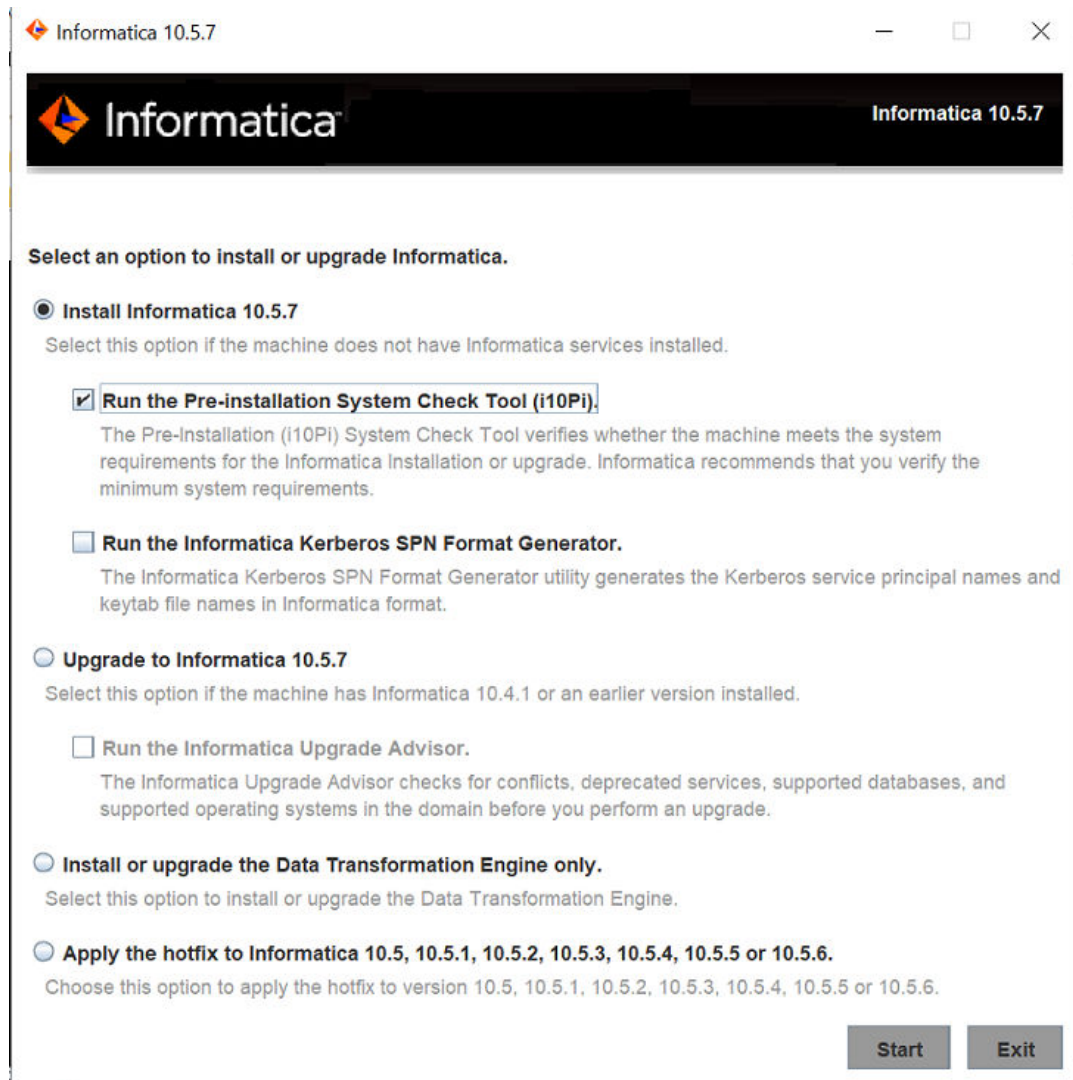
Hinweis: Die Installation oder das Upgrade von Informatica kann auch dann ausgeführt werden, wenn das Vorinstallations-Systemprüfungstool (i10Pi) nicht erfüllte Anforderungen ermittelt hat. Informatica empfiehlt jedoch dringend, sämtliche Probleme vor dem Fortsetzen der Installation oder des Upgrades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

Ausführen des Vorinstallations-Systemprüfungstools (i10Pi) im Grafikmodus

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

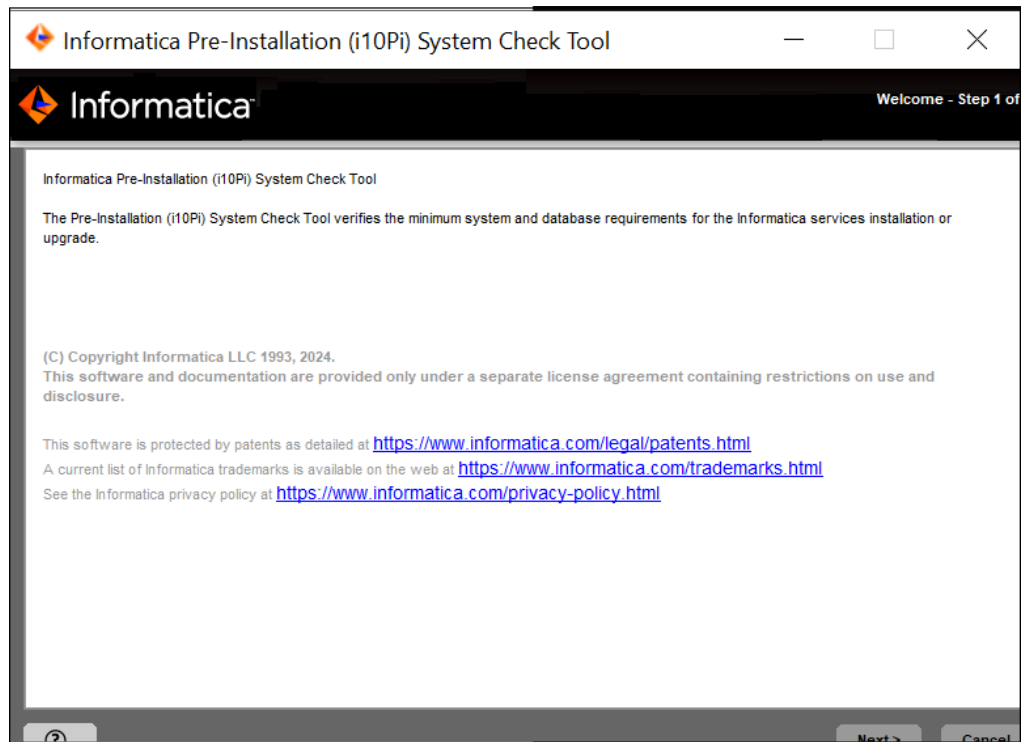
Stellen Sie sicher, dass Sie die Systemanforderungen überprüft und die Datenbank des Domänen-Konfigurations-Repository vorbereitet haben.

1. Melden Sie sich mit einem Systembenutzerkonto am Computer an.
2. Schließen Sie alle anderen Anwendungen.
3. Navigieren Sie zu dem Root-Verzeichnis, das die Installationsdateien enthält, und führen Sie die Datei „install.bat“ als Administrator aus.
4. Wählen Sie **Informatica 10.5.9 aus**.
5. Wählen Sie **Ausführen des Vorinstallations-Systemprüfungstools (i10Pi)**, um zu überprüfen, ob der Computer die Systemanforderungen für die Installation oder das Upgrade erfüllt.



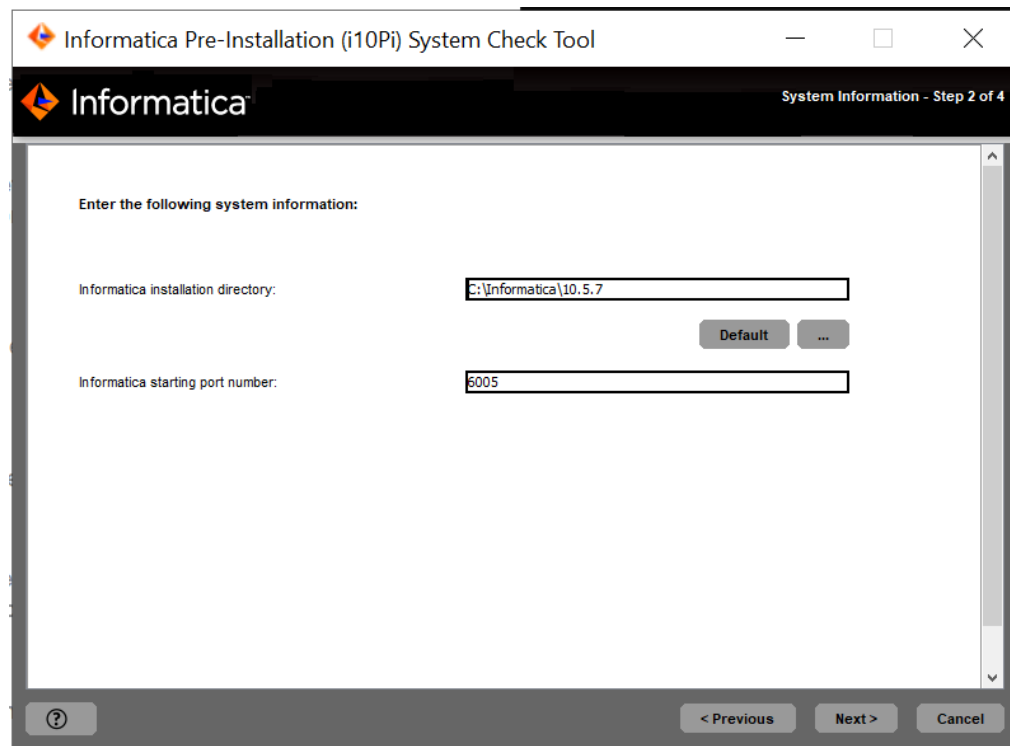
6. Klicken Sie auf **Start**.

Die Seite **Willkommen** im Vorinstallations-Systemprüfungstool (i10Pi) wird angezeigt.



7. Klicken Sie auf **Weiter**.

Die Seite **Systeminformationen** wird angezeigt.



8. Geben Sie den absoluten Pfad für das Installationsverzeichnis an.

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

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

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

Die Seite **Datenbank- und JDBC-Verbindungsinformationen** wird eingeblendet.

11. Geben Sie die Daten für die Datenbank des Domänen-Konfigurations-Repositorys ein.
In der folgenden Tabelle sind die Eigenschaften beschrieben, die Sie für die Datenbank und das Benutzerkonto festlegen:

Eigenschaft	Beschreibung
Datenbanktyp	Datenbank für das Repository. Wählen Sie eine der folgenden Datenbanken aus: <ul style="list-style-type: none"> - Oracle - IBM DB2 - Microsoft SQL Server - PostgreSQL - Sybase ASE
Datenbankbenutzer-ID	Benutzerkonto für die Repository-Datenbank.
Benutzerpasswort	Das Passwort für das Konto des Datenbankbenutzers.

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

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

Eigenschaft	Beschreibung
Datenbankadresse	Der Hostname und die Portnummer für die Datenbank im Format <code>host_name:port</code> .
Datenbankdienstname	Dienst- oder Datenbankname: <ul style="list-style-type: none"> - Oracle: Geben Sie den Dienstnamen ein. - Microsoft SQL Server: Geben Sie den Datenbanknamen ein. - IBM DB2: Geben Sie den Dienstnamen ein. - Sybase ASE: Geben Sie den Datenbanknamen ein. - PostgreSQL: Geben Sie den Namen der Datenbank ein.
JDBC-Parameter	Optionale Parameter, die in die Datenbankverbindungszeichenfolge aufgenommen werden können. Mit den Parametern können die Datenbankvorgänge für die Datenbank optimiert werden. Überprüfen Sie die Gültigkeit der Parameterzeichenfolge. Das Installationsprogramm führt vor dem Hinzufügen der Parameterzeichenfolge zur JDBC-URL keine Überprüfung der Zeichenfolge durch. Ist diese Option nicht aktiviert, erstellt das Installationsprogramm die JDBC-URL ohne zusätzliche Parameter.

- Um die Verbindungsdaten mithilfe einer benutzerdefinierten JDBC-Verbindungszeichenfolge einzugeben, wählen Sie **Benutzerdefinierte JDBC-Verbindungszeichenfolge** aus und geben Sie die Verbindungszeichenfolge ein.

Verwenden Sie die folgende Syntax in der JDBC-Verbindungszeichenfolge:

IBM DB2

```
jdbc:Informatica:db2://<hostname>:<portnummer>;DatabaseName=
```

Oracle

```
jdbc:Informatica:oracle://<hostname>:<portnummer>;ServiceName=
```

Verwenden Sie die folgende Verbindungszeichenfolge, um eine Verbindung zur Oracle-Datenbank über den Oracle Connection Manager herzustellen:

```
jdbc:Informatica:oracle:TNSNamesFile=<vollqualifizierter Pfad zur Datei  
tnsnames.ora>;TNSServerName=<TNS-Name>;
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://  
<hostname>:<portnummer>;SelectMethod=cursor;DatabaseName=
```

Microsoft SQL Server mit Windows NT-Anmeldeinformationen

Wenn Sie die Windows NT-Anmeldeinformationen für die Modellrepository-Datenbank in Microsoft SQL Server angegeben haben, schließen Sie die Authentifizierungsmethode mithilfe der Syntax der Verbindungszeichenfolge als NTLM ein.

Microsoft SQL Server, der die Standardinstanz mit Windows NT-Anmeldeinformationen verwendet:

```
"jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft SQL Server, der eine benannte Instanz mit Windows NT-Anmeldeinformationen verwendet:

```
"jdbc:informatica:sqlserver://<host name>\<named instance name>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft Azure SQL

```
jdbc:Informatica:sqlserver://  
<hostname>:<portnummer>;SelectMethod=cursor;DatabaseName=<datenbankname>;SnapshotS  
erializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net  
;ValidateServerCertificate=false
```

Azure SQL-Datenbank mit Active Directory-Authentifizierung

```
jdbc:informatica: sqlserver://  
<Hostname>:<Portnummer>;database=<Datenbankname>;encrypt=true;AuthenticationMethod  
=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertificate=*.data  
base.windows.net;loginTimeout=<Sekunden>
```

PostgreSQL

```
jdbc:Informatica:postgresql://<hostname>:<portnummer>;DatabaseName=
```

Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database  
name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TL  
Sv1.2;
```

Sybase

```
jdbc:Informatica:sybase://<Hostname>:<Portnummer>;DatabaseName=
```

Stellen Sie sicher, dass die Verbindungszeichenfolge alle vom Datenbanksystem benötigten Verbindungsparameter enthält.

- Wenn Sie die Option **Sichere Datenbank** auswählen, wählen Sie **Benutzerdefinierte JDBC-Verbindungszeichenfolge** und geben Sie die Verbindungszeichenfolge ein. Neben den Verbindungsparametern müssen die Sicherheitsparameter berücksichtigt werden. Informationen zu den Sicherheitsparametern, die in die JDBC-Verbindung für eine sichere Datenbank aufgenommen werden müssen, finden Sie unter ["Verbindungszeichenfolge für eine sichere Datenbank" auf Seite 105](#).

14. Klicken Sie auf **Verbindung testen**, um zu überprüfen, ob Sie eine Verbindung zur Datenbank herstellen können, und anschließend auf **OK**, um fortzufahren.
15. Klicken Sie auf **Weiter**, um die Systemprüfung zu starten.
Das Tool prüft die Einstellungen der Festplatte, die Verfügbarkeit der Ports und die Konfiguration der Datenbank. Nach abgeschlossener Systemprüfung wird die Seite **Systemprüfungsübersicht** angezeigt, auf der Sie die Ergebnisse der Systemprüfung sehen.
16. Kontrollieren Sie die Ergebnisse der Systemprüfung.

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

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

Die Ergebnisse der Systemüberprüfung werden in der folgenden Datei gespeichert: ...<Informatica-Installationsverzeichnis>/Server/I10PI/I10PI/en/I10PI_summary.txt

17. Klicken Sie auf **Fertig**, um das Vorinstallations-Systemprüfungstool (i10Pi) zu schließen.

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

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

Ausführen des Vorinstallations-Systemprüfungstools (i10pi) im automatischen Modus

Führen Sie das Vorinstallations-Systemprüfungstools (i10Pi) im automatischen Modus aus, um Systemanforderungen für die Installation ohne Benutzereingriff zu überprüfen.

1. Extrahieren Sie die Installationsprogrammdatei für Informatica-Dienste.
2. Navigieren Sie zu folgendem Speicherort:
`<Informatica-Installationsverzeichnis>/Server/I10PI`
3. Um die Eigenschaften für das Systemprüfungstool I10PI im automatischen Modus anzugeben, aktualisieren Sie die Datei `SilentInput.properties` im Ordner `I10PI`.
4. Um i10pi im automatischen Modus auszuführen, führen Sie die Datei `silentInstall` im Ordner `I10PI` aus.

Die Ergebnisse des Systemprüfungstools i10Pi im automatischen Modus finden Sie in der Datei `I10PI_summary.txt` im folgenden Speicherort:

`<Informatica-Installationsverzeichnis>/Server/I10PI/I10PI/en`

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

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

Teil III: Ausführen des Dienste-Installationsprogramms

Dieser Teil enthält die folgenden Kapitel:

- [Installation von Informatica-Diensten im Konsolenmodus, 123](#)
- [Installation von Informatica-Diensten im Grafikmodus, 175](#)
- [Ausführen des automatischen Installationsprogramms, 257](#)
- [Fehlerbehebung , 260](#)

KAPITEL 8

Installation von Informatica-Diensten im Konsolenmodus

Dieses Kapitel umfasst die folgenden Themen:

- [Installation von Informatica-Diensten - Übersicht, 123](#)
- [Erstellen einer Domäne, 123](#)
- [Anfügen einer Domäne, 159](#)

Installation von Informatica-Diensten - Übersicht

Sie können die Informatica-Dienste auf mehreren Rechnern installieren. Der Installationsprozess erstellt einen Dienst namens Informatica, der als Daemon ausgeführt wird.

Wenn Sie das Installationsprogramm zum ersten Mal ausführen, erstellen Sie eine Domäne. Wenn Sie eine Installation auf mehreren Computern durchführen und eine erstellte Domäne vorhanden ist, fügen Sie die Domäne an.

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 festlegen, dass zwischen Diensten innerhalb der Domäne sichere Kommunikation eingerichtet werden soll. Sie können sich auch dazu entscheiden, einige Anwendungsdienste während des Installationsvorgangs zu erstellen.

Wenn Sie eine Domäne anfügen, 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.

Hinweis: Beim Ausführen des Installationsprogramms im Konsolenmodus stellen die Wörter „Beenden“, „Hilfe“ und „Zurück“ reservierte Wörter dar. Verwenden Sie sie daher nicht als Eingabetext.

Erstellen einer Domäne

Erstellen Sie eine Domäne bei der Erstinstallation oder später, wenn Sie Knoten in separaten Domänen verwalten möchten.

Ausführen des Installationsprogramms

Führen Sie die folgenden Schritte aus, um das Installationsprogramm auszuführen:

1. Melden Sie sich mit einem Systembenutzerkonto am Computer an.
2. Verwenden Sie den folgenden Befehl, um die DISPLAY-Variable auf dem Computer zu löschen: `unset DISPLAY`
3. Schließen Sie alle anderen Anwendungen.
4. Führen Sie über eine Shell-Befehlszeile die Datei `install.sh` aus.
Der Installer zeigt die Nachricht an, um sicherzustellen, dass die Gebietsschema-Umgebungsvariablen gesetzt sind.
5. Wurden die Umgebungsvariablen nicht eingestellt, drücken Sie **n**, um den Installer zu beenden. Stellen Sie sie anschließend entsprechend den Anforderungen ein.
Wenn die Umgebungsvariablen eingestellt sind, drücken Sie **y**, um fortzufahren.

Willkommen beim Informatica-Installationsprogramm

- ▶ Drücken Sie **1**, um das Installationsprogramm auszuführen.
Im Installationsprogramm werden je nach Installationsplattform verschiedene Optionen angezeigt. Die folgenden Optionen werden angezeigt:
 - a. Drücken Sie **1**, um das Vorinstallations-Systemprüfungstools auszuführen.
Weitere Informationen zur Ausführung des Vorinstallations-Systemprüfungstools (i10Pi) finden Sie unter ["Ausführen des Vorinstallations-Systemprüfungstools \(i10Pi\) im Konsolenmodus" auf Seite 112](#).
 - b. Drücken Sie **2**, um den Kerberos SPN-Formatgenerator von Informatica auszuführen.
Weitere Informationen zur Ausführung des Kerberos SPN-Formatgenerators von Informatica finden Sie unter ["Ausführen des SPN-Formatgenerators " auf Seite 92](#).
 - c. Drücken Sie **3**, um das Installationsprogramm auszuführen.

Der Abschnitt **Willkommen** wird angezeigt.

Willkommen – Akzeptieren der allgemeinen Geschäftsbedingungen

- ▶ Lesen Sie die Bedingungen für die Informatica-Installation und das Toolkit zur Produktverwendung und wählen Sie **Ich stimme den Bedingungen zu** aus.
 - a. Drücken Sie **1**, wenn Sie die allgemeinen Geschäftsbedingungen nicht akzeptieren möchten.
 - b. Drücken Sie **2**, um die allgemeinen Geschäftsbedingungen zu akzeptieren.

Die Abschnitte zur **Komponentenauswahl** werden angezeigt.

Komponentenauswahl

Nachdem Sie die allgemeinen Geschäftsbedingungen akzeptiert haben, können Sie Informatica-Domänendienste installieren.

1. Drücken Sie **1**, um die Informatica-Domänendienste zu installieren.
Diese Option installiert Domänendienste der Version 10.5.9 und die Binärdateien des Anwendungsdiensts.

2. Wählen Sie aus, ob das Installationsprogramm in einem Netzwerk mit Kerberos-Authentifizierung ausgeführt werden soll.
 - a. Drücken Sie **1**, um die Informatica-Domäne zur Ausführung in einem Netzwerk ohne Kerberos-Authentifizierung zu konfigurieren.
 - b. Drücken Sie **2**, um die Informatica-Domäne zur Ausführung in einem Netzwerk mit Kerberos-Authentifizierung zu konfigurieren.
3. Wählen Sie aus, ob Sie Verteilungspakete über das Informatica-Installationsprogramm installieren möchten.
 - Drücken Sie **1**, wenn Sie keine Verteilungspakete benötigen oder diese später installieren möchten.
 - Drücken Sie **2**, wenn Sie Verteilungspakete über das Installationsprogramm installieren möchten.Standardwert ist 1.
4. Wenn Sie Verteilungspakete installieren möchten, wählen Sie ein oder mehrere Pakete aus der Liste aus, die Sie installieren möchten. Trennen Sie mehrere Pakete durch ein Komma.
Standardwert ist 1.

Im Abschnitt **Installationsvoraussetzungen** werden die Installationsanforderungen angezeigt. Stellen Sie sicher, dass alle Voraussetzungen erfüllt sind, bevor Sie die Installation fortsetzen.

Lizenz und Installationsverzeichnis

Nachdem Sie die Installationsvoraussetzungen überprüft haben, können Sie das Installationsverzeichnis angeben.

1. Geben Sie den absoluten Pfad für das Installationsverzeichnis an.
Die Verzeichnisnamen in dem Pfad dürfen weder Leerzeichen noch die folgenden Sonderzeichen enthalten: @ | * \$ # ! % () { } [] , ; '
Der Standardwert ist das Home-Verzeichnis des Benutzers, der die Informatica-Installation durchführt.
Hinweis: Informatica empfiehlt die Verwendung alphanumerischer Zeichen im Installationsverzeichnispfad. Wenn Sie ein Sonderzeichen wie á oder € verwenden, können zur Laufzeit unerwartete Ergebnisse auftreten.
2. Geben Sie den Pfad und Dateinamen des Informatica-Lizenzschlüssels ein und drücken Sie die **Eingabetaste**.
3. Geben Sie den Umgebungstyp an, der der Installation der Informatica-Dienste zugeordnet ist.
 - Drücken Sie **1**, um die Sandbox-Umgebung für eine Basisumgebung festzulegen, die für Machbarkeitsstudien mit minimaler Benutzerzahl verwendet wird.
 - Drücken Sie **2**, um die Entwicklungsumgebung für die Designumgebung festzulegen.
 - Drücken Sie **3**, um die Testumgebung für die Verarbeitung großer Datenmengen ähnlich der in einer Produktionsumgebung festzulegen.
 - Drücken Sie **4**, um die Produktionsumgebung für die massiv parallele Verarbeitung großer Datenmengen für Endbenutzer festzulegen. Bei erweiterten Produktionsumgebungen handelt es sich in der Regel um Setups mit mehreren Knoten.Der Standardwert ist „1“ für Sandbox.

Wenn Sie die Kerberos-Netzwerkauthentifizierung aktiviert haben, wird der Abschnitt **Dienstprinzipalebene** angezeigt.

Wenn Kerberos-Netzwerkauthentifizierung nicht aktiviert wurde, wird der Abschnitt **Vorinstallationsübersicht** angezeigt. Überprüfen Sie die Installationsinformationen und drücken Sie die **Eingabetaste**, um fortzufahren. Fahren Sie mit ["Domänenauswahl" auf Seite 127](#) fort.

Netzwerksicherheit – Dienstprinzipalebene

Nachdem Sie das Installationsverzeichnis angegeben haben, können Sie die Sicherheitsstufe konfigurieren.

- Wählen Sie im Abschnitt **Dienstprinzipalebene** die Ebene aus, auf der Sie die Kerberos-Dienstprinzipale für die Domäne festlegen möchten.

Hinweis: Alle Knoten in der Domäne müssen die gleiche Dienstprinzipalebene verwenden. Wenn Sie einen Knoten zu einer Domäne hinzufügen, wählen Sie die gleiche Dienstprinzipalebene aus, die vom Gateway-Knoten in der Domäne verwendet wird.

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

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

Der Abschnitt **Netzwerksicherheit – Kerberos-Authentifizierung** wird angezeigt.

Network Security - Kerberos Authentication

After you configure the security level, you can configure Kerberos authentication.

- In the **Network Security - Kerberos Authentication** section, enter the parameters required for Kerberos authentication.

The following table describes the Kerberos authentication parameters that you must set:

Property	Description
Domain name	Name of the domain. The name must not exceed 128 characters and must be 7-bit ASCII only. The name cannot contain a space or any of the following characters: ` % * + ; " ? , < > \ /
Node name	Name of the Informatica node.
Node host name	Fully qualified host name or the IP address of the machine on which to create the node. The node host name cannot contain the underscore (.) character. Hinweis: Do not use <i>localhost</i> . The host name must explicitly identify the machine.

Property	Description
Service realm name	Name of the Kerberos realm to which the Informatica domain services belong. The realm name must be in uppercase. The service realm name and the user realm name must be the same.
User realm name	Name of the Kerberos realm to which the Informatica domain users belong. The realm name must be in uppercase. The service realm name and the user realm name must be the same.
Keytab directory	Directory where all keytab files for the Informatica domain are stored. The name of a keytab file in the Informatica domain must follow a format set by Informatica.
Fully qualified path to the kerberos configuration file	Path and file name of the Kerberos configuration file. Informatica requires the following name for the Kerberos configuration file: <i>krb5.conf</i>

Wichtig: If you configure the domain to run with Kerberos authentication, the domain and node name and the node host name must match the names you specified when you ran the Informatica Kerberos SPN Format Generator to generate SPN and keytab file names. If you use a different domain, node, or host name, generate the SPN and keytab file names again and ask the Kerberos administrator to add the new SPN to the Kerberos principal database and create the keytab files.

The **Pre-Installation Summary** section appears. Review the installation information.

Domänenauswahl

Nachdem Sie sich die Vorinstallationszusammenfassung durchgesehen haben, können Sie die Domäneninformationen eingeben.

1. 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.

2. Legen Sie fest, ob Sie für Dienste in der Domäne sichere Kommunikation aktivieren möchten.

- a. Drücken Sie **1**, um sichere Kommunikation für die Domäne zu deaktivieren.
- b. Drücken Sie **2**, um sichere Kommunikation für die Domäne zu aktivieren.

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.

3. Geben Sie die Verbindungsdetails für Informatica Administrator ein.

- a. Wenn Sie sichere Kommunikation für die Domäne nicht aktivieren, können Sie angeben, ob eine sichere HTTPS-Verbindung für Informatica Administrator eingerichtet werden soll.

In der folgenden Tabelle werden die zum Aktivieren oder Deaktivieren einer sicheren Verbindung mit Informatica Administrator verfügbaren Optionen beschrieben:

Option	Beschreibung
HTTPS für Informatica Administrator aktivieren	Richten Sie eine sichere Verbindung zu Informatica Administrator ein.
HTTPS deaktivieren	Richten Sie keine sichere Verbindung zu Informatica Administrator ein.

- b. Wenn Sie die sichere Kommunikation für die Domäne oder eine HTTPS-Verbindung für Informatica Administrator aktivieren, geben Sie die Schlüsselspeicherdatei und Portnummer für die HTTPS-Verbindung ein.

In der folgenden Tabelle werden die Verbindungsinformationen beschrieben, die Sie bei Aktivierung von HTTPS eingeben müssen:

Option	Beschreibung
Port	Die Portnummer für die HTTPS-Verbindung.
Schlüsselspeicherdatei	<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.
- d. Wenn Sie die sichere Kommunikation für die Domäne aktiviert haben, wird der Abschnitt **Domänensicherheit – Sichere Kommunikation** angezeigt.
- e. Wenn sichere Kommunikation für die Domäne nicht aktiviert wurde, wird der Abschnitt **Domänenkonfigurations-Repository** angezeigt. Fahren Sie mit ["Domain Configuration Repository" auf Seite 132](#) fort.
4. Legen Sie fest, ob SAML-Authentifizierung aktiviert werden soll, um für webbasierte Informatica-Anwendungen in einer Informatica-Domäne SAML-basierte (Security Assertion Markup Language) Unterstützung von Single Sign-On (SSO) zu konfigurieren.
- Drücken Sie **1**, um die SAML-Authentifizierung zu deaktivieren, und fahren Sie mit ["Domänensicherheit – Sichere Kommunikation" auf Seite 130](#) fort. Drücken Sie **2**, um die SAML-Authentifizierung zu aktivieren und zu konfigurieren.
5. Geben Sie die URL des Identitäts-Providers für die Domäne ein.
6. Geben Sie den Vertrauensstellungsamen der vertrauenswürdigen Partei oder die Dienstanbieter-ID für die Domäne an, wie im Identitätsanbieter definiert. Wenn Sie „Nein“ auswählen, wird die Dienstanbieter-ID auf „Informatica“ festgelegt.
7. Geben Sie an, ob der IdP die SAML-Assertion signiert oder nicht.

8. Geben Sie den Aliasnamen des Signierzertifikats für die Identitätsanbieter-Assertion ein.
9. Legen Sie fest, ob Sie zum Aktivieren der SAML-Authentifizierung in der Domäne SSL-Standardzertifikate von Informatica oder eigene SSL-Zertifikate verwenden möchten.

In der folgenden Tabelle werden die SSL-Zertifikatsoptionen für die SAML-Authentifizierung beschrieben:

Option	Beschreibung
Standardmäßige SSL-Zertifikatsdatei von Informatica verwenden.	Wählen Sie diese Option aus, um für die SAML-Authentifizierung die Truststore-Standarddatei von Informatica zu verwenden.
Speicherort der SSL-Zertifikatsdatei eingeben.	Wählen Sie diese Option, um eine benutzerdefinierte Informatica-Truststore-Datei für die SAML-Authentifizierung zu verwenden. Geben Sie das Verzeichnis an, das die benutzerdefinierte Truststore-Datei auf Gateway-Knoten in der Domäne enthält. Geben Sie nur das Verzeichnis an, nicht den vollständigen Dateipfad.

10. Wenn Sie die Sicherheitszertifikate bereitstellen, geben Sie den Speicherort und die Passwörter der Schlüsselspeicher- und Truststore-Dateien an.

In der folgenden Tabelle werden Verzeichnis und Passwort der Truststore- und Schlüsselspeicherdateien beschrieben:

Eigenschaft	Beschreibung
Truststore-Verzeichnis	Geben Sie das Verzeichnis an, das die benutzerdefinierte Truststore-Datei auf Gateway-Knoten in der Domäne enthält. Geben Sie nur das Verzeichnis an, nicht den vollständigen Dateipfad.
Truststore-Passwort	Das Passwort für die benutzerdefinierte Truststore-Datei.
Schlüsselspeicherverzeichnis	Geben Sie das Verzeichnis an, das die benutzerdefinierte Schlüsselspeicherdatei enthält.
Schlüsselspeicherpasswort	Das Passwort für die benutzerdefinierte Schlüsselspeicherdatei.

11. Geben Sie zum Festlegen des Authentifizierungskontextvergleichs den Stärkevergleich des vom Benutzer verwendeten Authentifizierungsmechanismus mit dem IdP-Server an.
Unterstützte Werte sind die Optionen MINIMUM, MAXIMUM, BETTER oder EXACT. Standard ist MINIMUM.
12. Geben Sie zum Festlegen der Authentifizierungskontextklasse den erwarteten Mechanismus für die erstmalige Authentifizierung des Benutzers beim IdP-Server an.
Unterstützte Werte sind PASSWORD oder PASSWORDPROTECTEDTRANSPORT. Standard ist PASSWORD.
13. Geben Sie an, ob die Webanwendung die SAML-Authentifizierungsanforderung signieren soll oder nicht.
Der Standardwert ist „Deaktiviert“.
14. Geben Sie den Aliasnamen des privaten Schlüssels an, der in den SAML-Schlüsselspeicher des Knotens importiert wurde mit dem die SAML-Anfrage signiert werden soll.
15. Geben Sie das Passwort für den Zugriff auf den privaten Schlüssel an, der zum Signieren der SAML-Anforderung verwendet wird.
16. Geben Sie den Algorithmus an, den die Webanwendung zum Signieren der SAML-Anforderung verwendet.

Unterstützte Werte sind RSA_SHA256, DSA_SHA1, DSA_SHA256, RSA_SHA1, RSA_SHA224, RSA_SHA384, RSA_SHA512, ECDSA_SHA1, ECDSA_SHA224, ECDSA_SHA256, ECDSA_SHA384, ECDSA_SHA512, RIPEMD160 oder RSA_MD5.

17. Geben Sie an, ob IdP die SAML-Antwort signieren soll oder nicht.
Wählen Sie mit dieser Option, ob die Web-App die signierte SAML-Antwort empfangen kann oder nicht. Der Standardwert ist „Deaktiviert“.
18. Geben Sie an, ob der IdP die SAML-Assertion verschlüsselt oder nicht.
Wählen Sie diese Option, damit die Web-App eine verschlüsselte SAML-Assertion empfangen kann. Der Standardwert ist „Aktiviert“.
19. Geben Sie den Aliasnamen des privaten Schlüssels im SAML-Truststore des Gateway-Knotens an, den Informatica zum Entschlüsseln der SAML-Assertion verwendet.
20. Geben Sie das Passwort für den Zugriff auf den privaten Schlüssel an, der zum Entschlüsseln des Assertion-Verschlüsselungsschlüssels verwendet wird.
21. Klicken Sie auf **Weiter**.

Der Abschnitt **Domänensicherheit – Sichere Verbindung** wird angezeigt.

Domänensicherheit – Sichere Kommunikation

Nachdem Sie die Domänen konfiguriert haben, können Sie die Domänensicherheit konfigurieren.

- Geben Sie im Abschnitt „Domänensicherheit – Sichere Kommunikation“ an, ob die standardmäßigen SSL-Zertifikate von Informatica oder eigene SSL-Zertifikate zum Sichern der Domänenkommunikation verwendet werden sollen.
 - a. Wählen Sie den Typ der zu verwendenden SSL-Zertifikate aus.

In der folgenden Tabelle werden die Optionen für die SSL-Zertifikate beschrieben, die Sie zum Sichern der Informatica-Domäne verwenden können:

Option	Beschreibung
SSL-Standardzertifikatsdateien von Informatica verwenden	<p>Verwenden Sie die im Standardschlüsselspeicher und im Truststore enthaltenen SSL-Standardzertifikate.</p> <p>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.</p>
Benutzerdefinierte SSL-Zertifikate verwenden	<p>Geben Sie den Pfad für die Schlüsselspeicherdateien und Truststore-Dateien ein, die die SSL-Zertifikate enthalten. Sie müssen außerdem die Passwörter für Schlüsselspeicher und Truststore angeben.</p> <p>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.</p> <p>Informatica benötigt bestimmte Namen für die SSL-Zertifikatsdateien in der Informatica-Domäne. Sie müssen für alle Knoten in der Domäne dieselben SSL-Zertifikate verwenden.</p> <p>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.</p>

- 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 eine Datei namens <code>infa_keystore.jks</code> enthalten.
Schlüsselspeicherpasswort	Passwort für den Schlüsselspeicher „ <code>infa_keystore.jks</code> “.
Verzeichnis der Truststore-Datei	Verzeichnis, das die Truststore-Dateien enthält. Das Verzeichnis muss Dateien mit der Bezeichnung „ <code>infa_truststore.jks</code> “ und „ <code>infa_truststore.pem</code> “ enthalten.
Truststore-Passwort	Passwort für die Datei <code>infa_truststore.jks</code> .

Der Abschnitt **Domänen-Konfigurations-Repository** wird angezeigt.

Domain Configuration Repository

After you configure domain security, you can configure domain repository details.

1. Select the database to use for the domain configuration repository details.

The following table lists the databases you can use for the domain configuration repository:

Prompt	Description
Database type	Type of database for the domain configuration repository. Select from the following options: 1 - Oracle 2 - Microsoft SQL Server 3 - IBM DB2 4 - Sybase ASE 5 - PostgreSQL

The Informatica domain configuration repository stores metadata for domain operations and user authentication. The domain configuration repository must be accessible to all gateway nodes in the domain.

2. Enter the properties for the database user account.

The following table lists the properties for the database user account:

Property	Description
Database user ID	Name for the domain configuration database user account.
User password	Password for the domain configuration database user account.

3. Select whether to create a secure domain configuration repository.

You can create a domain configuration repository in a database secured with the SSL protocol. To create a domain configuration repository in a secure database, press 1 and skip to step to create a domain configuration repository.

To create a domain configuration repository in an unsecure database, press 2.

4. If you do not create a secure domain configuration repository, enter the parameters for the database.
 - a. If you select IBM DB2, select whether to configure a tablespace and enter the tablespace name.

The following table describes the properties that you must configure for the IBM DB2 database:

Eigenschaft	Beschreibung
Tablespace konfigurieren	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“ auswählen. Wählen Sie aus, ob ein Tablespace festgelegt werden soll. 1 – Nein 2 – Ja
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. Geben Sie in einer Datenbank mit einer einzigen Partition den Namen des Tablespace ein, in dem die Tabellen erstellt werden sollen. Geben Sie in einer Datenbank mit mehreren Partitionen den Namen des nicht partitionierten Tablespace an, der sich in der Katalogpartition der Datenbank befindet.

- b. If you select Microsoft SQL Server or PostgreSQL, enter the schema name for the database.

The following table describes the properties that you must configure for the database:

Eigenschaft	Beschreibung
Schemaname	Der Name des Schemas, das Domänenkonfigurationstabellen enthalten soll. Ist dieser Parameter leer, werden die Tabellen im Standardschema erstellt.

- c. To enter the JDBC connection information using the JDBC URL information, press **1**. To enter the JDBC connection information using a custom JDBC connection string, press **2**.

- d. Enter the JDBC connection information.

- To enter the connection information using the JDBC URL information, specify the JDBC URL properties.

The following table describes the database connection information:

Eingabeaufforderung	Beschreibung
Hostname der Datenbank	Hostname für die Datenbank
Portnummer der Datenbank	Die Portnummer für die Datenbank.

Eingabeaufforderung	Beschreibung
Datenbankdienstname	Dienst- oder Datenbankname: - Oracle: Geben Sie den Dienstnamen ein. - Microsoft SQL Server: Geben Sie den Datenbanknamen ein. - IBM DB2: Geben Sie den Dienstnamen ein. - Sybase ASE: Geben Sie den Datenbanknamen ein. - PostgreSQL: Geben Sie den Namen der Datenbank ein.
Konfigurieren von JDBC-Parametern	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.

- To enter the connection information using a custom JDBC connection string, type the connection string.

Verwenden Sie die folgende Syntax in der JDBC-Verbindungszeichenfolge:

IBM DB2

```
jdbc:Informatica:db2://<hostname>:<portnummer>;DatabaseName=
```

Oracle

```
jdbc:Informatica:oracle://<hostname>:<portnummer>;ServiceName=
```

Verwenden Sie die folgende Verbindungszeichenfolge, um eine Verbindung zur Oracle-Datenbank über den Oracle Connection Manager herzustellen:

```
jdbc:Informatica:oracle:TNSNamesFile=<vollqualifizierter Pfad zur Datei  
tnsnames.ora>;TNSServerName=<TNS-Name>;
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://  
<hostname>:<portnummer>;SelectMethod=cursor;DatabaseName=
```

Microsoft SQL Server mit Windows NT-Anmeldeinformationen

Wenn Sie die Windows NT-Anmeldeinformationen für die Modellrepository-Datenbank in Microsoft SQL Server angegeben haben, schließen Sie die Authentifizierungsmethode mithilfe der Syntax der Verbindungszeichenfolge als NTLM ein.

Microsoft SQL Server, der die Standardinstanz mit Windows NT-Anmeldeinformationen verwendet:

```
"jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database  
name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft SQL Server, der eine benannte Instanz mit Windows NT-Anmeldeinformationen verwendet:

```
"jdbc:informatica:sqlserver://<host name>\<named instance  
name>;DatabaseName=<database  
name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft Azure SQL

```
jdbc:Informatica:sqlserver://  
<hostname>:<portnummer>;SelectMethod=cursor;DatabaseName=<datenbankname>;Snap  
shotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.win  
dows.net;ValidateServerCertificate=false
```

Azure SQL-Datenbank mit Active Directory-Authentifizierung

```
jdbc:informatica: sqlserver://  
<Hostname>:<Portnummer>;database=<Datenbankname>;encrypt=true;AuthenticationMe  
thod=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertificat  
e=*.database.windows.net;loginTimeout=<Sekunden>
```

PostgreSQL

```
jdbc:Informatica:postgresql://<hostname>:<portnummer>;DatabaseName=
```

Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database  
name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersio  
n=TLSv1.2;
```

Sybase

```
jdbc:Informatica:sybase://<Hostname>:<Portnummer>;DatabaseName=
```

Stellen Sie sicher, dass die Verbindungszeichenfolge alle vom Datenbanksystem benötigten Verbindungsparameter enthält.

5. If you create a secure domain configuration repository, enter the parameters for the secure database.
If you create the domain configuration repository on a secure database, you must provide the truststore information for the database.

The following table describes the options available to create a secure domain configuration repository database:

Eigenschaft	Beschreibung
Datenbank-Truststore-Datei	Pfad und Dateiname der Truststore-Datei für die gesicherte Datenbank.
Datenbank-Truststore-Passwort	Passwort für die Truststore-Datei.
Benutzerdefinierte JDBC-Verbindungszeichenfolge	JDBC-Verbindungszeichenfolge zum Herstellen einer Verbindung mit der gesicherten Datenbank, einschließlich Hostname, Portnummer und Sicherheitsparameter für die Datenbank.

In addition to the host name and port number for the database server, you must include the following secure database parameters:

EncryptionMethod

Required. Indicates whether data is encrypted when transmitted over the network. This parameter must be set to `SSL`.

ValidateServerCertificate

Optional. Indicates whether Informatica validates the certificate that the database server sends.

If this parameter is set to True, Informatica validates the certificate that the database server sends. If you specify the `HostNameInCertificate` parameter, Informatica also validates the host name in the certificate.

If this parameter is set to False, Informatica does not validate the certificate that the database server sends. Informatica ignores any truststore information that you specify

Default is True.

HostNameInCertificate

Optional. Host name of the machine that hosts the secure database. If you specify a host name, Informatica validates the host name included in the connection string against the host name in the SSL certificate.

cryptoProtocolVersion

Required. Specifies the cryptographic protocol to use to connect to a secure database. You can set the parameter to `cryptoProtocolVersion=TLSv1.1` or `cryptoProtocolVersion=TLSv1.2` based on the cryptographic protocol used by the database server.

You must also provide a JDBC connection string that includes the security parameters for the database. You can use the following syntax for the connection strings:

- **Oracle:** `jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=<service name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>`
- **IBM DB2:** `jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>`
- **Microsoft SQL Server:** `jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>`
- **Microsoft SQL Server with Windows NT credentials:**
If you have previously specified the Windows NT credentials for the Model repository database on Microsoft SQL Server, specify the connection string syntax to include the authentication method as NTLM.
 - Microsoft SQL Server that uses the default instance with Windows NT credentials:
`"jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"`
 - Microsoft SQL Server that uses a named instance with Windows NT credentials:
`"jdbc:informatica:sqlserver://<host name>\<named instance name>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"`

- **Microsoft Azure SQL:** jdbc:Informatica:sqlserver://<host name:port number>;SelectMethod=cursor;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>
- **PostgreSQL:** jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>
- **Azure PostgreSQL:** jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLSv1.2;

Hinweis: The installer does not validate the connection string. Verify that the connection string contains all the connection parameters and security parameters required by your database.

6. If the database contains a domain configuration repository for a previous domain, select to overwrite the data or set up another database.
 - a. Press 1 for OK to enter the connection information for a new database.
 - b. Press 2 for Continue for the installer to overwrite the data in the database with new domain configuration.

The **Domain Security - Encryption Key** section appears.

Domänensicherheit – Verschlüsselungsschlüssel

Nachdem Sie das Domänen-Repository konfiguriert haben, können Sie den Verschlüsselungsschlüssel konfigurieren.

- Geben Sie im Abschnitt **Domänensicherheit – Verschlüsselungsschlüssel** das Verzeichnis für den Verschlüsselungsschlüssel in der Informatica-Domäne ein.

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

Eigenschaft	Beschreibung
Verzeichnis des Verschlüsselungsschlüssels	Verzeichnis, in dem der Verschlüsselungsschlüssel für die Domäne gespeichert werden soll. Standardmäßig wird der Verschlüsselungsschlüssel in folgendem Verzeichnis erstellt: <Informatica-Installationsverzeichnis>/isp/config/keys.
Geben Sie an, ob Sie den vom Installationsprogramm generierten Site-Schlüssel sichern möchten oder nicht	<p>Ein eindeutiger Site-Schlüssel wird generiert. Wenn Sie den Site-Schlüssel verlieren, können Sie ihn nicht erneut generieren. Speichern Sie unbedingt eine Kopie dieses Schlüssels und teilen Sie den eindeutigen Site-Schlüssel nicht mit anderen.</p> <p>Geben Sie an, ob Sie den vom Installationsprogramm generierten Site-Schlüssel sichern möchten oder nicht:</p> <ul style="list-style-type: none"> - Wählen Sie 1 für Nein. Wenn Sie „Nein“ wählen, generiert das Installationsprogramm einen Fehler. Drücken Sie die Eingabetaste, um fortzufahren. - Wählen Sie 2 für JA. Wenn Sie Ja wählen, stimmen Sie zu, die Datei manuell zu sichern.

Das Installationsprogramm legt verschiedene Berechtigungen für das Verzeichnis und die Dateien im Verzeichnis fest. Weitere Informationen über die Berechtigungen für die Verschlüsselungsschlüsseldatei und das Verzeichnis finden Sie unter ["Sichere Dateien und Verzeichnisse" auf Seite 110](#).

Der Abschnitt **Domänen- und Knotenkonfiguration** wird angezeigt.

Domänen- und Knotenkonfiguration

Nachdem Sie den Verschlüsselungsschlüssel konfiguriert haben, können Sie die Domäne und den Knoten konfigurieren.

- 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 die Domäne und den Gateway-Knoten festlegen:

Eigenschaft	Beschreibung
Domänenname	<p>Name der zu erstellenden Informatica-Domäne. Der Standardname der Domäne lautet Domain_<MachineName>.</p> <p>Der Name darf maximal 128 Zeichen umfassen und muss im 7-Bit-ASCII-Format vorliegen. Der Name darf weder Leerzeichen noch eines der folgenden Zeichen enthalten: ` % * + ; " ? , < > \ /</p>
Knotenname	Name des zu erstellenden Knotens.

Eigenschaft	Beschreibung
Hostname des Knotens	<p>Hostname oder IP-Adresse des Computers, auf dem der Knoten erstellt werden soll.</p> <p>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.</p> <p>Hinweis: Der Hostname des Knotens darf keine Unterstriche (_) enthalten. Verwenden Sie nicht localhost. Der Hostname muss den Computer eindeutig kennzeichnen.</p>
Portnummer des Knotens	<p>Die Portnummer für den Knoten. Die Standardportnummer für den Knoten lautet 6005. Wenn die Portnummer auf dem Rechner nicht verfügbar ist, zeigt das Installationsprogramm die nächste verfügbare Portnummer an.</p>
Domänenbenutzername	<p>Benutzername für den Domänenadministrator. Sie können diesen Benutzernamen für die 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 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.

2. Wählen Sie aus, ob die Passwortkomplexität zum Sichern vertraulicher Daten in der Domäne aktiviert werden soll.

In der folgenden Tabelle wird die Passwortkomplexität beschrieben:

Eigenschaft	Beschreibung
Passwortkomplexität	<p>Wählen Sie aus, ob die Passwortkomplexität aktiviert werden soll.</p> <p>1 – Ja 2 – Nein</p> <p>Wenn Sie „Ja“ auswählen, muss das Passwort die folgenden Anforderungen erfüllen: Es muss mindestens acht Zeichen lang sein und mindestens ein alphabetisches Zeichen, ein numerisches Zeichen und ein Sonderzeichen enthalten.</p>
Passwortrichtlinie konfigurieren	<p>Wählen Sie aus, ob eine Passwortrichtlinie konfiguriert werden soll.</p> <p>1 – Ja 2 – Nein</p> <p>Wenn Sie „Ja“ auswählen, können Sie Passwortkomplexitätsregeln konfigurieren. Wenn Sie „Nein“ auswählen, gelten die Standardregeln der Informatica-Passwortrichtlinie.</p>
Anzahl der Sonderzeichen	<p>Die Mindestanzahl der erforderlichen Sonderzeichen in einem Passwort.</p> <p>Sie können die folgenden Sonderzeichen verwenden: " # \$ % & ' () * + , - . / : ; < = > ? @ [] ^ _ ` { } ~]</p> <p>Sie können einen Wert zwischen 0 und 128 eingeben. Standardwert ist 1.</p>

Eigenschaft	Beschreibung
Anzahl der alphabetischen Zeichen	Die Mindestanzahl der erforderlichen alphabetischen Zeichen in einem Passwort. Sie können einen Wert zwischen 0 und 128 eingeben. Standardwert ist 1.
Anzahl der numerischen Zeichen	Die Mindestanzahl der erforderlichen numerischen Zeichen in einem Passwort. Sie können einen Wert zwischen 0 und 128 eingeben. Standardwert ist 1.
Minimale Passwortlänge	Die Mindestanzahl der erforderlichen Zeichen in einem Passwort. Sie können einen Wert zwischen 1 und 128 eingeben. Standardwert ist 8.
Anzahl der zu speichernden vorherigen Passwörter	Die Anzahl der aufeinanderfolgenden vorherigen Passwörter, die nicht wiederverwendet werden können. Sie können einen Wert zwischen 0 und 12 eingeben. Standardwert ist 0.
Passwortablauf in Tagen	Die Gültigkeitsdauer eines Passworts. Wenn Passwörter nicht ablaufen sollen, legen Sie den Wert 0 fest. Standardwert ist 0.
Domänenpasswort	Das Passwort für den Domänenadministrator. <ul style="list-style-type: none"> - Wenn Sie die Passwortkomplexität nicht aktivieren, muss das Passwort zwischen 2 und 16 Zeichen lang sein. - Wenn Sie die Passwortkomplexität aktivieren, muss das Passwort mindestens acht Zeichen umfassen und mindestens ein alphabetisches Zeichen, ein numerisches Zeichen und ein Sonderzeichen enthalten. - Wenn Sie eine Passwortrichtlinie konfigurieren, muss das Passwort die von Ihnen festgelegten Komplexitätsregeln erfüllen. Nicht verfügbar, wenn Sie die Informatica-Domäne zur Ausführung in einem Netzwerk mit Kerberos-Authentifizierung konfigurieren.
Passwort bestätigen	Geben Sie das Passwort zur Bestätigung erneut ein. Nicht verfügbar, wenn Sie die Informatica-Domäne zur Ausführung in einem Netzwerk mit Kerberos-Authentifizierung konfigurieren.

3. Legen Sie fest, ob die vom Installationsprogramm zugewiesenen Standardports für die Domänen- und Knotenkomponenten angezeigt werden sollen.

In der folgenden Tabelle wird die Seite „Erweiterte Port-Konfiguration“ beschrieben:

Eingabeaufforderung	Beschreibung
Seite für erweiterte Portkonfiguration anzeigen	Legen Sie fest, ob die vom Installationsprogramm zugewiesenen Portnummern für die Domänen- und Knotenkomponenten angezeigt werden sollen: 1 – Nein 2 – Ja Wenn Sie „Ja“ auswählen, zeigt das Installationsprogramm die den Domänenkomponenten zugewiesenen Standardportnummern an. Sie können die für die Domänen- und Knotenkomponenten zu verwendenden Portnummern festlegen. Außerdem können Sie einen Bereich von Portnummern für den auf dem Knoten ausgeführten Serviceprozess angeben. Sie können die Standardportnummern verwenden oder neue Portnummern festlegen. Stellen Sie sicher, dass die eingegebenen Portnummern nicht bereits von anderen Anwendungen verwendet werden.

4. Geben Sie auf der Seite „Portkonfiguration“ neue Portnummern ein, wenn Sie dazu aufgefordert werden, oder drücken Sie die Eingabetaste, um die Standardportnummern zu verwenden.

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

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

5. Wählen Sie aus, ob Sie die Dienste und die Verbindung konfigurieren möchten.

Wenn Sie „Ja“ auswählen, können Sie den Modellrepository-Dienst, den Datenintegrationsdienst, den Content-Management-Dienst, den PowerCenter-Repository-Dienst und den PowerCenter-Integrationsdienst sowie die Profiling-Warehouse-Verbindung und die Verbindungen, die mit der Clusterkonfiguration verbunden sind, konfigurieren.

Wenn Sie „Nein“ auswählen, können Sie die Anwendungsdienste über das Administrator Tool konfigurieren.

Wenn Sie sich für die Konfiguration der Dienste und Verbindungen entscheiden, wird der Abschnitt **Konfigurieren von Informatica-Anwendungsdiensten** angezeigt. Wenn Sie sich entscheiden, die Dienste und Verbindungen nicht zu konfigurieren, wird im Abschnitt **Installationsübersicht** angegeben, ob die Installation erfolgreich abgeschlossen wurde. Die Übersicht zeigt außerdem den Status der installierten Komponenten und ihre Konfiguration an.

Konfigurieren von Informatica-Anwendungsdiensten

1. Wählen Sie aus, ob Sie den Modellrepository-Dienst und den Datenintegrationsdienst konfigurieren möchten.
2. Wählen Sie aus, ob Sie den Überwachungsmodellrepository-Dienst konfigurieren möchten.

3. Wählen Sie aus, ob Sie den Content-Management-Dienst konfigurieren möchten.
4. Wählen Sie aus, ob Sie die Profiling-Warehouse-Verbindung konfigurieren möchten.
5. Geben Sie an, ob Sie einen Metadaten-Zugriffsdienst erstellen möchten. Wenn die Domäne die Kerberos-Authentifizierung verwendet, erstellen Sie den Metadaten-Zugriffsdienst nicht.
6. Wählen Sie aus, ob Sie einen PowerCenter-Repository-Dienst und einen PowerCenter-Integrationsdienst erstellen möchten.

Konfigurieren der Modellrepository-Datenbank

Nachdem Sie die Domäne und den Knoten konfiguriert haben, können Sie die Eigenschaften der Modellrepository-Datenbank konfigurieren.

1. Geben Sie den Modellrepository-Dienstnamen ein.

Geben Sie den Dienstnamen ein. 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:

` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ()] [

Nachdem Sie den Dienst erstellt haben, können Sie seinen Namen nicht mehr ändern.

Bei Auswahl des SPN auf Prozessebene geben Sie die Keytab-Datei des Modellrepository-Diensts an. Die Keytab-Datei für den Modellrepository-Dienstprozess. Die Keytab-Datei muss folgenden Namen aufweisen: .keytab

2. Wählen Sie die Datenbank aus, um das Modellrepository zu konfigurieren.

In der folgenden Tabelle sind die Datenbanken aufgeführt, die Sie für das Modellrepository konfigurieren können:

Eingabeaufforderung	Beschreibung
Datenbanktyp	Der Datenbanktyp für das Modellrepository. Wählen Sie eine der folgenden Optionen aus: 1 – Oracle 2 – Microsoft SQL Server 3 – IBM DB2 4 – PostgreSQL

3. 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 in der Modellrepository-Datenbank. Sie können den Namen des Windows NT-Benutzers für eine vertrauenswürdige Verbindung in Microsoft SQL Server eingeben.
Benutzerpasswort	Das Passwort für das Konto des Modellrepository-Benutzers. Sie können das Windows NT-Passwort für eine vertrauenswürdige Verbindung in Microsoft SQL Server eingeben.

4. Geben Sie an, ob eine gesicherte Modellrepository-Datenbank erstellt werden soll.

In einer mit dem SSL-Protokoll gesicherten Datenbank können Sie einen Modellrepository-Dienst erstellen. Um einen Modellrepository-Dienst in einer gesicherten Datenbank zu erstellen, drücken Sie **1** und gehen Sie zu dem Schritt für die Eingabe der JDBC-Informationen.

Um einen Modellrepository-Dienst in einer ungesicherten Datenbank zu erstellen, drücken Sie **2**.

5. Wenn Sie kein gesichertes Modellrepository erstellen, geben Sie die Parameter für die Datenbank ein.

- a. Geben Sie bei Auswahl von IBM DB2 an, ob ein Tablespace konfiguriert werden soll. Geben Sie dann den Namen des Tablespace ein.

In der folgenden Tabelle werden die Eigenschaften beschrieben, die Sie für die IBM DB2-Datenbank konfigurieren müssen:

Eigenschaft	Beschreibung
Tablespace konfigurieren	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“ auswählen. Wählen Sie aus, ob ein Tablespace festgelegt werden soll. 1 – Nein 2 – Ja
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. Geben Sie in einer Datenbank mit einer einzigen Partition den Namen des Tablespace ein, in dem die Tabellen erstellt werden sollen. Geben Sie in einer Datenbank mit mehreren Partitionen den Namen des nicht partitionierten Tablespace an, der sich in der Katalogpartition der Datenbank befindet.

- b. Geben Sie bei Auswahl von Microsoft SQL Server oder PostgreSQL den Schemanamen für die Datenbank ein.

In der folgenden Tabelle werden die Eigenschaften beschrieben, die Sie für die -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.
Datenbankdienstname	Dienst- oder Datenbankname: <ul style="list-style-type: none">- Oracle: Geben Sie den Dienstnamen ein.- Microsoft SQL Server: Geben Sie den Datenbanknamen ein.- IBM DB2: Geben Sie den Dienstnamen ein.- PostgreSQL: Geben Sie den Namen der Datenbank ein.
JDBC-Parameter konfigurieren	Geben Sie an, ob der Verbindungszeichenfolge weitere JDBC-Parameter hinzugefügt werden sollen: 1 – Ja 2 – Nein Geben Sie bei Auswahl von „Ja“ die Parameter ein oder drücken Sie die Eingabetaste, um die Standardparameter zu übernehmen. Bei Auswahl von „Nein“ wird die JDBC-Verbindungszeichenfolge ohne Parameter erstellt.

- Um die Verbindungsdaten mithilfe einer benutzerdefinierten JDBC-Verbindungszeichenfolge einzugeben, geben Sie die Verbindungszeichenfolge ein.
Verwenden Sie die folgende Syntax in der JDBC-Verbindungszeichenfolge:

IBM DB2

```
jdbc:Informatica:db2://<hostname>:<portnummer>;DatabaseName=
```

Oracle

```
jdbc:Informatica:oracle://<hostname>:<portnummer>;ServiceName=
```

Verwenden Sie die folgende Verbindungszeichenfolge, um eine Verbindung zur Oracle-Datenbank über den Oracle Connection Manager herzustellen:

```
jdbc:Informatica:oracle:TNSNamesFile=<vollqualifizierter Pfad zur Datei  
tnsnames.ora>;TNSServerName=<TNS-Name>;
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://  
<hostname>:<portnummer>;SelectMethod=cursor;DatabaseName=
```

Microsoft SQL Server mit Windows NT-Anmeldeinformationen

Wenn Sie die Windows NT-Anmeldeinformationen für die Modellrepository-Datenbank in Microsoft SQL Server angegeben haben, schließen Sie die Authentifizierungsmethode mithilfe der Syntax der Verbindungszeichenfolge als NTLM ein.

Microsoft SQL Server, der die Standardinstanz mit Windows NT-Anmeldeinformationen verwendet:

```
"jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database  
name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft SQL Server, der eine benannte Instanz mit Windows NT-Anmeldeinformationen verwendet:

```
"jdbc:informatica:sqlserver://<host name>\<named instance  
name>;DatabaseName=<database  
name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft Azure SQL-Datenbank

```
jdbc:Informatica:sqlserver://  
<hostname>:<portnummer>;SelectMethod=cursor;DatabaseName=<datenbankname>;Snap  
shotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.win  
dows.net;ValidateServerCertificate=false
```

Azure SQL-Datenbank mit Active Directory-Authentifizierung

```
"jdbc:informatica: sqlserver://  
<host_name>:<port_number>;database=<database_name>;encrypt=true;Authentication  
Method=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertific  
ate=*.database.windows.net;loginTimeout=<seconds>"
```

PostgreSQL

```
jdbc:Informatica:postgresql://<hostname>:<portnummer>;DatabaseName=
```

Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLsv1.2;
```

Stellen Sie sicher, dass die Verbindungszeichenfolge alle vom Datenbanksystem benötigten Verbindungsparameter enthält.

Der Abschnitt **Serviceparameter** wird angezeigt.

Datenintegrationsdienst

Nachdem Sie die Modellrepository-Datenbank konfiguriert haben, können Sie die Dienstparameter für die Anwendungsdienste konfigurieren.

1. Geben Sie die folgenden Informationen für Dienstparameter ein:

Port	Beschreibung
Name des Datenintegrationsdiensts	Der Name des Datenintegrationsdiensts, der in der Informatica-Domäne erstellt werden soll.
HTTP-Protokolltyp	Typ der Verbindung zum Datenintegrationsdienst. Wählen Sie eine der folgenden Optionen aus: <ul style="list-style-type: none">- HTTP. Erfordert, dass der Dienst eine HTTP-Verbindung benutzt.- HTTPS. Erfordert, dass der Dienst eine sichere HTTP-Verbindung benutzt.- HTTP&HTTPS. In Anfragen an den Dienst kann entweder eine HTTP- oder eine HTTPS-Verbindung verwendet werden.
HTTP-Port	Für den Datenintegrationsdienst zu verwendende Portnummer. Der Standardwert ist 9085.
HTTPS-Port	Für den Datenintegrationsdienst zu verwendende Portnummer. Der Standardwert ist 9085.

2. Wählen Sie die SSL-Zertifikate aus, die für den Schutz des Datenintegrationsdiensts verwendet werden sollen.

Option	Beschreibung
SSL-Standardzertifikatsdateien von Informatica verwenden	<p>Zur Verwendung der im Standardschlüsselspeicher und im Truststore enthaltenen SSL-Standardzertifikate von Informatica.</p> <p>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.</p>
Benutzerdefinierte SSL-Zertifikate verwenden	<p>Zur Verwendung von benutzerdefinierten SSL-Zertifikaten. Sie müssen den Speicherort der Schlüsselspeicher- und Truststore-Dateien angeben.</p> <p>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.</p>

Wenn Sie benutzerdefinierte SSL-Zertifikate verwenden möchten, geben Sie die folgenden Informationen ein.

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.

Konfigurieren der Überwachungsmodellrepository-Datenbank

Nachdem Sie die Modellrepository-Datenbank konfiguriert haben, können Sie die Eigenschaften der Überwachungsmodellrepository-Datenbank konfigurieren.

1. Geben Sie den Überwachungsmodellrepository-Dienstnamen ein.

Geben Sie den Dienstnamen ein. 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:

` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! () [

Nachdem Sie den Dienst erstellt haben, können Sie seinen Namen nicht mehr ändern.

Bei Auswahl des SPN auf Prozessebene geben Sie die Keytab-Datei des Überwachungsmodellrepository-Diensts an. Die Keytab-Datei für den Überwachungs-Modellrepository-Dienstprozess. Die Keytab-Datei muss folgenden Namen aufweisen: .keytab

2. Wählen Sie den Datenbanktyp für das Überwachungsmodellrepository aus.

In der folgenden Tabelle sind die Datenbanken für das Überwachungsmodellrepository aufgeführt.

Eingabeaufforderung	Beschreibung
Datenbanktyp	Typ der Datenbank für das Überwachungsmodellrepository. Wählen Sie eine der folgenden Optionen aus: 1 – Oracle 2 – Microsoft SQL Server 3 – IBM DB2 4 – PostgreSQL

3. 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 in der Überwachungsmodellrepository-Datenbank. Sie können den Namen des Windows NT-Benutzers für eine vertrauenswürdige Verbindung in Microsoft SQL Server eingeben.
Benutzerpasswort	Das Passwort für das Konto des Benutzers des Überwachungsmodellrepositorys. Sie können das Windows NT-Passwort für eine vertrauenswürdige Verbindung in Microsoft SQL Server eingeben.

4. Geben Sie an, ob eine gesicherte Überwachungsmodellrepository-Datenbank erstellt werden soll.

Sie können ein Überwachungsmodellrepository in einer mit dem SSL-Protokoll gesicherten Datenbank erstellen. Um einen Überwachungsmodellrepository in einer gesicherten Datenbank zu erstellen, drücken Sie 1 und gehen Sie zu dem Schritt für die Eingabe der JDBC-Informationen.

Um ein Überwachungsmodellrepository in einer ungesicherten Datenbank zu erstellen, drücken Sie 2.

5. Wenn Sie kein gesichertes Überwachungsmodellrepository erstellen, geben Sie die Parameter für die Datenbank ein.
- a. Geben Sie bei Auswahl von IBM DB2 an, ob ein Tablespace konfiguriert werden soll. Geben Sie dann den Namen des Tablespace ein.

In der folgenden Tabelle werden die Eigenschaften beschrieben, die Sie für die IBM DB2-Datenbank konfigurieren müssen:

Eigenschaft	Beschreibung
Tablespace konfigurieren	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“ auswählen. Wählen Sie aus, ob ein Tablespace festgelegt werden soll. 1 – Nein 2 – Ja
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. Geben Sie in einer Datenbank mit einer einzigen Partition den Namen des Tablespace ein, in dem die Tabellen erstellt werden sollen. Geben Sie in einer Datenbank mit mehreren Partitionen den Namen des nicht partitionierten Tablespace an, der sich in der Katalogpartition der Datenbank befindet.

- b. Geben Sie bei Auswahl von Microsoft SQL Server oder PostgreSQL den Schemanamen für die Datenbank ein.

In der folgenden Tabelle werden die Eigenschaften beschrieben, die Sie für die -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.
Datenbankdienstname	Dienst- oder Datenbankname: <ul style="list-style-type: none">- Oracle: Geben Sie den Dienstnamen ein.- Microsoft SQL Server: Geben Sie den Datenbanknamen ein.- IBM DB2: Geben Sie den Dienstnamen ein.- PostgreSQL: Geben Sie den Namen der Datenbank ein.
JDBC-Parameter konfigurieren	Geben Sie an, ob der Verbindungszeichenfolge weitere JDBC-Parameter hinzugefügt werden sollen: 1 – Ja 2 – Nein Geben Sie bei Auswahl von „Ja“ die Parameter ein oder drücken Sie die Eingabetaste, um die Standardparameter zu übernehmen. Bei Auswahl von „Nein“ wird die JDBC-Verbindungszeichenfolge ohne Parameter erstellt.

- Um die Verbindungsdaten mithilfe einer benutzerdefinierten JDBC-Verbindungszeichenfolge einzugeben, geben Sie die Verbindungszeichenfolge ein.
Verwenden Sie die folgende Syntax in der JDBC-Verbindungszeichenfolge:

IBM DB2

```
jdbc:Informatica:db2://<hostname>:<portnummer>;DatabaseName=
```

Oracle

```
jdbc:Informatica:oracle://<hostname>:<portnummer>;ServiceName=
```

Verwenden Sie die folgende Verbindungszeichenfolge, um eine Verbindung zur Oracle-Datenbank über den Oracle Connection Manager herzustellen:

```
jdbc:Informatica:oracle:TNSNamesFile=<vollqualifizierter Pfad zur Datei  
tnsnames.ora>;TNSServerName=<TNS-Name>;
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://  
<hostname>:<portnummer>;SelectMethod=cursor;DatabaseName=
```

Microsoft SQL Server mit Windows NT-Anmeldeinformationen

Wenn Sie die Windows NT-Anmeldeinformationen für die Modellrepository-Datenbank in Microsoft SQL Server angegeben haben, schließen Sie die Authentifizierungsmethode mithilfe der Syntax der Verbindungszeichenfolge als NTLM ein.

Microsoft SQL Server, der die Standardinstanz mit Windows NT-Anmeldeinformationen verwendet:

```
"jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database  
name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft SQL Server, der eine benannte Instanz mit Windows NT-Anmeldeinformationen verwendet:

```
"jdbc:informatica:sqlserver://<host name>\<named instance  
name>;DatabaseName=<database  
name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft Azure SQL-Datenbank

```
jdbc:Informatica:sqlserver://  
<hostname>:<portnummer>;SelectMethod=cursor;DatabaseName=<datenbankname>;Snap  
shotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.win  
dows.net;ValidateServerCertificate=false
```

Azure SQL-Datenbank mit Active Directory-Authentifizierung

```
"jdbc:informatica: sqlserver://  
<host_name>:<port_number>;database=<database_name>;encrypt=true;Authentication  
Method=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertific  
ate=*.database.windows.net;loginTimeout=<seconds>"
```

PostgreSQL

```
jdbc:Informatica:postgresql://<hostname>:<portnummer>;DatabaseName=
```

Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLSv1.2;
```

Stellen Sie sicher, dass die Verbindungszeichenfolge alle vom Datenbanksystem benötigten Verbindungsparameter enthält.

Der Abschnitt **Serviceparameter** wird angezeigt.

Parameter und Datenbank des Content-Management-Diensts

Nach der Konfiguration des Datenintegrationsdiensts können Sie die Parameter für den Content-Management-Dienst konfigurieren.

1. Geben Sie die folgenden Informationen für Dienstparameter ein:

Parameter	Beschreibung
Name des Content-Management-Diensts	Name des Content-Management-Diensts, der in der Informatica-Domäne erstellt werden soll.
HTTP-Protokolltyp	Typ der Verbindung des Content-Management-Diensts. Wählen Sie eine der folgenden Optionen aus: <ul style="list-style-type: none">- HTTP. Für Anfragen an den Dienst wird eine HTTP-Verbindung verwendet.- HTTPS. Für Anfragen an den Dienst wird eine sichere HTTP-Verbindung verwendet.
HTTP-Port	Portnummer für den Content-Management-Dienst. Standardwert ist 8105.

2. Wenn Sie einen Schlüsselspeicher für den Content-Management-Dienst auswählen, geben Sie die Schlüsselspeicherdatei und die Portnummer für die HTTPS-Verbindung zum Content-Management-Dienst ein.

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.

- Verwenden Sie den vom Installationsprogramm generierten Schlüsselspeicher.
- Geben Sie den Speicherort und das Passwort einer benutzerdefinierten Schlüsselspeicherdatei an.

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/

Die Schlüsselspeicherzertifikatstypen für den Content-Management-Dienst richten sich nach den Zertifikatstypen, die vom Administrator Tool verwendet werden:

- Bei Verwendung des standardmäßigen Schlüsselspeicherzertifikats für das Administrator Tool können Sie entweder das standardmäßige oder ein benutzerdefiniertes Schlüsselspeicherzertifikat für den Content-Management-Dienst verwenden.
- Bei Verwendung eines benutzerdefinierten Schlüsselspeicherzertifikats für das Administrator Tool müssen Sie ein benutzerdefiniertes Schlüsselspeicherzertifikat für den Content-Management-Dienst verwenden.

3. Wählen Sie den Datenbanktyp für das Referenzdaten-Warehouse aus.

In der folgenden Tabelle sind die Datenbanken für das Referenzdaten-Warehouse aufgeführt:

Eingabeaufforderung	Beschreibung
Datenbanktyp	Typ der Datenbank für das Referenzdaten-Warehouse. Wählen Sie eine der folgenden Optionen aus: <ul style="list-style-type: none"> - IBM DB2 - Microsoft Azure SQL-Datenbank - Microsoft SQL Server - Oracle - PostgreSQL mit JDBC

4. 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	Name für das Benutzerkonto des Referenzdaten-Warehouse.
Passwort des Datenbankbenutzers	Passwort für das Benutzerkonto des Referenzdaten-Warehouse.

Geben Sie bei Auswahl von IBM DB2 den Tablespace für die Repository-Tabellen an:

Eigenschaft	Beschreibung
Tablespace	Der Name des Tablespace, in dem die Tabellen erstellt werden sollen. Geben Sie einen Tablespace an, der die Anforderungen an die Seitengröße (pageSize) von 32768 Byte erfüllt. Wenn Sie in einer Datenbank mit einer einzigen Partition diese Option nicht auswählen, erstellt das Installationsprogramm die Tabellen im Standard-Tablespace. Wählen Sie diese Option in einer Datenbank mit mehreren Partitionen aus und geben Sie den Namen des nicht partitionierten Tablespace an, der sich in der Katalogpartition der Datenbank befindet.

5. Drücken Sie **1**, um den Schemanamen anzugeben. Wenn Sie keinen Schemanamen angeben möchten, drücken Sie **2**. Standardwert ist 2. Geben Sie bei Auswahl von Microsoft SQL Server das Schema für die Repository-Tabellen und die Datenbankverbindung an. Wenn Sie keinen Schemanamen angeben, erstellt das Installationsprogramm die Tabellen im Standardschema.
6. Um die JDBC-Verbindungsinformationen mithilfe der JDBC-URL-Informationen einzugeben, drücken Sie **1**. Um die JDBC-Verbindungsinformationen mithilfe einer benutzerdefinierten JDBC-Verbindungszeichenfolge einzugeben, drücken Sie **2**.
- a. 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
Hostname der Datenbank	Hostname für die Datenbank
Portnummer der Datenbank	Die Portnummer für die Datenbank.
Datenbankdienstname	Dienst- oder Datenbankname: <ul style="list-style-type: none">- Oracle: Geben Sie den Dienstnamen ein.- Microsoft SQL Server: Geben Sie den Datenbanknamen ein.- IBM DB2: Geben Sie den Dienstnamen ein.
Konfigurieren von JDBC-Parametern	Geben Sie an, ob der Verbindungszeichenfolge weitere JDBC-Parameter hinzugefügt werden sollen: 1 – Ja 2 – Nein Geben Sie bei Auswahl von „Ja“ die Parameter ein oder drücken Sie die Eingabetaste, um die Standardparameter zu übernehmen. Bei Auswahl von „Nein“ wird die JDBC-Verbindungszeichenfolge ohne Parameter erstellt.

- Um die Verbindungsdaten mithilfe einer benutzerdefinierten JDBC-Verbindungszeichenfolge einzugeben, geben Sie die Verbindungszeichenfolge ein.
Verwenden Sie die folgende Syntax in der JDBC-Verbindungszeichenfolge:

IBM DB2

```
jdbc:Informatica:db2://<hostname>:<portnummer>;DatabaseName=
```

Oracle

```
jdbc:Informatica:oracle://<hostname>:<portnummer>;ServiceName=
```

Verwenden Sie die folgende Verbindungszeichenfolge, um eine Verbindung zur Oracle-Datenbank über den Oracle Connection Manager herzustellen:

```
jdbc:Informatica:oracle:TNSNamesFile=<vollqualifizierter Pfad zur Datei  
tnsnames.ora>;TNSServerName=<TNS-Name>;
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://  
<hostname>:<portnummer>;SelectMethod=cursor;DatabaseName=
```

Microsoft Azure SQL

```
jdbc:Informatica:sqlserver://  
<hostname>:<portnummer>;SelectMethod=cursor;DatabaseName=<datenbankname>;Snap  
shotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.win  
dows.net;ValidateServerCertificate=false
```

PostgreSQL

```
jdbc:Informatica:postgresql://<hostname>:<portnummer>;DatabaseName=
```

Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database  
name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersio  
n=TLSv1.2;
```

Stellen Sie sicher, dass die Verbindungszeichenfolge alle vom Datenbanksystem benötigten Verbindungsparameter enthält.

7. Geben Sie die Verbindungszeichenfolge für den Datenzugriff ein.

Profiling Warehouse Database

After you configure the Content Management Service, you can configure the data profiling warehouse database.

1. Select the database type for the data profiling warehouse.

The following table lists the databases for the data profiling warehouse.

Prompt	Description
Database type	Type of database for the data profiling warehouse. Select from the following options: <ul style="list-style-type: none">- IBM DB2- Microsoft SQL Server- Oracle- PostgreSQL

2. Enter the properties for the database user account.

The following table lists the properties for the database user account:

Property	Description
Database user ID	Name for the data profiling warehouse user account.
Database user password	Password for the data profiling warehouse user account.

Geben Sie bei Auswahl von IBM DB2 den Tablespace für die Repository-Tabellen an:

Eigenschaft	Beschreibung
Tablespace	<p>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.</p> <p>Wenn Sie in einer Datenbank mit einer einzigen Partition diese Option nicht auswählen, erstellt das Installationsprogramm die Tabellen im Standard-Tablespace.</p> <p>Wählen Sie diese Option in einer Datenbank mit mehreren Partitionen aus und geben Sie den Namen des nicht partitionierten Tablespace an, der sich in der Katalogpartition der Datenbank befindet.</p>

3. To specify the schema name, press **1**. If you do not want to specify a schema name, press **2**. Default is **2**. If you select Microsoft SQL Server, specify the schema for the repository tables and database connection. If you do not specify a schema name, the installer creates the tables in the default schema.
4. To enter the JDBC connection information using the JDBC URL information, press **1**. To enter the JDBC connection information using a custom JDBC connection string, press **2**.

Geben Sie bei Auswahl von IBM DB2 den Tablespace für die Repository-Tabellen an:

Eigenschaft	Beschreibung
Tablespace	<p>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.</p> <p>Wenn Sie in einer Datenbank mit einer einzigen Partition diese Option nicht auswählen, erstellt das Installationsprogramm die Tabellen im Standard-Tablespace.</p> <p>Wählen Sie diese Option in einer Datenbank mit mehreren Partitionen aus und geben Sie den Namen des nicht partitionierten Tablespace an, der sich in der Katalogpartition der Datenbank befindet.</p>

- a. 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
Hostname der Datenbank	Hostname für die Datenbank
Portnummer der Datenbank	Die Portnummer für die Datenbank.
Datenbankdienstname	Dienst- oder Datenbankname: <ul style="list-style-type: none">- Oracle: Geben Sie den Dienstnamen ein.- Microsoft SQL Server: Geben Sie den Datenbanknamen ein.- IBM DB2: Geben Sie den Dienstnamen ein.
Konfigurieren von JDBC-Parametern	Geben Sie an, ob der Verbindungszeichenfolge weitere JDBC-Parameter hinzugefügt werden sollen: 1 – Ja 2 – Nein Geben Sie bei Auswahl von „Ja“ die Parameter ein oder drücken Sie die Eingabetaste, um die Standardparameter zu übernehmen. Bei Auswahl von „Nein“ wird die JDBC-Verbindungszeichenfolge ohne Parameter erstellt.

- Um die Verbindungsdaten mithilfe einer benutzerdefinierten JDBC-Verbindungszeichenfolge einzugeben, geben Sie die Verbindungszeichenfolge ein.
Verwenden Sie die folgende Syntax in der JDBC-Verbindungszeichenfolge:

IBM DB2

```
jdbc:Informatica:db2://<hostname>:<portnummer>;DatabaseName=
```

Oracle

```
jdbc:Informatica:oracle://<hostname>:<portnummer>;ServiceName=
```

Verwenden Sie die folgende Verbindungszeichenfolge, um eine Verbindung zur Oracle-Datenbank über den Oracle Connection Manager herzustellen:

```
jdbc:Informatica:oracle:TNSNamesFile=<vollqualifizierter Pfad zur Datei  
tnsnames.ora>;TNSServerName=<TNS-Name>;
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://  
<hostname>:<portnummer>;SelectMethod=cursor;DatabaseName=
```

Microsoft Azure SQL

```
jdbc:Informatica:sqlserver://  
<hostname>:<portnummer>;SelectMethod=cursor;DatabaseName=<datenbankname>;Snap  
shotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.win  
dows.net;ValidateServerCertificate=false
```

PostgreSQL

```
jdbc:Informatica:postgresql://<hostname>:<portnummer>;DatabaseName=
```

Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database  
name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersio  
n=TLSv1.2;
```

Stellen Sie sicher, dass die Verbindungszeichenfolge alle vom Datenbanksystem benötigten Verbindungsparameter enthält.

5. Enter the data access connection string.

PowerCenter-Repository-Dienst und PowerCenter-Integrationsdienst

Sie können den PowerCenter-Repository-Dienst und den PowerCenter-Integrationsdienst konfigurieren.

1. Wählen Sie die Datenbank aus, die für das PowerCenter-Repository konfiguriert werden soll.
Sie können das PowerCenter-Repository mit einer der folgenden Datenbanken konfigurieren:
 - 1 – Oracle
 - 2 – Microsoft SQL Server
 - 3 – PostgreSQL
2. 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 für das Konto des Benutzers der PowerCenter-Repository-Datenbank.
Benutzerpasswort	Das Passwort des Benutzerkontos für die PowerCenter-Konfigurationsdatenbank.
Datenbankdienstname	Dienst- oder Datenbankname für PowerCenter: <ul style="list-style-type: none">- Oracle: Geben Sie den Dienstnamen ein.- Microsoft SQL Server: Geben Sie den Datenbanknamen ein.- PostgreSQL: Geben Sie den Namen der Datenbank ein.
Hostname der Datenbank	Geben Sie den Hostnamen für die PowerCenter Datenbank ein .

3. Geben Sie den Namen des zu erstellenden PowerCenter-Repository-Diensts ein.
4. Geben Sie den Namen des zu erstellenden PowerCenter-Integrationsdiensts ein.
5. Wählen Sie die Codepage des PowerCenter-Repository-Diensts aus. Der Standardwert ist 7-Bit-ASCII.
6. Wählen Sie die Codepage des PowerCenter-Integrationsdiensts aus. Der Standardwert ist 7-Bit-ASCII.

In der **Installationsübersicht** wird angezeigt, ob die Installation erfolgreich abgeschlossen wurde. Die Übersicht zeigt außerdem den Status der installierten Komponenten und ihre Konfiguration an.

Anfügen einer Domäne

Sie können eine Domäne anfügen, wenn Sie eine Installation auf mehreren Computern vornehmen und bereits eine Domäne auf einem anderen Computer erstellt haben.

Ausführen des Installationsprogramms

Führen Sie die folgenden Schritte aus, um das Installationsprogramm auszuführen:

1. Melden Sie sich mit einem Systembenutzerkonto am Computer an.
2. Verwenden Sie den folgenden Befehl, um die DISPLAY-Variable auf dem Computer zu löschen: `unset DISPLAY`
3. Schließen Sie alle anderen Anwendungen.
4. Führen Sie über eine Shell-Befehlszeile die Datei `install.sh` aus.
Der Installer zeigt die Nachricht an, um sicherzustellen, dass die Gebietsschema-Umgebungsvariablen gesetzt sind.
5. Wurden die Umgebungsvariablen nicht eingestellt, drücken Sie **n**, um den Installer zu beenden. Stellen Sie sie anschließend entsprechend den Anforderungen ein.
Wenn die Umgebungsvariablen eingestellt sind, drücken Sie **y**, um fortzufahren.

Willkommen – Akzeptieren der allgemeinen Geschäftsbedingungen

- Lesen Sie die Bedingungen für die Informatica-Installation und das Toolkit zur Produktverwendung und wählen Sie **Ich stimme den Bedingungen zu** aus.

Informatica DiscoveryIQ ist ein Produktnutzungstool, das Routineberichte über Datennutzung und Systemstatistiken an Informatica sendet. Nach der Installation und Konfiguration der Informatica-Domäne lädt Informatica DiscoveryIQ alle 15 Minuten Daten an Informatica hoch. Danach sendet die Domäne die Daten alle 30 Tage. Sie können die Verwendung von Statistiken im Administrator Tool deaktivieren.

- a. Drücken Sie **1**, wenn Sie die allgemeinen Geschäftsbedingungen nicht akzeptieren möchten
- b. Drücken Sie **2**, um die allgemeinen Geschäftsbedingungen zu akzeptieren.

Wenn Sie die allgemeinen Geschäftsbedingungen nicht akzeptieren, werden Sie vom Installationsprogramm hierzu aufgefordert.

Der Abschnitt **Komponentenauswahl** wird angezeigt.

Komponentenauswahl

Nachdem Sie die allgemeinen Geschäftsbedingungen akzeptiert haben, können Sie Informatica-Domänendienste installieren.

1. Drücken Sie **1**, um die Informatica-Domänendienste zu installieren.
Diese Option installiert Domänendienste der Version 10.5.9 und die Binärdateien des Anwendungsdiensts.
2. Wählen Sie aus, ob das Installationsprogramm in einem Netzwerk mit Kerberos-Authentifizierung ausgeführt werden soll.
 - a. Drücken Sie **1**, um die Informatica-Domäne zur Ausführung in einem Netzwerk ohne Kerberos-Authentifizierung zu konfigurieren.
 - b. Drücken Sie **2**, um die Informatica-Domäne zur Ausführung in einem Netzwerk mit Kerberos-Authentifizierung zu konfigurieren.
3. Wählen Sie aus, ob Sie Verteilungspakete über das Informatica-Installationsprogramm installieren möchten.
 - Drücken Sie **1**, wenn Sie keine Verteilungspakete benötigen oder diese später installieren möchten.
 - Drücken Sie **2**, wenn Sie Verteilungspakete über das Installationsprogramm installieren möchten.Standardwert ist 1.
4. Wenn Sie Verteilungspakete installieren möchten, wählen Sie ein oder mehrere Pakete aus der Liste aus, die Sie installieren möchten. Trennen Sie mehrere Pakete durch ein Komma.
Standardwert ist 1.

Im Abschnitt **Installationsvoraussetzungen** werden die Installationsanforderungen angezeigt. Stellen Sie sicher, dass alle Voraussetzungen erfüllt sind, bevor Sie die Installation fortsetzen.

Voraussetzungen für die Installation

Überprüfen Sie den für die Installation erforderlichen Festplattenspeicherplatz und Arbeitsspeicher und schließen Sie die Vorabaufgaben für die Installation ab.

1. Überprüfen Sie, ob genügend Festplattenspeicher und Arbeitsspeicher (RAM) zur Installation verfügbar sind.

2. Überprüfen Sie die Datenbankanforderungen für das Domänenkonfigurations-Repository.
3. Schließen Sie die Vorabaufgaben für die Installation ab, einschließlich des Abrufs Ihres Informatica-Lizenzschlüssels, der Festlegung von Umgebungsvariablen und der Überprüfung der Portverfügbarkeit.

Der Abschnitt **Lizenz- und Installationsverzeichnis** wird angezeigt.

Lizenz und Installationsverzeichnis

Nachdem Sie die Installationsvoraussetzungen überprüft haben, können Sie das Installationsverzeichnis angeben.

1. Geben Sie den absoluten Pfad für das Installationsverzeichnis an.

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

Der Standardwert ist das Home-Verzeichnis des Benutzers, der die Informatica-Installation durchführt.

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

2. Geben Sie den Pfad und Dateinamen des Informatica-Lizenzschlüssels ein und drücken Sie die **Eingabetaste**.
3. Geben Sie den Umgebungstyp an, der der Installation der Informatica-Dienste zugeordnet ist.
 - Drücken Sie **1**, um die Sandbox-Umgebung für eine Basisumgebung festzulegen, die für Machbarkeitsstudien mit minimaler Benutzerzahl verwendet wird.
 - Drücken Sie **2**, um die Entwicklungsumgebung für die Designumgebung festzulegen.
 - Drücken Sie **3**, um die Testumgebung für die Verarbeitung großer Datenmengen ähnlich der in einer Produktionsumgebung festzulegen.
 - Drücken Sie **4**, um die Produktionsumgebung für die massiv parallele Verarbeitung großer Datenmengen für Endbenutzer festzulegen. Bei erweiterten Produktionsumgebungen handelt es sich in der Regel um Setups mit mehreren Knoten.

Der Standardwert ist „1“ für Sandbox.

Wenn Sie die Kerberos-Netzwerkauthentifizierung aktiviert haben, wird der Abschnitt **Dienstprinzipalebene** angezeigt.

Wenn Kerberos-Netzwerkauthentifizierung nicht aktiviert wurde, wird der Abschnitt **Vorinstallationsübersicht** angezeigt. Überprüfen Sie die Installationsinformationen und drücken Sie die **Eingabetaste**, um fortzufahren. Fahren Sie mit ["Domänenauswahl" auf Seite 162](#) fort.

Dienstprinzipalebene

Nachdem Sie das Installationsverzeichnis angegeben haben, können Sie die Sicherheitsstufe konfigurieren.

- Wählen Sie die Ebene aus, auf die die Kerberos-Dienstprinzipale für die Domäne festgelegt werden.

Hinweis: Alle Knoten in der Domäne müssen die gleiche Dienstprinzipalebene verwenden. Wenn Sie einen Knoten zu einer Domäne hinzufügen, wählen Sie die gleiche Dienstprinzipalebene aus, die vom Gateway-Knoten in der Domäne verwendet wird.

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

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

Der Abschnitt **Vorinstallationsübersicht** wird angezeigt. Drücken Sie zur Fortsetzung die **Eingabetaste**.

Domänenauswahl

Nachdem Sie sich die Vorinstallationsübersicht durchgesehen haben, können Sie die Domäneninformationen eingeben.

- Drücken Sie **2**, um eine Domäne anzufügen.
Das Installationsprogramm fügt einen Knoten auf dem Computer an, auf dem die Installation erfolgt.
- Geben Sie an, ob für die anzufügende Domäne die Option zur sicheren Kommunikation aktiviert wurde.
Drücken Sie **1**, um eine ungesicherte Domäne anzufügen, oder **2**, um eine sichere Domäne anzufügen.
- Wählen Sie den Knotentyp aus, den Sie erstellen möchten.
Drücken 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.
- Wenn Sie eine HTTPS-Verbindung für den Informatica Administrator aktivieren, geben Sie die zum Sichern der Verbindung zu verwendende HTTPS-Portnummer ein.
- Legen Sie fest, ob Sie zum Aktivieren der SAML-Authentifizierung in der Domäne SSL-Standardzertifikate von Informatica oder eigene SSL-Zertifikate verwenden möchten.

In der folgenden Tabelle werden die SSL-Zertifikatsoptionen für die SAML-Authentifizierung beschrieben:

Option	Beschreibung
Standardmäßige SSL-Zertifikatsdatei von Informatica verwenden.	Wählen Sie diese Option aus, um für die SAML-Authentifizierung die Truststore-Standarddatei von Informatica zu verwenden.
Speicherort der SSL-Zertifikatsdatei eingeben.	Wählen Sie diese Option, um eine benutzerdefinierte Informatica-Truststore-Datei für die SAML-Authentifizierung zu verwenden. Geben Sie das Verzeichnis an, das die benutzerdefinierte Truststore-Datei auf Gateway-Knoten in der Domäne enthält. Geben Sie nur das Verzeichnis an, nicht den vollständigen Dateipfad.

6. Wählen Sie aus, ob die SAML-Authentifizierung (Security Assertion Markup Language) aktiviert werden soll, um für webbasierte Informatica-Anwendungen in einer Informatica-Domäne die SAML-basierte Unterstützung von Single Sign-On (SSO) zu konfigurieren.

Wählen Sie aus, ob die Domäne SAML-Authentifizierung verwendet:

- a. Drücken Sie 1 für „Nein“, um die SAML-Authentifizierung zu deaktivieren.

Wenn Sie „Nein“ wählen, fahren Sie fort mit [“ Domänensicherheit – Sichere Kommunikation” auf Seite 163](#).

- b. Drücken Sie 2 für „Ja“, um die SAML-Authentifizierung zu aktivieren.

Wenn Sie „Ja“ auswählen, konfigurieren Sie die SAML-Authentifizierung.

Der Abschnitt **Domänensicherheit – Sichere Kommunikation** wird angezeigt.

Domänensicherheit – Sichere Kommunikation

Nachdem Sie die Domäne ausgewählt haben, können Sie die Domänensicherheit konfigurieren.

- Geben Sie an, ob die standardmäßigen SSL-Zertifikate von Informatica oder eigene SSL-Zertifikate für die sichere Domänenkommunikation verwendet werden sollen.
 - a. Wählen Sie den Typ der zu verwendenden SSL-Zertifikate aus.

In der folgenden Tabelle werden die Optionen für die SSL-Zertifikate beschrieben, die Sie zum Sichern der Informatica-Domäne verwenden können:

Option	Beschreibung
SSL-Standardzertifikatsdateien von Informatica verwenden	Verwenden Sie die im Standardschlüsselspeicher und im Truststore enthaltenen 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.
Benutzerdefinierte SSL-Zertifikate verwenden	Geben Sie den Pfad für die Schlüsselspeicherdateien und Truststore-Dateien ein, die die SSL-Zertifikate enthalten. Sie müssen außerdem die Passwörter für Schlüsselspeicher und Truststore 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 eine Datei namens <code>infa_keystore.jks</code> enthalten.
Schlüsselspeicherpasswort	Passwort für den Schlüsselspeicher „ <code>infa_keystore.jks</code> “.
Verzeichnis der Truststore-Datei	Verzeichnis, das die Truststore-Dateien enthält. Das Verzeichnis muss Dateien mit der Bezeichnung „ <code>infa_truststore.jks</code> “ und „ <code>infa_truststore.pem</code> “ enthalten.
Truststore-Passwort	Passwort für die Datei <code>infa_truststore.jks</code> .

Der Abschnitt **Domänenkonfiguration** wird angezeigt.

Domänenkonfiguration

Nachdem Sie die Domänensicherheit konfiguriert haben, können Sie die Verbindungsdetails für das Domänen-Repository konfigurieren.

- Geben Sie die Informationen für die Domäne ein, die Sie anfügen möchten.

In der folgenden Tabelle werden die Eigenschaften beschrieben, die Sie für die Domäne festlegen:

Eigenschaft	Beschreibung
Domänenname	Der Name der zu verknüpfenden Domäne.
Host des Gateway-Knotens	Der Hostname des Computers, der den Gateway-Knoten für die Domäne hostet.
Port des Gateway-Knotens	Die Portnummer des Gateway-Knotens.
Domänenbenutzername	Der Benutzername des Administrators der Domäne, zu der Sie eine Verknüpfung herstellen möchten.
Domänenpasswort	Das Passwort für den Domänenadministrator.
Sicherheitsdomänenname	Name der gesicherten Domäne.

Der Abschnitt **Domänensicherheit – Verschlüsselungsschlüssel** wird angezeigt.

Domänensicherheit – Verschlüsselungsschlüssel

Nachdem Sie das Domänen-Repository konfiguriert haben, können Sie den Verschlüsselungsschlüssel konfigurieren.

- Geben Sie das Verzeichnis für den Verschlüsselungsschlüssel für die Informatica-Domäne ein.

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

Eingabeaufforderung	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.

Das Installationsprogramm legt verschiedene Berechtigungen für das Verzeichnis und die Dateien im Verzeichnis fest. Weitere Informationen über die Berechtigungen für die Verschlüsselungsschlüsseldatei und das Verzeichnis finden Sie unter ["Sichere Dateien und Verzeichnisse" auf Seite 110](#).

Der Abschnitt **Knotenkonfiguration der hinzuzufügenden Domäne** wird angezeigt.

Knotenkonfiguration der hinzuzufügenden Domäne

Nachdem Sie den Verschlüsselungsschlüssel konfiguriert haben, können Sie die Domäne und den Knoten konfigurieren, die angefügt werden.

1. Geben Sie die Informationen für die Domäne und den Knoten ein, die Sie anfügen möchten.

In der folgenden Tabelle werden die Eigenschaften beschrieben, die Sie für den aktuellen Knoten festlegen:

Eigenschaft	Beschreibung
Hostname des Knotens	Hostname oder IP-Adresse des Computers, auf dem der Knoten angefügt werden soll. Wenn der Computer nur einen Netzwerknamen aufweist, verwenden Sie den Standardhostname. Wenn der Computer mehrere Netzwerknamen aufweist, können Sie den Standardhostnamen ändern und einen alternativen Netzwerknamen verwenden. Hinweis: Der Hostname des Knotens darf keine Unterstriche (_) enthalten. Verwenden Sie nicht localhost. Der Hostname muss den Computer eindeutig kennzeichnen.
Knotenname	Der Name des Knotens, den Sie anfügen möchten.
Portnummer des Knotens	Die Portnummer für den Knoten. Die Standardportnummer für den Knoten lautet 6005. Wenn die Portnummer auf dem Rechner nicht verfügbar ist, zeigt das Installationsprogramm die nächste verfügbare Portnummer an.

2. Legen Sie fest, ob die vom Installationsprogramm zugewiesenen erweiterten Portkonfigurationen für die Domänen- und Knotenkomponenten angezeigt werden sollen.

Wenn Sie **1** auswählen, zeigt das Installationsprogramm die Port-Konfigurationen nicht an. Wenn Sie **2** auswählen, um die Ports zu erstellen, wird der Abschnitt **Port-Konfiguration** angezeigt. Das Installationsprogramm zeigt die Standard-Portnummern an, die den Domänenkomponenten zugewiesen sind. Sie können die für die Domänen- und Knotenkomponenten zu verwendenden Portnummern festlegen. Außerdem können Sie einen Bereich von Portnummern für den auf dem Knoten ausgeführten Serviceprozess angeben. Sie können die Standardportnummern verwenden oder neue Portnummern festlegen. Stellen Sie sicher, dass die eingegebenen Portnummern nicht bereits von anderen Anwendungen verwendet werden.

3. Wählen Sie **1**, um den Modellrepository-Dienst und den Datenintegrationsdienst über das Installationsprogramm zu erstellen. Wählen Sie **2**, um sie später zu erstellen.
4. Wählen Sie **1**, um den PowerCenter-Repository-Dienst und den PowerCenter-Integrationsdienst über das Installationsprogramm zu erstellen. Wählen Sie **2**, um sie später zu erstellen.

In der **Installationsübersicht** wird angezeigt, ob die Installation erfolgreich abgeschlossen wurde. Die Übersicht zeigt außerdem den Status der installierten Komponenten und ihre Konfiguration an.

Port-Konfiguration

Falls Sie sich entscheiden, die erweiterte Portkonfigurationsseite anzuzeigen, können Sie die Ports für die Domänenkomponenten festlegen.

- Geben Sie an der Eingabeaufforderung die neuen Portnummern ein oder drücken Sie die **Eingabetaste**, um die Standardportnummern zu verwenden.

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

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

Der Abschnitt **Installationsübersicht** wird angezeigt. In der **Installationsübersicht** wird angezeigt, ob die Installation erfolgreich abgeschlossen wurde. Der Bericht zeigt außerdem den Status der installierten Komponenten und deren Konfiguration an.

Konfigurieren der Modellrepository-Datenbank

Nachdem Sie die Domäne und den Knoten konfiguriert haben, können Sie die Eigenschaften der Modellrepository-Datenbank konfigurieren.

1. Geben Sie den Modellrepository-Dienstnamen ein.

Geben Sie den Dienstnamen ein. 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:

` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ()] [

Nachdem Sie den Dienst erstellt haben, können Sie seinen Namen nicht mehr ändern.

Bei Auswahl des SPN auf Prozessebene geben Sie die Keytab-Datei des Modellrepository-Diensts an. Die Keytab-Datei für den Modellrepository-Dienstprozess. Die Keytab-Datei muss folgenden Namen aufweisen: .keytab

2. Wählen Sie die Datenbank aus, um das Modellrepository zu konfigurieren.

In der folgenden Tabelle sind die Datenbanken aufgeführt, die Sie für das Modellrepository konfigurieren können:

Eingabeaufforderung	Beschreibung
Datenbanktyp	Der Datenbanktyp für das Modellrepository. Wählen Sie eine der folgenden Optionen aus: 1 – Oracle 2 – Microsoft SQL Server 3 – IBM DB2 4 – PostgreSQL

3. 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 in der Modellrepository-Datenbank. Sie können den Namen des Windows NT-Benutzers für eine vertrauenswürdige Verbindung in Microsoft SQL Server eingeben.
Benutzerpasswort	Das Passwort für das Konto des Modellrepository-Benutzers. Sie können das Windows NT-Passwort für eine vertrauenswürdige Verbindung in Microsoft SQL Server eingeben.

4. Geben Sie an, ob eine gesicherte Modellrepository-Datenbank erstellt werden soll.

In einer mit dem SSL-Protokoll gesicherten Datenbank können Sie einen Modellrepository-Dienst erstellen. Um einen Modellrepository-Dienst in einer gesicherten Datenbank zu erstellen, drücken Sie **1** und gehen Sie zu dem Schritt für die Eingabe der JDBC-Informationen.

Um einen Modellrepository-Dienst in einer ungesicherten Datenbank zu erstellen, drücken Sie **2**.

5. Wenn Sie kein gesichertes Modellrepository erstellen, geben Sie die Parameter für die Datenbank ein.

- a. Geben Sie bei Auswahl von IBM DB2 an, ob ein Tablespace konfiguriert werden soll. Geben Sie dann den Namen des Tablespace ein.

In der folgenden Tabelle werden die Eigenschaften beschrieben, die Sie für die IBM DB2-Datenbank konfigurieren müssen:

Eigenschaft	Beschreibung
Tablespace konfigurieren	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“ auswählen. Wählen Sie aus, ob ein Tablespace festgelegt werden soll. 1 – Nein 2 – Ja
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. Geben Sie in einer Datenbank mit einer einzigen Partition den Namen des Tablespace ein, in dem die Tabellen erstellt werden sollen. Geben Sie in einer Datenbank mit mehreren Partitionen den Namen des nicht partitionierten Tablespace an, der sich in der Katalogpartition der Datenbank befindet.

- b. Geben Sie bei Auswahl von Microsoft SQL Server oder PostgreSQL den Schemanamen für die Datenbank ein.

In der folgenden Tabelle werden die Eigenschaften beschrieben, die Sie für die -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.
Datenbankdienstname	Dienst- oder Datenbankname: <ul style="list-style-type: none">- Oracle: Geben Sie den Dienstnamen ein.- Microsoft SQL Server: Geben Sie den Datenbanknamen ein.- IBM DB2: Geben Sie den Dienstnamen ein.- PostgreSQL: Geben Sie den Namen der Datenbank ein.
JDBC-Parameter konfigurieren	Geben Sie an, ob der Verbindungszeichenfolge weitere JDBC-Parameter hinzugefügt werden sollen: 1 – Ja 2 – Nein Geben Sie bei Auswahl von „Ja“ die Parameter ein oder drücken Sie die Eingabetaste, um die Standardparameter zu übernehmen. Bei Auswahl von „Nein“ wird die JDBC-Verbindungszeichenfolge ohne Parameter erstellt.

- Um die Verbindungsdaten mithilfe einer benutzerdefinierten JDBC-Verbindungszeichenfolge einzugeben, geben Sie die Verbindungszeichenfolge ein.
Verwenden Sie die folgende Syntax in der JDBC-Verbindungszeichenfolge:

IBM DB2

```
jdbc:Informatica:db2://<hostname>:<portnummer>;DatabaseName=
```

Oracle

```
jdbc:Informatica:oracle://<hostname>:<portnummer>;ServiceName=
```

Verwenden Sie die folgende Verbindungszeichenfolge, um eine Verbindung zur Oracle-Datenbank über den Oracle Connection Manager herzustellen:

```
jdbc:Informatica:oracle:TNSNamesFile=<vollqualifizierter Pfad zur Datei  
tnsnames.ora>;TNSServerName=<TNS-Name>;
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://  
<hostname>:<portnummer>;SelectMethod=cursor;DatabaseName=
```

Microsoft SQL Server mit Windows NT-Anmeldeinformationen

Wenn Sie die Windows NT-Anmeldeinformationen für die Modellrepository-Datenbank in Microsoft SQL Server angegeben haben, schließen Sie die Authentifizierungsmethode mithilfe der Syntax der Verbindungszeichenfolge als NTLM ein.

Microsoft SQL Server, der die Standardinstanz mit Windows NT-Anmeldeinformationen verwendet:

```
"jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database  
name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft SQL Server, der eine benannte Instanz mit Windows NT-Anmeldeinformationen verwendet:

```
"jdbc:informatica:sqlserver://<host name>\<named instance  
name>;DatabaseName=<database  
name>;SnapshotSerializable=true;authenticationMethod=NTLM"
```

Microsoft Azure SQL-Datenbank

```
jdbc:Informatica:sqlserver://  
<hostname>:<portnummer>;SelectMethod=cursor;DatabaseName=<datenbankname>;Snap  
shotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.win  
dows.net;ValidateServerCertificate=false
```

Azure SQL-Datenbank mit Active Directory-Authentifizierung

```
"jdbc:informatica: sqlserver://  
<host_name>:<port_number>;database=<database_name>;encrypt=true;Authentication  
Method=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertific  
ate=*.database.windows.net;loginTimeout=<seconds>"
```

PostgreSQL

```
jdbc:Informatica:postgresql://<hostname>:<portnummer>;DatabaseName=
```

Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TLsv1.2;
```

Stellen Sie sicher, dass die Verbindungszeichenfolge alle vom Datenbanksystem benötigten Verbindungsparameter enthält.

Der Abschnitt **Serviceparameter** wird angezeigt.

Datenintegrationsdienst

Nachdem Sie die Modellrepository-Datenbank konfiguriert haben, können Sie die Dienstparameter für die Anwendungsdienste konfigurieren.

1. Geben Sie die folgenden Informationen für Dienstparameter ein:

Port	Beschreibung
Name des Datenintegrationsdiensts	Der Name des Datenintegrationsdiensts, der in der Informatica-Domäne erstellt werden soll.
HTTP-Protokolltyp	Typ der Verbindung zum Datenintegrationsdienst. Wählen Sie eine der folgenden Optionen aus: <ul style="list-style-type: none">- HTTP. Erfordert, dass der Dienst eine HTTP-Verbindung benutzt.- HTTPS. Erfordert, dass der Dienst eine sichere HTTP-Verbindung benutzt.- HTTP&HTTPS. In Anfragen an den Dienst kann entweder eine HTTP- oder eine HTTPS-Verbindung verwendet werden.
HTTP-Port	Für den Datenintegrationsdienst zu verwendende Portnummer. Der Standardwert ist 9085.
HTTPS-Port	Für den Datenintegrationsdienst zu verwendende Portnummer. Der Standardwert ist 9085.

- Wählen Sie die SSL-Zertifikate aus, die für den Schutz des Datenintegrationsdiensts verwendet werden sollen.

Option	Beschreibung
SSL-Standardzertifikatsdateien von Informatica verwenden	<p>Zur Verwendung der im Standardschlüsselspeicher und im Truststore enthaltenen SSL-Standardzertifikate von Informatica.</p> <p>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.</p>
Benutzerdefinierte SSL-Zertifikate verwenden	<p>Zur Verwendung von benutzerdefinierten SSL-Zertifikaten. Sie müssen den Speicherort der Schlüsselspeicher- und Truststore-Dateien angeben.</p> <p>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.</p>

Wenn Sie benutzerdefinierte SSL-Zertifikate verwenden möchten, geben Sie die folgenden Informationen ein.

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.

PowerCenter-Repository-Dienst und PowerCenter-Integrationsdienst

Sie können den PowerCenter-Repository-Dienst und den PowerCenter-Integrationsdienst konfigurieren.

- Wählen Sie die Datenbank aus, die für das PowerCenter-Repository konfiguriert werden soll.
Sie können das PowerCenter-Repository mit einer der folgenden Datenbanken konfigurieren:
 - Oracle
 - Microsoft SQL Server
 - PostgreSQL

2. 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 für das Konto des Benutzers der PowerCenter-Repository-Datenbank.
Benutzerpasswort	Das Passwort des Benutzerkontos für die PowerCenter-Konfigurationsdatenbank.
Datenbankdienstname	Dienst- oder Datenbankname für PowerCenter: <ul style="list-style-type: none">- Oracle: Geben Sie den Dienstnamen ein.- Microsoft SQL Server: Geben Sie den Datenbanknamen ein.- PostgreSQL: Geben Sie den Namen der Datenbank ein.
Hostname der Datenbank	Geben Sie den Hostnamen für die PowerCenter Datenbank ein .

3. Geben Sie den Namen des zu erstellenden PowerCenter-Repository-Diensts ein.
4. Geben Sie den Namen des zu erstellenden PowerCenter-Integrationsdiensts ein.
5. Wählen Sie die Codepage des PowerCenter-Repository-Diensts aus. Der Standardwert ist 7-Bit-ASCII.
6. Wählen Sie die Codepage des PowerCenter-Integrationsdiensts aus. Der Standardwert ist 7-Bit-ASCII.

In der **Installationsübersicht** wird angezeigt, ob die Installation erfolgreich abgeschlossen wurde. Die Übersicht zeigt außerdem den Status der installierten Komponenten und ihre Konfiguration an.

KAPITEL 9

Installation von Informatica-Diensten im Grafikmodus

Dieses Kapitel umfasst die folgenden Themen:

- [Übersicht über die Installation der Dienste im Grafikmodus, 175](#)
- [Erstellen einer Domäne, 175](#)
- [Beitreten zu einer Domäne, 224](#)

Übersicht über die Installation der Dienste im Grafikmodus

Sie können die Informatica-Dienste im Grafikmodus unter Windows installieren.

Wenn Sie das Vorinstallations-Systemprüfungstool (i10Pi) vor der Installation ausführen, legt das Installationsprogramm die Werte für bestimmte Felder (beispielsweise die Datenbankverbindung und die Domänenportnummern) basierend auf den während der Systemüberprüfung eingegebenen Daten fest.

Wenn unter Windows beim Ausführen der Datei „install.bat“ im Root-Verzeichnis Probleme auftreten, führen Sie folgende Datei aus: <Verzeichnis der Installationsdateien>\server\install.exe

Erstellen einer Domäne

Erstellen Sie eine Domäne, wenn Sie zum ersten Mal installieren oder Knoten in separaten Domänen verwalten möchten.

Ausführen des Installationsprogramms

Führen Sie die folgenden Schritte aus, um das Installationsprogramm auszuführen:

1. Melden Sie sich mit einem Systembenutzerkonto am Computer an.
2. Schließen Sie alle anderen Anwendungen.

3. Wechseln Sie in das Stammverzeichnis für die Installationsdateien und führen Sie die Datei „install.bat“ als Administrator aus.

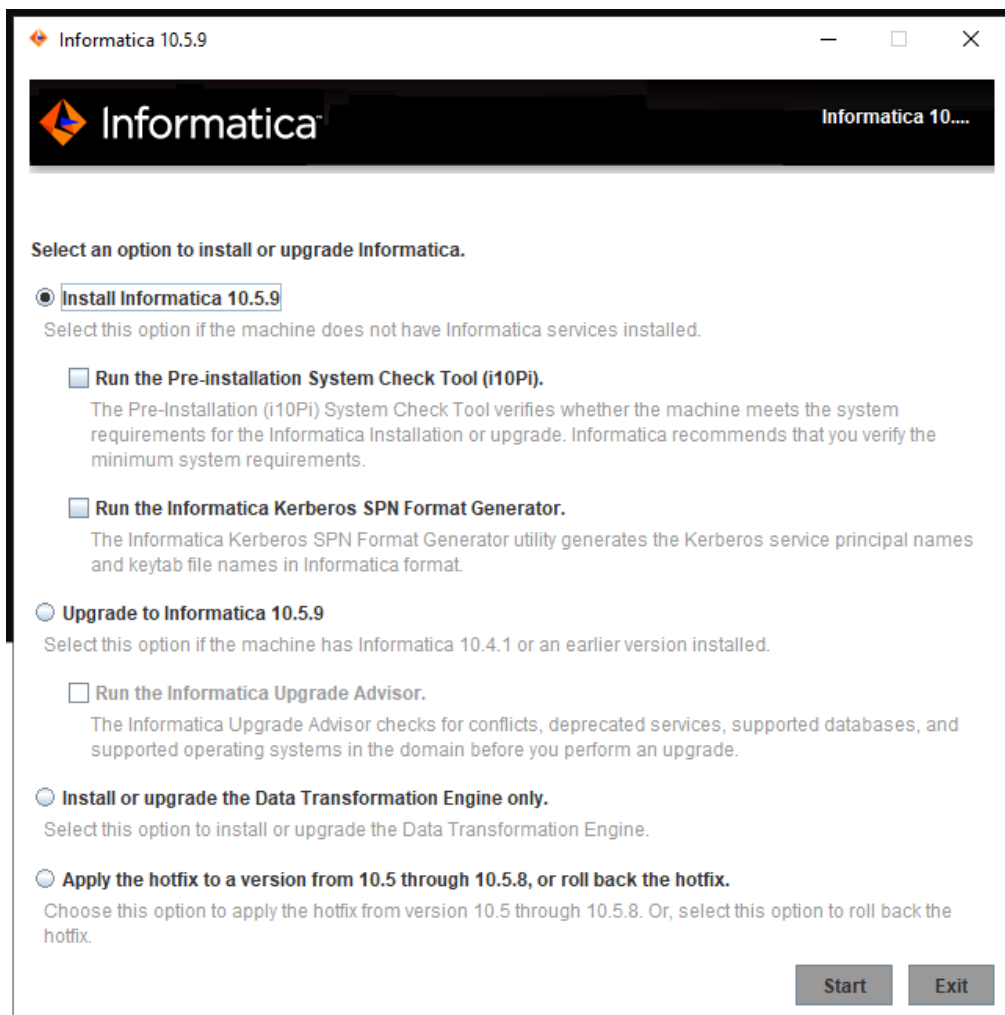
Klicken Sie zum Ausführen der Datei als Administrator mit der rechten Maustaste auf die Datei „install.bat“ und wählen Sie **Als Administrator ausführen** aus.

Hinweis: Wenn Sie das Installationsprogramm nicht als Administrator ausführen, meldet der Windows-Systemadministrator möglicherweise Probleme, wenn Sie auf die Dateien im Informatica-Installationsverzeichnis zugreifen.

Die Seite Informatica 10.5.9 wird geöffnet.

Willkommen beim Informatica-Installationsprogramm

1. Wählen Sie **Informatica 10.5.9** aus.



Informatica stellt Dienstprogramme bereit, um die Installation der Informatica-Dienste zu vereinfachen. Führen Sie die folgenden Dienstprogramme vor der Installation von Informatica-Diensten aus:

- Vorinstallations-Systemprüfungstool (i10Pi). Stellt sicher, dass der Computer, auf dem die Informatica-Dienste installiert werden, die Systemanforderungen für die Installation erfüllt.
Weitere Informationen zum Ausführen des Vorinstallations-Systemprüfungstools (i10Pi) finden Sie unter [“Ausführen des Vorinstallations-Systemprüfungstools \(i10Pi\) im Grafikmodus” auf Seite 115](#).
- Kerberos SPN-Formatgenerator von Informatica. Erstellt eine Liste der Kerberos-Dienstprinzipalnamen und Keytab-Dateinamen, die zum Ausführen von Informatica-Diensten in einem Netzwerk mit Kerberos-Authentifizierung benötigt werden.

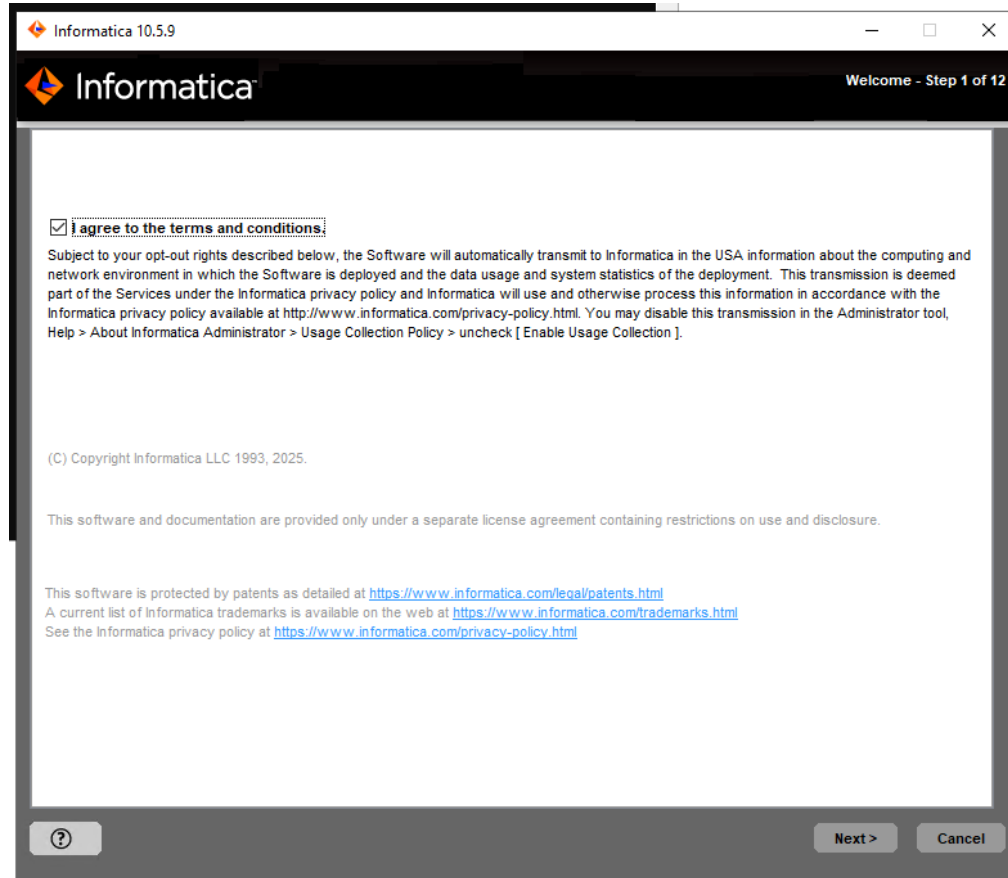
Sie können das Installationsprogramm zum Ausführen der Dienstprogramme verwenden, bevor Sie die Informatica-Dienste installieren. Starten Sie nach dem Beenden eines Dienstprogramms das Installationsprogramm erneut, um das nächste Dienstprogramm auszuführen oder die Informatica-Dienste zu installieren.

2. Klicken Sie auf **Start**.

Der Abschnitt **Willkommen** wird angezeigt.

Willkommen – Akzeptieren der allgemeinen Geschäftsbedingungen

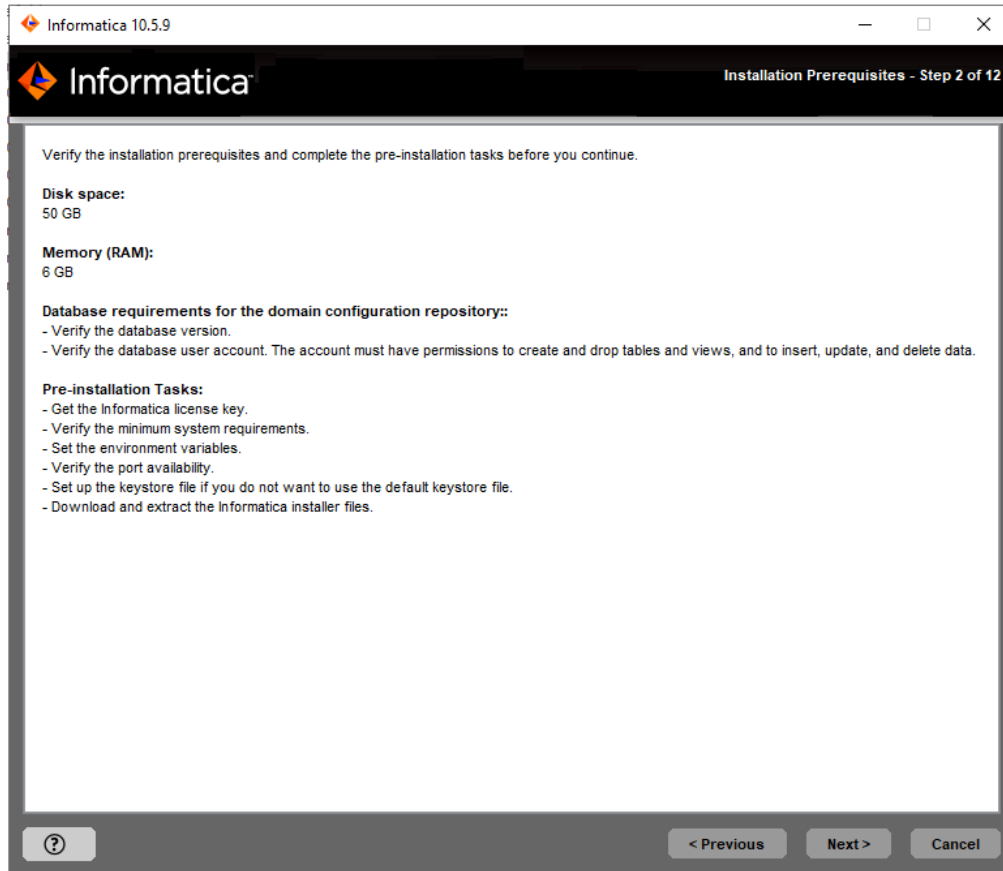
1. Lesen Sie die Bedingungen für die Informatica-Installation und das Toolkit zur Produktverwendung und wählen Sie **Ich stimme den Bedingungen zu** aus.



Informatica DiscoveryIQ ist ein Produktnutzungstool, das Routineberichte über Datennutzung und Systemstatistiken an Informatica sendet. Nach der Installation und Konfiguration der Informatica-Domäne lädt Informatica DiscoveryIQ alle 15 Minuten Daten an Informatica hoch. Danach sendet die Domäne die Daten alle 30 Tage. Sie können die Verwendung von Statistiken im Administrator Tool deaktivieren.

2. Klicken Sie auf **Weiter**.

Auf der Seite **Installationsvoraussetzungen** werden die Installationsanforderungen angezeigt. Stellen Sie sicher, dass alle Voraussetzungen erfüllt sind, bevor Sie die Installation fortsetzen.



3. Klicken Sie auf „Weiter“.

Der Abschnitt **Lizenz- und Installationsverzeichnis** wird angezeigt.

Lizenz und Installationsverzeichnis

Nachdem Sie die Installationsvoraussetzungen überprüft haben, können Sie das Installationsverzeichnis angeben.

1. Geben Sie auf der Seite **Lizenz und Installationsverzeichnis** den Informatica-Lizenzschlüssel, das Installationsverzeichnis, die Installationsumgebung und die Verteilungspakete ein.

In der folgenden Tabelle werden der Lizenzschlüssel und das Verzeichnis beschrieben, die für die Installation der Informatica-Dienste und die Installation der Integrationspakete angegeben werden:

Eigenschaft	Beschreibung
Lizenzschlüsseldatei	Pfad und Dateinamen des Informatica-Lizenzschlüssels.
Installationsverzeichnis	<p>Absoluter Pfad für das Installationsverzeichnis. Das Installationsverzeichnis muss sich auf dem Computer befinden, auf dem Informatica installiert wird. Die Verzeichnisnamen im Pfad dürfen weder Leerzeichen noch die folgenden Sonderzeichen enthalten: @ * \$ # ! % () { } []</p> <p>Hinweis: Informatica empfiehlt die Verwendung alphanumerischer Zeichen im Installationsverzeichnispfad. Wenn Sie ein Sonderzeichen wie á oder € verwenden, können zur Laufzeit unerwartete Ergebnisse auftreten.</p>
Installationsumgebung	<p>Umgebungstyp, der der Installation der Informatica-Dienste zugeordnet ist.</p> <ul style="list-style-type: none"> - Legen Sie die Sandbox-Umgebung für eine Basisumgebung fest, die für Machbarkeitsstudien mit minimaler Benutzerzahl verwendet wird. - Legen Sie die Entwicklungsumgebung für die Designumgebung fest. - Legen Sie die Testumgebung für die Verarbeitung großer Datenmengen ähnlich der in einer Produktionsumgebung fest. - Legen Sie die Produktionsumgebung für die massiv parallele Verarbeitung großer Datenmengen für Endbenutzer fest. Bei erweiterten Produktionsumgebungen handelt es sich in der Regel um Setups mit mehreren Knoten.
Verteilungspakete	<p>Sie können auswählen, ob die Verteilungspakete über das Informatica-Installationsprogramm installiert werden sollen.</p> <p>Wenn Sie Verteilungspakete installieren möchten, wählen Sie ein oder mehrere Pakete aus der Liste aus, die Sie installieren möchten.</p>

Informatica 10.5.9

Informatica License and Installation Directory - Step 3 of 12

Specify the license key and directory for the installation.

Enter the installation directory:

C:\Informatica\10.5.9_server ... Default

☐ Do you want to enable Kerberos network authentication for the Informatica domain?

Enter the path to the license key file:

C:\license\1057_License_12071.key ...

Installation environment:

Sandbox

You must install an integration package to process complex files within the domain, or to connect to a Hadoop or Databricks environment but process within the domain.

☒ Do you want to install them now?

- Cloudera 7.2
- Cloudera 7.218
- Databricks 10.4
- Databricks 11.3
- Dataproc 2.0
- Elastic MapReduce 6.4
- Elastic MapReduce 7.1
- MapR 7.2

? < Previous Next > Cancel

2. Klicken Sie auf **Weiter**.

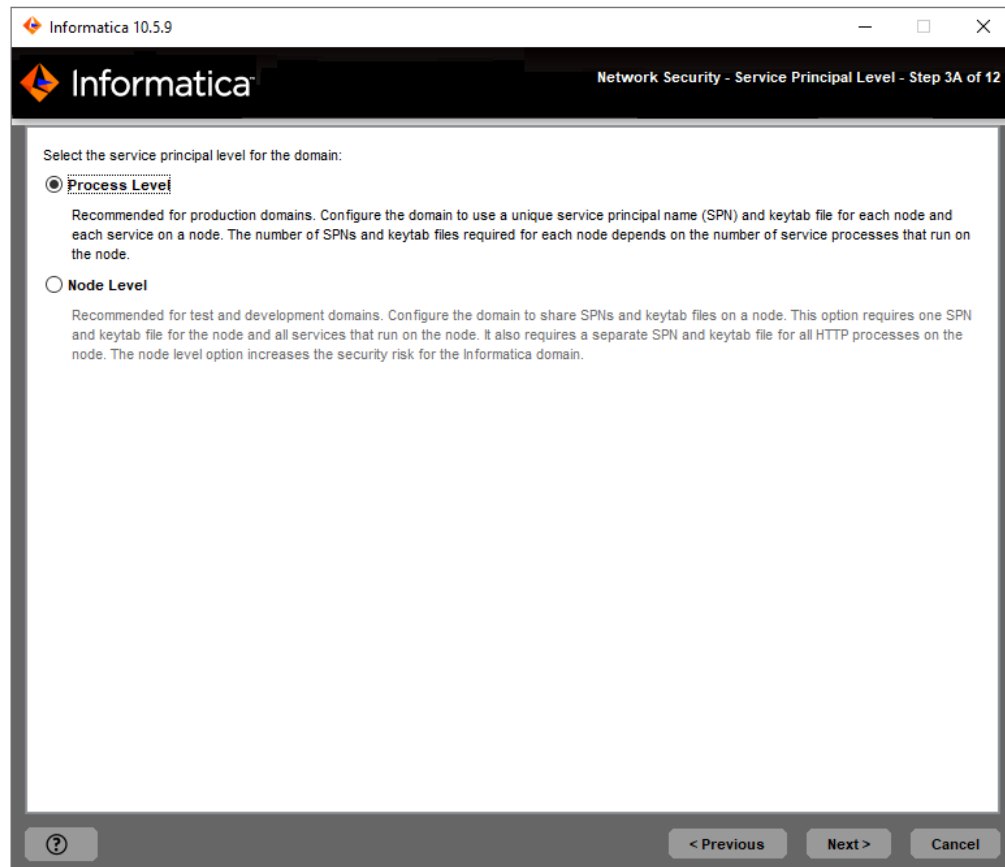
Wenn Sie die Kerberos-Netzwerkauthentifizierung aktiviert haben, wird der Abschnitt **Dienstprinzipalebene** angezeigt.

Wenn Kerberos-Netzwerkauthentifizierung nicht aktiviert wurde, wird der Abschnitt **Vorinstallationsübersicht** angezeigt. Überprüfen Sie die Installationsinformationen und drücken Sie die **Eingabetaste**, um fortzufahren. Fahren Sie mit ["Domänenauswahl" auf Seite 127](#) fort.

Netzwerksicherheit – Dienstprinzipalebene

Nachdem Sie das Installationsverzeichnis angegeben haben, können Sie die Sicherheitsstufe konfigurieren.

1. Wenn Sie die Kerberos-Netzwerkauthentifizierung aktiviert haben, wird die Seite **Netzwerksicherheit – Dienstprinzipalebene** angezeigt.



2. Wählen Sie auf der Seite **Netzwerksicherheit - Dienstprinzipalebene** die Ebene aus, auf die Sie die Kerberos-Dienstprinzipale für die Domäne festlegen möchten.

In der folgenden Tabelle werden die Dienstprinzipalebenen beschrieben, die Sie auswählen können:

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

3. Klicken Sie auf **Weiter**.

Der Abschnitt **Netzwerksicherheit – Kerberos-Authentifizierung** wird angezeigt.

Network Security - Kerberos Authentication

After you configure the security level, you can configure Kerberos authentication.

- 1. The **Network Security - Kerberos Authentication** page, enter the domain and keytab information required for Kerberos authentication.

The following table describes the Informatica domain and node information that you must provide:

Property	Description
Domain name	Name of the domain to create. Der Name darf maximal 128 Zeichen umfassen und muss im 7-Bit-ASCII-Format vorliegen. Der Name darf weder Leerzeichen noch eines der folgenden Zeichen enthalten: ` % * + ; " ? , < > \ /
Node name	Name des zu erstellenden Knotens.
Node host name	Fully qualified host name or IP address of the machine on which to create the node. Hinweis: Der Hostname des Knotens darf keine Unterstriche (_) enthalten. Verwenden Sie nicht localhost. Der Hostname muss den Computer eindeutig kennzeichnen.

In der folgenden Tabelle werden der Kerberos-Bereich und die Keytab-Informationen beschrieben, die Sie angeben müssen:

Eigenschaft	Beschreibung
Dienstbereichsname	<p>Name des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird. Der Bereichsname muss in Großbuchstaben angegeben werden und unterliegt der Groß-/Kleinschreibung.</p> <p>Zum Konfigurieren von bereichsübergreifender Kerberos-Authentifizierung geben Sie den Namen des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird, getrennt durch Kommas ein. Beispiel: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM</p> <p>Verwenden Sie ein Sternchen als Platzhalterzeichen vor dem Bereichsnamen, um alle Bereiche mit diesem Namen einzuschließen. Beispiel: *EAST.COMPANY.COM</p>
Benutzerbereichsname	<p>Name des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird. Der Bereichsname muss in Großbuchstaben angegeben werden und unterliegt der Groß-/Kleinschreibung.</p> <p>Zum Konfigurieren von bereichsübergreifender Kerberos-Authentifizierung geben Sie den Namen des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird, getrennt durch Kommas ein. Beispiel: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM</p> <p>Verwenden Sie ein Sternchen als Platzhalterzeichen vor dem Bereichsnamen, um alle Bereiche mit diesem Namen einzuschließen. Beispiel: *EAST.COMPANY.COM</p>
Keytab-Verzeichnis	<p>Verzeichnis, in dem alle Keytab-Dateien für die Informatica-Domäne gespeichert werden. Der Name einer Keytab-Datei in der Informatica-Domäne muss einem von Informatica festgelegten Format entsprechen.</p>
Kerberos-Konfigurationsdatei	<p>Pfad und Dateiname der Kerberos-Konfigurationsdatei. Informatica benötigt folgenden Namen für die Kerberos-Konfigurationsdatei: <i>krb5.conf</i></p>

Wichtig: Wenn Sie die Domäne zur Ausführung mit Kerberos-Authentifizierung konfigurieren, müssen der Domänen- und Knotenname sowie der Knoten-Hostname mit den Namen übereinstimmen, die bei Ausführung des Kerberos SPN-Formatgenerators von Informatica zum Erzeugen der SPNs und Keytab-Dateinamen angegeben wurden. Wenn Sie einen anderen Domänen-, Knoten- oder Hostnamen verwenden, erzeugen Sie den SPN und die Keytab-Dateinamen neu und bitten Sie den Kerberos-Administrator, den neuen SPN der Kerberos-Prinzipaldatenbank hinzuzufügen und die Keytab-Dateien zu erstellen.

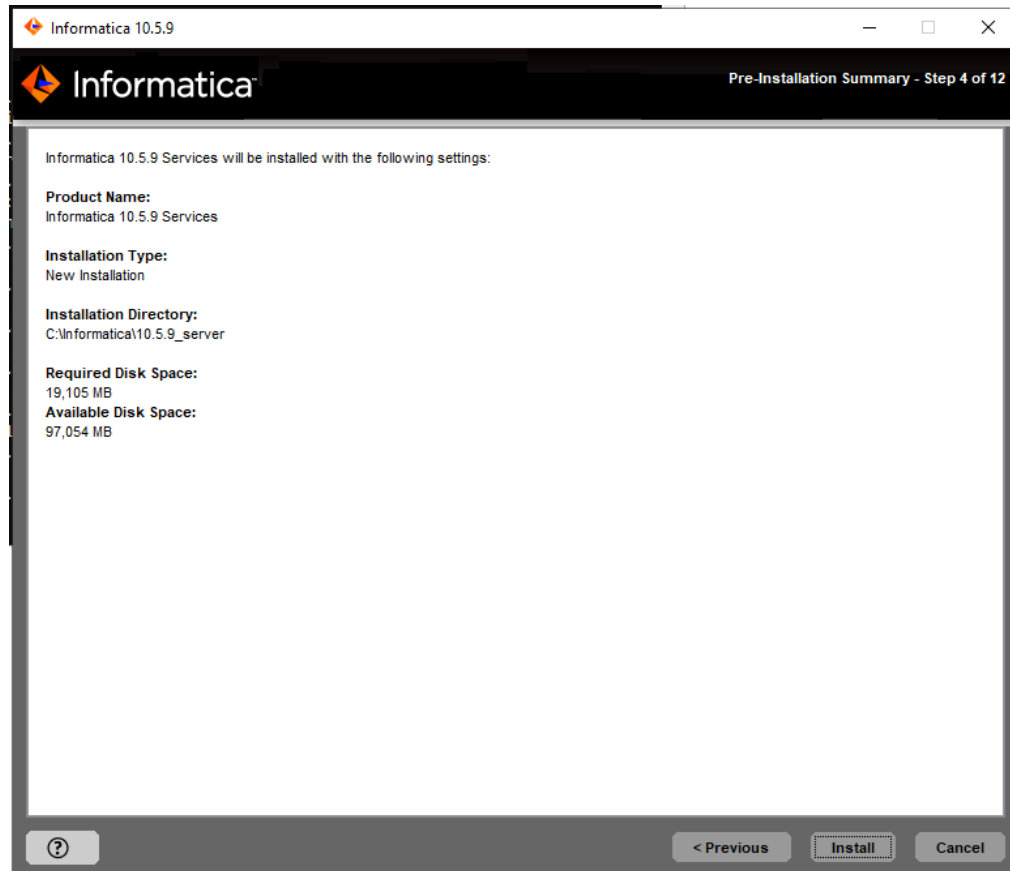
2. Click **Next**.

The **Pre-Installation Summary** section appears. Review the installation information.

Domänenauswahl

Nachdem Sie sich die Vorinstallationszusammenfassung durchgesehen haben, können Sie die Domäneninformationen eingeben.

1. Überprüfen Sie die Seite **Vor der Installation – Zusammenfassung**.



2. Überprüfen Sie die Installationsinformationen und klicken Sie auf **Installieren**, um fortzufahren.

Der Installer kopiert die Informatica-Dateien in das Installationsverzeichnis. Nach dem Kopieren der Dateien durch das Installationsprogramm wird die Seite **Domänenauswahl** angezeigt.

Informatica 10.5.9

Informatica Domain Selection - Step 5 of 12

Do you want to create a domain or join a domain?

☒ **Create a domain.**
Create an Informatica domain if you are installing for the first time or if you are creating multiple domains.

☒ **Do you want to enable secure communication for the domain?**

☐ **Join a domain.**
Join an Informatica domain on another node.

☐ Do you want to join a secure domain?

☐ Do you want this node to be a gateway node?

☒ **Enable HTTPS for Informatica Administrator.** Port:

☒ **Use the default keystore generated by the installer.**

☐ **Specify the location and password of a custom keystore file.**
Keystore password:
Keystore file:

☐ **Do you want to enable Security Assertion Markup Language (SAML) authentication?**

? Next > Cancel

3. Wählen Sie **Eine Domäne erstellen** aus.

Beim Erstellen einer Domäne übernimmt der zugehörige Knoten die Funktion eines Gateway-Knotens in der Domäne. Der Gateway-Knoten enthält einen Dienstmanager, der alle Domänenvorgänge verwaltet.

4. Aktivieren Sie das Kontrollkästchen, um sichere Kommunikation zwischen Diensten in der Domäne zu aktivieren.

Wenn Sie sichere Kommunikation für die Domäne aktivieren, richtet das Installationsprogramm standardmäßig eine HTTPS-Verbindung für Informatica Administrator ein. Sie können auch ein Domänenkonfigurations-Repository für eine gesicherte Datenbank erstellen.

5. Wählen Sie zum Sichern der Verbindung zu Informatica Administrator **HTTPS für Informatica Administrator aktivieren** aus.

In der folgenden Tabelle werden die Eigenschaften beschrieben, die Sie für eine sichere Verbindung zum Administrator Tool einrichten:

Eigenschaft	Beschreibung
HTTPS für Informatica Administrator aktivieren	Wählen Sie diese Option zum Sichern der Verbindung zu Informatica Administrator. Deaktivieren Sie diese Option, um eine ungesicherte HTTP-Verbindung zu verwenden. Wenn sichere Kommunikation für die Domäne aktiviert ist, wird diese Option vom Installationsprogramm aktiviert. Sie können diese Option auch aktivieren, wenn für die Domäne keine gesicherte Kommunikation aktiviert wurde.
Port	Der für die Kommunikation zwischen Informatica Administrator und dem Dienstmanager zu verwendende Port.
Vom Installer generierte Schlüsselspeicherdatei verwenden	Verwenden Sie eine vom Installationsprogramm generierte selbstsignierte Schlüsselspeicherdatei. Das Installationsprogramm erstellt eine Schlüsselspeicherdatei mit dem Namen Default.keystore am folgenden Speicherort: <Informatica-Installationsverzeichnis>\tomcat\conf\
Schlüsselspeicherdatei und Passwort eingeben	Verwenden Sie eine selbst erstellte Schlüsselspeicherdatei. Sie können eine Schlüsselspeicherdatei mit einem selbstsignierten Zertifikat oder einem von einer Zertifizierungsbehörde signierten Zertifikat verwenden.
Schlüsselspeicher-Passwort	Ein Volltext-Passwort für die Schlüsselspeicherdatei. Bei Verwendung einer von Ihnen erstellten Schlüsselspeicherdatei erforderlich.
Schlüsselspeicherdatei	Pfad und Dateiname der Schlüsselspeicherdatei. Bei Verwendung einer von Ihnen erstellten Schlüsselspeicherdatei erforderlich.

- Zur Konfiguration der Unterstützung von Single Sign-On (SSO) auf der Basis der Security Assertion Markup Language (SAML) für webbasierte Informatica-Anwendungen in einer Informatica-Domäne aktivieren Sie das Kontrollkästchen, um die SAML-Authentifizierung zu aktivieren.

Hinweis: Wenn Sie die Kerberos-Netzwerkauthentifizierung aktivieren, können Sie die SAML-Authentifizierung nicht konfigurieren.

- Klicken Sie auf **Weiter**.

Wenn Sie das Kontrollkästchen zum Aktivieren der SAML-Authentifizierung aktiviert haben, wird die Seite **SAML-Authentifizierung** angezeigt.

The screenshot shows the Informatica 10.5.9 SAML Authentication configuration window, Step 5A of 12. The window has a title bar with the Informatica logo and version number. The main content area is titled "SAML Authentication - Step 5A of 12".

Identity Provider URL

☒ Do you want to enter a relying party trust name or a service provider identifier? If you choose No, the service provider identifier

Service Provider ID

☒ Enable SAML Assertion Signature Validation

SAML Assertion Signing Certificate Alias Name

Select the truststore for SAML authentication where you imported the identity provider assertion signing certificate

☒ Use the default Informatica truststore and keystore.

☐ Use a custom truststore and keystore.

Specify the directory that contains the custom truststore to use for SAML authentication:

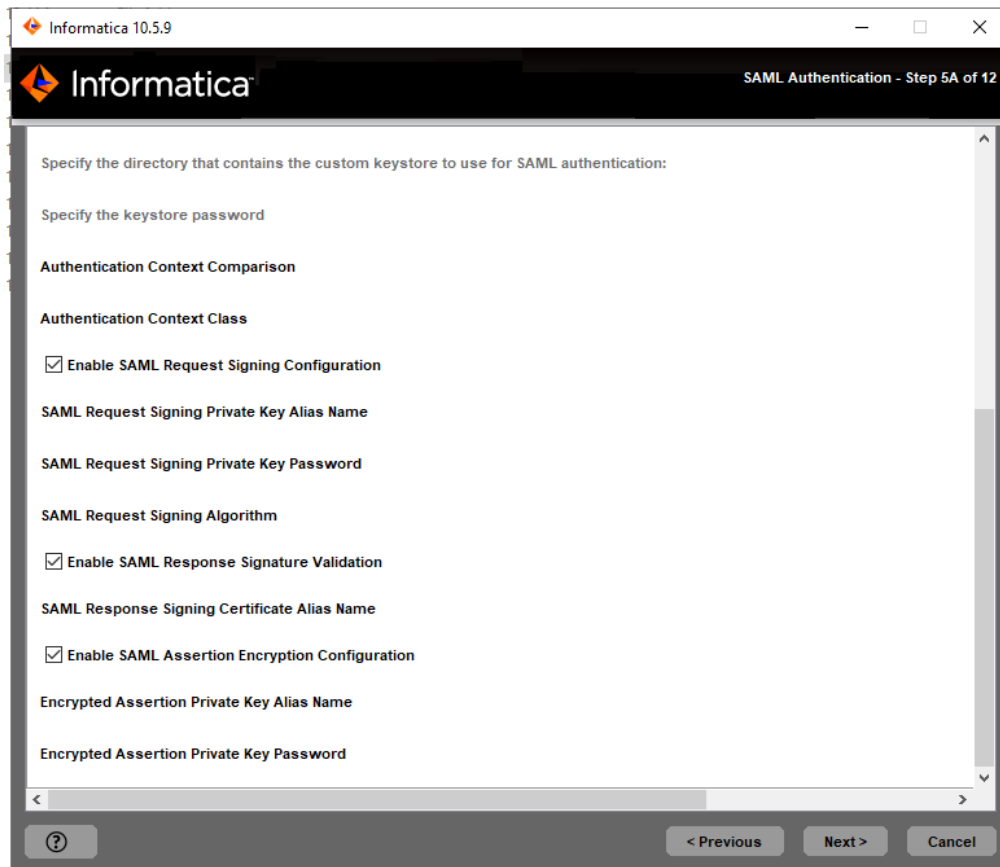
Specify the truststore password

Specify the directory that contains the custom keystore to use for SAML authentication:

Specify the keystore password

Authentication Context Comparison

At the bottom, there is a progress bar and navigation buttons: "?", "< Previous", "Next >", and "Cancel".



8. Geben Sie die URL des Identitäts-Providers für die Domäne ein.
9. Geben Sie den Vertrauensstellungsamen der vertrauenswürdigen Partei oder die Dienstanbieter-ID für die Domäne an, wie im Identitätsanbieter definiert. Wenn Sie „Nein“ auswählen, wird die Dienstanbieter-ID auf „Informatica“ festgelegt.
10. Geben Sie an, ob der IdP die SAML-Assertion signiert oder nicht.
11. Geben Sie den Aliasnamen des Signierzertifikats für die Identitätsanbieter-Assertion ein.
12. Geben Sie an, ob die standardmäßigen SSL-Zertifikate von Informatica oder eigene SSL-Zertifikate zum Aktivieren sicherer Kommunikation in der Domäne verwendet werden sollen.

In der folgenden Tabelle werden die SSL-Zertifikatsoptionen für die SAML-Authentifizierung beschrieben:

Option	Beschreibung
Standardmäßige SSL-Zertifikatsdatei von Informatica verwenden	Wählen Sie diese Option aus, um für die SAML-Authentifizierung die Truststore-Standarddatei von Informatica zu verwenden.
Speicherort der SSL-Zertifikatsdatei eingeben	Wählen Sie diese Option, um eine benutzerdefinierte Informatica-Truststore-Datei für die SAML-Authentifizierung zu verwenden. Geben Sie das Verzeichnis an, das die benutzerdefinierte Truststore-Datei auf Gateway-Knoten in der Domäne enthält. Geben Sie nur das Verzeichnis an, nicht den vollständigen Dateipfad.

13. Wenn Sie die Sicherheitszertifikate bereitstellen, geben Sie den Speicherort und die Passwörter der Schlüsselspeicher- und Truststore-Dateien an.

In der folgenden Tabelle werden Verzeichnis und Passwort der Truststore- und Schlüsselspeicherdateien beschrieben:

Eigenschaft	Beschreibung
Truststore-Verzeichnis	Geben Sie das Verzeichnis an, das die benutzerdefinierte Truststore-Datei auf Gateway-Knoten in der Domäne enthält. Geben Sie nur das Verzeichnis an, nicht den vollständigen Dateipfad.
Truststore-Passwort	Das Passwort für die benutzerdefinierte Truststore-Datei.
Schlüsselspeicherverzeichnis	Geben Sie das Verzeichnis an, das die benutzerdefinierte Schlüsselspeicherdatei enthält.
Schlüsselspeicherpasswort	Das Passwort für die benutzerdefinierte Schlüsselspeicherdatei.

14. Geben Sie zum Festlegen des Authentifizierungskontextvergleichs den Stärkevergleich des vom Benutzer verwendeten Authentifizierungsmechanismus mit dem IdP-Server an.

Unterstützte Werte sind die Optionen MINIMUM, MAXIMUM, BETTER oder EXACT. Standard ist MINIMUM.

15. Geben Sie zum Festlegen der Authentifizierungskontextklasse den erwarteten Mechanismus für die erstmalige Authentifizierung des Benutzers beim IdP-Server an.

Unterstützte Werte sind PASSWORD oder PASSWORDPROTECTEDTRANSPORT. Standard ist PASSWORD.

16. Geben Sie an, ob die Webanwendung die SAML-Authentifizierungsanforderung signieren soll oder nicht. Der Standardwert ist „Deaktiviert“.

17. Geben Sie den Aliasnamen des privaten Schlüssels an, der in den SAML-Schlüsselspeicher des Knotens importiert wurde mit dem die SAML-Anfrage signiert werden soll.

18. Geben Sie das Passwort für den Zugriff auf den privaten Schlüssel an, der zum Signieren der SAML-Anforderung verwendet wird.

19. Geben Sie den Algorithmus an, den die Webanwendung zum Signieren der SAML-Anforderung verwendet.

Unterstützte Werte sind RSA_SHA256, DSA_SHA1, DSA_SHA256, RSA_SHA1, RSA_SHA224, RSA_SHA384, RSA_SHA512, ECDSA_SHA1, ECDSA_SHA224, ECDSA_SHA256, ECDSA_SHA384, ECDSA_SHA512, RIPEMD160 oder RSA_MD5.

20. Geben Sie an, ob IdP die SAML-Antwort signieren soll oder nicht.

Wählen Sie mit dieser Option, ob die Web-App die signierte SAML-Antwort empfangen kann oder nicht. Der Standardwert ist „Deaktiviert“.

21. Geben Sie an, ob der IdP die SAML-Assertion verschlüsselt oder nicht.

Wählen Sie diese Option, damit die Web-App eine verschlüsselte SAML-Assertion empfangen kann. Der Standardwert ist „Aktiviert“.

22. Geben Sie den Aliasnamen des privaten Schlüssels im SAML-Truststore des Gateway-Knotens an, den Informatica zum Entschlüsseln der SAML-Assertion verwendet.

23. Geben Sie das Passwort für den Zugriff auf den privaten Schlüssel an, der zum Entschlüsseln des Assertion-Verschlüsselungsschlüssels verwendet wird.

24. Klicken Sie auf **Weiter**.

Wenn Sie die sichere Kommunikation für die Domäne nicht aktivieren, wird die Seite **Domänenkonfigurations-Repository** angezeigt. Fahren Sie mit dem Schritt fort, der die Seite „Domänenkonfigurations-Repository“ beschreibt. Wenn Sie das Kontrollkästchen zum Aktivieren der sicheren Kommunikation für die Domäne aktiviert haben, wird die Seite **Domänensicherheit – Sichere Kommunikation** angezeigt.

Domänensicherheit – Sichere Kommunikation

Nachdem Sie die Domänen konfiguriert haben, können Sie die Domänensicherheit konfigurieren.

1. Geben Sie auf der Seite **Domänensicherheit – Sichere Kommunikation** an, ob die standardmäßigen SSL-Zertifikate von Informatica oder eigene SSL-Zertifikate zum Aktivieren sicherer Kommunikation in der Domäne verwendet werden sollen.

The screenshot shows the Informatica 10.5.9 configuration window titled "Domain Security - Secure Communication - Step 5B of 12". The main instruction is "Select the SSL certificates to enable secure communication within the domain:". There are two radio button options: the first is selected and reads "Use the default Informatica SSL certificates contained in the default keystore and truststore.", and the second is "Use custom SSL certificates. Specify the path, file name, and passwords for the keystore and truststore files that contain the certificates". Below these options are four input fields: "Keystore file directory:" (containing "c:\temp"), "Keystore password:" (empty), "Truststore file directory:" (containing "c:\temp"), and "Truststore password:" (empty). At the bottom, there is a question mark icon, a "< Previous" button, a "Next >" button, and a "Cancel" button.

In der folgenden Tabelle werden die SSL-Zertifikatsoptionen zum Sichern der Informatica-Domäne beschrieben:

Option	Beschreibung
SSL-Standardzertifikate 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 standardmäßigen Schlüsselspeicherdateien und Truststore-Dateien von Informatica verwenden, ist 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.
Benutzerdefinierte SSL-Zertifikate verwenden	Geben Sie den Pfad zur Schlüsselspeicher- und zur Truststore-Datei ein, die die SSL-Zertifikate enthalten. Sie können ein selbstsigniertes Zertifikat oder ein von einer Zertifizierungsstelle ausgegebenes Zertifikat angeben. 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-Dateien und Schlüsselspeicherdateien in einem Verzeichnis, auf das alle Knoten in der Domäne zugreifen können, und geben Sie für alle Knoten in derselben Domäne dasselbe Verzeichnis für Schlüsselspeicherdateien und Truststore-Dateien an. Um die privaten Truststore-Dateien festzulegen, müssen Sie die Zertifikate manuell importieren. Führen Sie den keytool-Befehl im Verzeichnis <INFA_JDK_HOME> aus, um die privaten Truststore-Zertifikate zu importieren. Verwenden Sie beispielsweise den folgenden keytool-Befehl: keytool -noprompt -importkeystore -srckeystore <source truststore file path> -srcstorepass <source truststore file password> -srcalias <alias> -srcstoretype JKS -destkeystore <destination truststore file path> -deststorepass <destination truststore file password> -keypass <private key password> -deststoretype JKS

- Wenn Sie die Sicherheitszertifikate bereitstellen, geben Sie den Speicherort und die Passwörter der KeyStore- und Truststore-Dateien an.

In der folgenden Tabelle werden die Parameter beschrieben, die für die SSL-Zertifikatsdateien eingegeben werden müssen:

Eigenschaft	Beschreibung
Verzeichnis der Schlüsselspeicherdatei	Das Verzeichnis, das die Schlüsselspeicherdateien enthält. Das Verzeichnis muss Dateien namens infa_keystore.jks und infa_keystore.pem enthalten.
Schlüsselspeicher-Passwort	Das Passwort für den Schlüsselspeicher infa_keystore.jks.
Verzeichnis der Truststore-Datei	Das Verzeichnis, das die Truststore-Dateien enthält. Das Verzeichnis muss Dateien namens infa_truststore.jks und infa_truststore.pem enthalten.
Truststore-Passwort	Das Passwort für die Datei infa_truststore.jks.

3. Klicken Sie auf **Weiter**.

Die Seite **Domänen-Konfigurations-Repository** wird angezeigt.

Domänenkonfigurations-Repository

Nachdem Sie die Domänensicherheit konfiguriert haben, können Sie die Details für das Domänen-Repository konfigurieren.

1. Geben Sie auf der Seite **Domänen-Konfigurations-Repository** die entsprechenden Datenbank- und Benutzerkontodaten für das Domänen-Konfigurations-Repository ein.

Informatica 10.5.9

Domain Configuration - Step 6 of 12

Enter database information for the domain configuration repository.

Database type: Oracle

Database user ID: Satish11

Database user password: ●●●●●●●●

Database connection

☒ Enter the JDBC URL.

Database address: invkrh74rnd02.informatica.com:1521

Database service name: QA18C1.informatica.com

☐ JDBC parameters:

MaxPooledStatements=20;CatalogOptions=0;BatchPerformanceWorkaround=true

☐ Enter the JDBC connection string.

jdbc:informatica:oracle://host_name:port_no;ServiceName=

Test Connection

? < Previous Next > Cancel

Im Domänenkonfigurations-Repository werden Metadaten für Domänenvorgänge und die Benutzerauthentifizierung gespeichert. Die Datenbank muss allen Gateway-Knoten in der Domäne zugänglich sein.

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

Eigenschaft	Beschreibung
Datenbanktyp	Datenbank für das Repository. Wählen Sie eine der folgenden Datenbanken aus: <ul style="list-style-type: none"> - Oracle - IBM DB2 - Microsoft SQL Server - PostgreSQL - Sybase ASE
Datenbankbenutzer-ID	Benutzerkonto für die Repository-Datenbank.
Benutzerpasswort	Das Passwort für das Konto des Datenbankbenutzers.

Geben Sie bei Auswahl von IBM DB2 den Tablespace für die Repository-Tabellen an:

Eigenschaft	Beschreibung
Tablespace	Der Name des Tablespace, in dem die Tabellen erstellt werden sollen. Geben Sie einen Tablespace an, der die Anforderungen an die Seitengröße (pageSize) von 32768 Byte erfüllt. Wenn Sie in einer Datenbank mit einer einzigen Partition diese Option nicht auswählen, erstellt das Installationsprogramm die Tabellen im Standard-Tablespace. Wählen Sie diese Option in einer Datenbank mit mehreren Partitionen aus und geben Sie den Namen des nicht partitionierten Tablespace an, der sich in der Katalogpartition der Datenbank befindet.

Geben Sie bei Auswahl von Microsoft SQL Server oder PostgreSQL das Schema für die Repository-Tabellen und die Datenbankverbindung an:

Eigenschaft	Beschreibung
Schemaname	Name des Schemas, das die Repository-Tabellen enthält. Ist diese Option nicht aktiviert, erstellt das Installationsprogramm die Tabellen im Standardschema.
Vertrauenswürdige Verbindung	Zeigt an, ob eine vertrauenswürdige Verbindung zu Microsoft SQL Server hergestellt werden soll. Die vertrauenswürdige Authentifizierung verwendet die Sicherheitsanmeldedaten des aktuellen Benutzers zur Herstellung der Verbindung zu Microsoft SQL Server. Ist diese Option nicht aktiviert, wird die Microsoft SQL Server-Authentifizierung verwendet.

Wenn Sie sichere Kommunikation für die Domäne aktiviert haben, können Sie das Domänen-Konfigurations-Repository in einer mit dem SSL-Protokoll gesicherten Datenbank erstellen. Aktivieren Sie das Kontrollkästchen, wenn Sie eine Datenbank sichern möchten, und fahren Sie mit Schritt [3](#) fort.

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

2. Geben Sie die Verbindungsinformationen für die Datenbank ein.

Wenn Sie kein sicheres Domänenkonfigurations-Repository erstellen, können Sie die Verbindungseigenschaften für die JDBC-URL angeben oder die JDBC-Verbindungszeichenfolge bereitstellen.

- Um die Verbindungsdaten über die JDBC-URL einzugeben, wählen Sie **JDBC URL** aus, und geben Sie die Eigenschaften der Datenbankverbindung ein.
In der folgenden Tabelle werden die JDBC-URL-Eigenschaften beschrieben, die Sie festlegen:

Eigenschaft	Beschreibung
Datenbankadresse	Der Hostname und die Portnummer für die Datenbank im Format <code>host_name:port</code> .
Datenbankdienstname	Dienst- oder Datenbankname: <ul style="list-style-type: none"> - Oracle: Geben Sie den Dienstnamen ein. - Microsoft SQL Server: Geben Sie den Datenbanknamen ein. - IBM DB2: Geben Sie den Dienstnamen ein. - Sybase ASE: Geben Sie den Datenbanknamen ein. - PostgreSQL: Geben Sie den Namen der Datenbank ein.
JDBC-Parameter	Optionale Parameter, die in die Datenbankverbindungszeichenfolge aufgenommen werden können. Mit den Parametern können die Datenbankvorgänge für die Datenbank optimiert werden. Überprüfen Sie die Gültigkeit der Parameterzeichenfolge. Das Installationsprogramm führt vor dem Hinzufügen der Parameterzeichenfolge zur JDBC-URL keine Überprüfung der Zeichenfolge durch. Ist diese Option nicht aktiviert, erstellt das Installationsprogramm die JDBC-URL ohne zusätzliche Parameter.

- Um die Verbindung mithilfe einer benutzerdefinierten JDBC-Verbindungszeichenfolge herzustellen, wählen Sie **Benutzerdefinierte JDBC-Verbindungszeichenfolge** aus und geben Sie die Verbindungszeichenfolge ein.
3. Wenn Sie eine Datenbank sichern möchten, geben Sie die Verbindungsinformationen anhand einer benutzerdefinierten JDBC-Verbindungszeichenfolge ein.

Wenn Sie das Repository in einer gesicherten Datenbank erstellen, müssen Sie die Truststore-Informationen für die Datenbank angeben. Außerdem müssen Sie eine JDBC-Verbindungszeichenfolge angeben, die die Sicherheitsparameter für die Datenbank enthält.

In der folgenden Tabelle werden die Eigenschaften beschrieben, die für eine sichere Datenbank eingerichtet werden müssen:

Eigenschaft	Beschreibung
Datenbank-Truststore-Datei	Pfad und Dateiname der Truststore-Datei für die gesicherte Datenbank.
Datenbank-Truststore-Passwort	Passwort für die Truststore-Datei.
Benutzerdefinierte JDBC-Verbindungszeichenfolge	JDBC-Verbindungszeichenfolge zum Herstellen einer Verbindung mit der gesicherten Datenbank, einschließlich Hostname, Portnummer und Sicherheitsparameter für die Datenbank.

Informationen zu den Sicherheitsparametern, die in die JDBC-Verbindung für eine sichere Datenbank aufgenommen werden müssen, finden Sie unter [“Verbindungszeichenfolge für eine sichere Datenbank” auf Seite 105](#).

4. Klicken Sie auf **Verbindung testen**, um zu überprüfen, ob Sie eine Verbindung zur Datenbank herstellen können, und anschließend auf **OK**, um fortzufahren.
5. Klicken Sie auf **Weiter**.

Der Abschnitt **Domänensicherheit – Verschlüsselungsschlüssel** wird angezeigt.

Domänensicherheit – Verschlüsselungsschlüssel

Nachdem Sie das Domänen-Repository konfiguriert haben, können Sie den Verschlüsselungsschlüssel konfigurieren.

1. Geben Sie im Abschnitt **Domänensicherheit – Verschlüsselungsschlüssel** die Verschlüsselungsschlüsselparameter ein, die Sie beim Erstellen einer Domäne angeben müssen.

The screenshot shows the 'Domain Security - Encryption Key - Step 7 of 12' window in Informatica 10.5.9. The window title bar says 'Informatica 10.5.9'. The Informatica logo is in the top left, and the title 'Domain Security - Encryption Key - Step 7 of 12' is in the top right. The main content area has the heading 'Enter the encryption key information.' Below this is the 'Encryption key directory:' label, followed by a text box containing 'C:\Informatica\10.5.9_server\isplconfig\keys'. To the right of the text box are two buttons: '...' and 'Default'. Below the text box, there is a paragraph: 'A unique site key is generated. If you lose the site key, you cannot generate the site key again. Make sure that you save a copy of this key and do not share the unique site key with others. Specify if you want to backup the site key that the installer generates or not:'. Below this paragraph is a checkbox labeled 'Do you agree?' which is checked. At the bottom of the window, there is a question mark icon on the left, and three buttons: '< Previous', 'Next >', and 'Cancel'.

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

Eigenschaft	Beschreibung
Verzeichnis des Verschlüsselungsschlüssels	Verzeichnis, in dem der Verschlüsselungsschlüssel für die Domäne gespeichert werden soll. Standardmäßig wird der Verschlüsselungsschlüssel im folgenden Verzeichnis erstellt: <Informatica-Installationsverzeichnis>/isp/config/keys.
Geben Sie an, ob Sie den vom Installationsprogramm generierten Site-Schlüssel sichern möchten oder nicht:	<p>Ein eindeutiger Site-Schlüssel wird generiert. Wenn Sie den Site-Schlüssel verlieren, können Sie ihn nicht erneut generieren. Speichern Sie unbedingt eine Kopie dieses Schlüssels und teilen Sie den eindeutigen Site-Schlüssel nicht mit anderen.</p> <p>Geben Sie an, ob Sie den vom Installationsprogramm generierten Site-Schlüssel sichern möchten oder nicht:</p> <ul style="list-style-type: none"> - Wählen Sie 1 für Nein. Wenn Sie Nein wählen, wird das Installationsprogramm beendet. - Wählen Sie 2 für JA. Wenn Sie Ja wählen, stimmen Sie zu, die Datei manuell zu sichern.

Das Installationsprogramm legt verschiedene Berechtigungen für das Verzeichnis und die Dateien im Verzeichnis fest. Weitere Informationen über die Berechtigungen für die Verschlüsselungsschlüsseldatei und das Verzeichnis finden Sie unter ["Sichere Dateien und Verzeichnisse" auf Seite 110](#).

2. Klicken Sie auf **Weiter**.

Der Abschnitt **Domänen- und Knotenkonfiguration** wird angezeigt.

Domänen- und Knotenkonfiguration

Nachdem Sie den Verschlüsselungsschlüssel konfiguriert haben, können Sie die Domäne und den Knoten konfigurieren.

- 1. Geben Sie die Informationen für die Domäne und den Knoten ein, die Sie erstellen möchten.

Informatica 10.5.9

Informatica

Domain and Node Configuration - Step 8 of 12

Enter information for the Informatica domain.

Domain name:

Domain

Node host name:

lninstwin201901.informatica.com

Node name:

node01

Node port number:

7560

Domain user name:

Administrator

☐ Do you want to enable password complexity?

Domain password:

••••••••

Confirm password:

••••••••

☒ Do you want to display the advanced port configuration page?

☒ Do you want to create the Model Repository Service and Data Integration Service?

☒ Do you want to create a monitoring Model Repository Service to monitor domain statistics?

☒ Do you want to create Content Management Service for data domain discovery?

☒ Do you want to configure the profiling warehouse connection?

☒ Do you want to create a PowerCenter Repository Service and a PowerCenter Integration Service?

?

< Previous

Next >

Cancel

In der folgenden Tabelle sind die Eigenschaften beschrieben, die Sie für die Domäne und den Gateway-Knoten festlegen:

Eigenschaft	Beschreibung
Domänenname	Name der zu erstellenden Informatica-Domäne. Der Standardname der Domäne lautet Domain_<MachineName>. Der Name darf maximal 128 Zeichen umfassen und muss im 7-Bit-ASCII-Format vorliegen. Der Name darf weder Leerzeichen noch eines der folgenden Zeichen enthalten: ` % * + ; " ? , < > \ /
Knotenname	Name des zu erstellenden Knotens.

Eigenschaft	Beschreibung
Hostname des Knotens	<p>Hostname oder IP-Adresse des Computers, auf dem der Knoten erstellt werden soll.</p> <p>Wenn der Computer nur einen Netzwerknamen aufweist, verwenden Sie den Standardhostname. Wenn der Computer mehrere Netzwerknamen aufweist, können Sie den Standardhostnamen ändern und einen alternativen Netzwerknamen verwenden.</p> <p>Hinweis: Der Hostname des Knotens darf keine Unterstriche (_) enthalten. Verwenden Sie nicht localhost. Der Hostname muss den Computer eindeutig kennzeichnen.</p>
Portnummer des Knotens	Die Portnummer für den Knoten. Die Standardportnummer für den Knoten lautet 6005. Wenn die Portnummer auf dem Rechner nicht verfügbar ist, zeigt das Installationsprogramm die nächste verfügbare Portnummer an.
Domänenbenutzername	<p>Benutzername für den Domänenadministrator. Sie können diesen Benutzernamen für die 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 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.

In der folgenden Tabelle wird die Passwortkomplexität beschrieben:

Eingabeaufforderung	Beschreibung
Passwortkomplexität	<p>Wählen Sie aus, ob die Passwortkomplexität aktiviert werden soll.</p> <p>Wenn Sie „Ja“ auswählen, muss das Passwort die folgenden Anforderungen erfüllen: Es muss mindestens acht Zeichen lang sein und mindestens ein alphabetisches Zeichen, ein numerisches Zeichen und ein Sonderzeichen enthalten.</p>
Passwortrichtlinie konfigurieren	<p>Wählen Sie aus, ob eine Passwortrichtlinie konfiguriert werden soll.</p> <p>Wenn Sie „Ja“ auswählen, können Sie Passwortkomplexitätsregeln konfigurieren.</p> <p>Wenn Sie „Nein“ auswählen, gelten die Standardregeln der Informatica-Passwortrichtlinie.</p>
Anzahl der Sonderzeichen	<p>Die Mindestanzahl der erforderlichen Sonderzeichen in einem Passwort.</p> <p>Sie können die folgenden Sonderzeichen verwenden: " # \$ % & ' () * + , - . / : ; < = > ? @ [] ^ _ ` { } ~]</p> <p>Sie können einen Wert zwischen 0 und 128 eingeben. Standardwert ist 1.</p>
Anzahl der alphabetischen Zeichen	<p>Die Mindestanzahl der erforderlichen alphabetischen Zeichen in einem Passwort.</p> <p>Sie können einen Wert zwischen 0 und 128 eingeben. Standardwert ist 1.</p>
Anzahl der numerischen Zeichen	<p>Die Mindestanzahl der erforderlichen numerischen Zeichen in einem Passwort.</p> <p>Sie können einen Wert zwischen 0 und 128 eingeben. Standardwert ist 1.</p>
Minimale Passwortlänge	<p>Die Mindestanzahl der erforderlichen Zeichen in einem Passwort.</p> <p>Sie können einen Wert zwischen 1 und 128 eingeben. Standardwert ist 8.</p>

Eingabeaufforderung	Beschreibung
Anzahl der zu speichernden vorherigen Passwörter	Die Anzahl der aufeinanderfolgenden vorherigen Passwörter, die nicht wiederverwendet werden können. Sie können einen Wert zwischen 0 und 12 eingeben. Standardwert ist 0.
Passwortablauf in Tagen	Die Gültigkeitsdauer eines Passworts. Wenn Passwörter nicht ablaufen sollen, legen Sie den Wert 0 fest. Standardwert ist 0.
Domänenpasswort	Das Passwort für den Domänenadministrator. <ul style="list-style-type: none"> - Wenn Sie die Passwortkomplexität nicht aktivieren, muss das Passwort zwischen 2 und 16 Zeichen lang sein. - Wenn Sie die Passwortkomplexität aktivieren, muss das Passwort mindestens acht Zeichen umfassen und mindestens ein alphabetisches Zeichen, ein numerisches Zeichen und ein Sonderzeichen enthalten. - Wenn Sie eine Passwortrichtlinie konfigurieren, muss das Passwort die von Ihnen festgelegten Komplexitätsregeln erfüllen. Nicht verfügbar, wenn Sie die Informatica-Domäne zur Ausführung in einem Netzwerk mit Kerberos-Authentifizierung konfigurieren.
Passwort bestätigen	Geben Sie das Passwort zur Bestätigung erneut ein. Nicht verfügbar, wenn Sie die Informatica-Domäne zur Ausführung in einem Netzwerk mit Kerberos-Authentifizierung konfigurieren.

2. Aktivieren Sie zur Anzeige der vom Installationsprogramm zugewiesenen Standardports für die Domänen- und Knotenkomponenten die Option **Seite für erweiterte Portkonfiguration anzeigen**.

Wenn Sie die Seite für die Portkonfiguration öffnen, werden vom Installationsprogramm die der Domäne und dem Knoten zugewiesenen Standardportnummern angezeigt. Sie können die Portnummern ändern und einen anderen Portnummernbereich für die Anwendungsdienstprozesse angeben. Wenn Sie die Seite für die Portkonfiguration nicht öffnen, zeigt das Installationsprogramm die Standardportnummern nicht an und die zugewiesenen Portnummern können nicht geändert werden.

3. Aktivieren Sie das Kontrollkästchen, um während der Installation den Modellrepository-Dienst und den Datenintegrationsdienst zu erstellen.

Wenn Sie die Dienste nicht konfigurieren, erstellt das Installationsprogramm weder einen Modellrepository- noch einen Datenintegrationsdienst in der neuen Domäne. Sie können die Dienste im Administrator Tool nach der Installation erstellen.

Wenn Sie die Dienste konfigurieren, erstellt das Installationsprogramm einen Modellrepository- und einen Datenintegrationsdienst in der neuen Domäne. Sie müssen die Datenbank für das Modellrepository angeben und die Verbindung zum Datenintegrationsdienst konfigurieren. Standardmäßig startet das Installationsprogramm die Dienste nach Abschluss der Installation.

4. Wählen Sie, ob Sie einen Überwachungsmodellrepository-Dienst zum Überwachen der Domänenstatistiken erstellen möchten.
5. Wählen Sie, ob Sie während der Installation einen Content-Management-Dienst für Datendomänenerkennung erstellen möchten.
6. Wählen Sie, ob Sie während der Installation die Verbindung des Profiling-Warehouse konfigurieren möchten.
7. Wählen Sie, ob während der Installation ein PowerCenter-Repository-Dienst und ein PowerCenter-Integrationsdienst erstellt werden sollen.

Wenn Sie angegeben haben, dass die Seite für die Port-Konfiguration angezeigt werden soll, wird die Seite **Port-Konfiguration** geöffnet.

Wenn Sie nicht angegeben haben, dass die Seite für die Port-Konfiguration angezeigt werden soll, zeigt das Installationsprogramm die Seite **Windows-Dienstkonfiguration** an.

Port-Konfiguration

Sie können die Portnummern für Dienstmanager und Informatica Administrator aktualisieren.

1. Wenn Sie angegeben haben, dass die Seite für die Port-Konfiguration angezeigt werden soll, wird die Seite **Port-Konfiguration** geöffnet.

Informatica 10.5.9

Port Configuration - Step 8A of 12

Enter the port numbers for the Service Manager and Informatica Administrator.

Service Manager port:	7561
Service Manager shutdown port:	7562
Informatica Administrator port:	7563
Informatica Administrator shutdown port:	7564

Enter a range of port numbers for service processes in the node.

Minimum port number:	7569
Maximum port number:	7669

Default

< Previous Next > Cancel

2. Geben Sie auf der Seite **Portkonfiguration** die Portnummern für den Dienstmanager der Domäne und die Dienstprozesse ein, die auf dem Knoten ausgeführt werden.

Stellen Sie sicher, dass die von Ihnen eingegebenen Portnummern nicht von anderen Anwendungen verwendet werden.

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

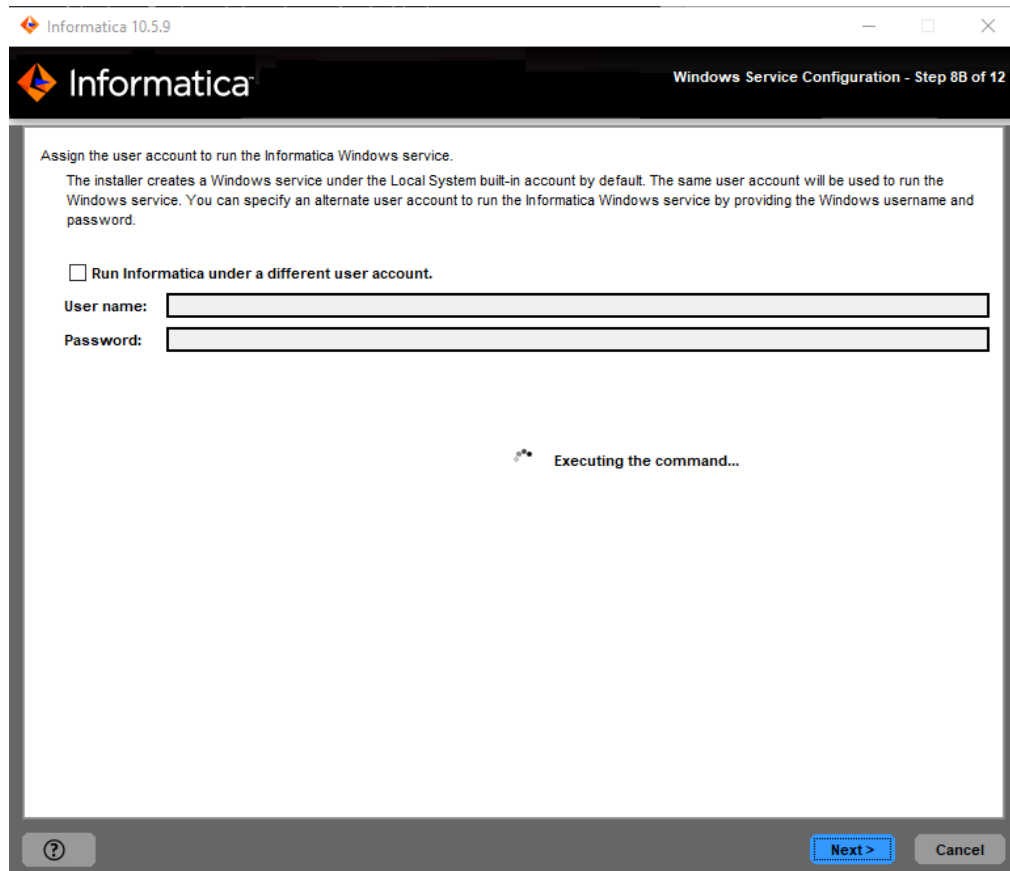
Port	Beschreibung
Dienstmanager-Port	Die vom Dienstmanager auf dem Knoten verwendete Portnummer. Der Dienstmanager überwacht eingehende Verbindungsanfragen an diesem Port. Clientanwendungen verwenden diesen Port zur Kommunikation mit den Diensten in dieser Domäne. Die Informatica-Befehlszeilenprogramme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

- Klicken Sie auf **Weiter**.

Die Seite **Windows-Dienstkonfiguration** wird angezeigt.

Windows-Dienstkonfiguration

1. Wenn Sie nicht angegeben haben, dass die Seite für die Port-Konfiguration angezeigt werden soll, zeigt das Installationsprogramm die Seite **Windows-Dienstkonfiguration** an.



2. Geben Sie auf der Seite **Windows-Dienstkonfiguration** an, ob der Windows-Dienst unter einem anderen Benutzerkonto ausgeführt werden soll.

Das Installationsprogramm erstellt einen Dienst zum Starten von Informatica. Der Dienst wird standardmäßig unter demselben Benutzerkonto ausgeführt wie dem, das für die Installation verwendet wurde. Sie können den Windows-Dienst unter einem anderen Benutzerkonto ausführen.

In der folgenden Tabelle werden die Eigenschaften beschrieben, die zum Ausführen von Informatica unter einem anderen Benutzerkonto eingerichtet werden:

Eigenschaft	Beschreibung
Informatica unter einem anderen Benutzerkonto ausführen	Zeigt die Option an, den Windows-Dienst unter einem anderen Benutzerkonto auszuführen.
Benutzername	Das Benutzerkonto, unter dem der Informatica-Windows-Dienst ausgeführt werden soll. Verwenden Sie das folgende Format: <Domänenname>\<Benutzerkonto> Dieses Benutzerkonto muss „Aktion“ als Betriebssystemberechtigung haben.
Passwort	Das Passwort zum Benutzerkonto, unter dem der Informatica-Windows-Dienst ausgeführt werden soll.

- Klicken Sie auf **Weiter**.

Wenn Sie die Dienste nicht erstellen möchten, wird im Installationsprogramm die Seite **Installationsabschlussbericht** angezeigt. Auf der Seite **Nach der Installation – Zusammenfassung** wird angezeigt, ob die Installation erfolgreich abgeschlossen wurde.

Wenn Sie die Informatica-Anwendungsdienste konfiguriert haben, wird im Installationsprogramm die Seite **Datenbank des Modellrepository-Diensts** angezeigt.

Konfigurieren der Datenbank des Modellrepository-Diensts

Nachdem Sie die Domäne und den Knoten konfiguriert haben, können Sie die Eigenschaften der Modellrepository-Datenbank konfigurieren.

- Geben Sie auf der Seite **Datenbank des Modellrepository-Diensts** die Datenbank- und Benutzerkontoinformationen für das Modellrepository ein.

Informatica 10.5.9

Informatica Model Repository Database - Step 9A of 12

Model Repository Service name:

Enter database information for the Model repository:

Database type:

Database user ID:

Database user password:

☐ Is the database secure?

Database connection

☒ Enter the JDBC URL.

Database address:

Database service name:

☐ JDBC parameters:

☐ Enter the JDBC connection string.

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

Eigenschaft	Beschreibung
Datenbanktyp	Datenbank für das Repository. Wählen Sie eine der folgenden Datenbanken aus: <ul style="list-style-type: none"> - Oracle - IBM DB2 - Microsoft SQL Server - PostgreSQL
Datenbankbenutzer-ID	Benutzerkonto für die Repository-Datenbank.
Benutzerpasswort	Das Passwort für das Konto des Datenbankbenutzers.

Geben Sie bei Auswahl von IBM DB2 den Tablespace für die Repository-Tabellen an:

Eigenschaft	Beschreibung
Tablespace	<p>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.</p> <p>Wenn Sie in einer Datenbank mit einer einzigen Partition diese Option nicht auswählen, erstellt das Installationsprogramm die Tabellen im Standard-Tablespace.</p> <p>Wählen Sie diese Option in einer Datenbank mit mehreren Partitionen aus und geben Sie den Namen des nicht partitionierten Tablespace an, der sich in der Katalogpartition der Datenbank befindet.</p>

Geben Sie bei Auswahl von Microsoft SQL Server oder PostgreSQL das Schema für die Repository-Tabellen und die Datenbankverbindung an:

Eigenschaft	Beschreibung
Schemaname	Name des Schemas, das die Repository-Tabellen enthält. Ist diese Option nicht aktiviert, erstellt das Installationsprogramm die Tabellen im Standardschema.
Vertrauenswürdige Verbindung	Zeigt an, ob eine vertrauenswürdige Verbindung zu Microsoft SQL Server hergestellt werden soll. Die vertrauenswürdige Authentifizierung verwendet die Sicherheitsanmeldedaten des aktuellen Benutzers zur Herstellung der Verbindung zu Microsoft SQL Server. Ist diese Option nicht aktiviert, wird die Microsoft SQL Server-Authentifizierung verwendet.

Wenn Sie sichere Kommunikation für die Domäne aktivieren, können Sie das Modellrepository in einer mit dem SSL-Protokoll gesicherten Datenbank erstellen. Zum Erstellen eines sicheren Modellrepositorys fahren Sie mit Schritt [3](#) fort.

2. Geben Sie die Verbindungsinformationen für die Datenbank ein.

Wenn Sie kein sicheres Modellrepository erstellen, können Sie die Verbindungseigenschaften für die JDBC-URL angeben oder die JDBC-Verbindungszeichenfolge bereitstellen.

- Um die Verbindungsdaten mithilfe der JDBC-URL einzugeben, wählen Sie **JDBC-URL** aus und geben Sie die Eigenschaften der Datenbankverbindung ein.

In der folgenden Tabelle werden die JDBC-URL-Eigenschaften beschrieben, die Sie festlegen:

Eigenschaft	Beschreibung
Datenbankadresse	Der Hostname und die Portnummer für die Datenbank im Format <code>host_name:port</code> .
Datenbankdienstname	Dienst- oder Datenbankname: <ul style="list-style-type: none">- Oracle: Geben Sie den Dienstnamen ein.- Microsoft SQL Server: Geben Sie den Datenbanknamen ein.- IBM DB2: Geben Sie den Dienstnamen ein.- PostgreSQL: Geben Sie den Namen der Datenbank ein.
JDBC-Parameter	Optionale Parameter, die in die Datenbankverbindungszeichenfolge aufgenommen werden können. Mit den Parametern können die Datenbankvorgänge für die Datenbank optimiert werden. Überprüfen Sie die Gültigkeit der Parameterzeichenfolge. Das Installationsprogramm führt vor dem Hinzufügen der Parameterzeichenfolge zur JDBC-URL keine Überprüfung der Zeichenfolge durch. Ist diese Option nicht aktiviert, erstellt das Installationsprogramm die JDBC-URL ohne zusätzliche Parameter.

- Um die Verbindungsdaten mithilfe einer benutzerdefinierten JDBC-Verbindungszeichenfolge einzugeben, wählen Sie **Benutzerdefinierte JDBC-Verbindungszeichenfolge** aus und geben Sie die Verbindungszeichenfolge ein.

IBM DB2

```
jdbc:Informatica:db2://<Hostname>:<Portnummer>;DatabaseName=
```

Oracle

```
jdbc:Informatica:oracle://<Hostname>:<Portnummer>;ServiceName=
```

Verwenden Sie die folgende Verbindungszeichenfolge, um eine Verbindung zur Oracle-Datenbank über den Oracle Connection Manager herzustellen:

```
jdbc:Informatica:oracle:TNSNamesFile=<vollqualifizierter Pfad zur Datei  
tnsnames.ora>;TNSServerName=<TNS-Name>;
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://  
<Hostname>:<Portnummer>;SelectMethod=cursor;DatabaseName=
```

Microsoft Azure SQL

```
jdbc:Informatica:sqlserver://  
<hostname>:<portnummer>;SelectMethod=cursor;DatabaseName=<datenbankname>;SnapshotS  
erializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net  
;ValidateServerCertificate=false
```

Azure SQL-Datenbank mit Active Directory-Authentifizierung

```
"jdbc:informatica: sqlserver://  
<host_name>:<port_number>;database=<database_name>;encrypt=true;AuthenticationMeth  
od=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertificate=*.da  
tabase.windows.net;loginTimeout=<seconds>"
```

PostgreSQL

```
jdbc:Informatica:postgresql://<hostname>:<portnummer>;DatabaseName=
```

Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database  
name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TL  
Sv1.2;
```

Stellen Sie sicher, dass die Verbindungszeichenfolge alle vom Datenbanksystem benötigten Verbindungsparameter enthält.

3. Wählen Sie, ob ein sicheres Modellrepository erstellt werden soll.

Wenn Sie das Repository in einer gesicherten Datenbank erstellen, müssen Sie die Truststore-Informationen für die Datenbank angeben. Außerdem müssen Sie eine JDBC-Verbindungszeichenfolge angeben, die die Sicherheitsparameter für die Datenbank enthält.

In der folgenden Tabelle werden die Eigenschaften beschrieben, die für eine sichere Datenbank eingerichtet werden müssen:

Eigenschaft	Beschreibung
Datenbank-Truststore-Datei	Pfad und Dateiname der Truststore-Datei für die gesicherte Datenbank.
Datenbank-Truststore-Passwort	Passwort für die Truststore-Datei.
Benutzerdefinierte JDBC-Verbindungszeichenfolge	JDBC-Verbindungszeichenfolge zum Herstellen einer Verbindung mit der gesicherten Datenbank, einschließlich Hostname, Portnummer und Sicherheitsparameter für die Datenbank.

Informationen zu den Sicherheitsparametern, die in die JDBC-Verbindung für eine sichere Datenbank aufgenommen werden müssen, finden Sie unter [“Verbindungszeichenfolge für eine sichere Datenbank” auf Seite 105](#).

4. Klicken Sie auf **Verbindung testen**, um zu überprüfen, ob Sie eine Verbindung zur Datenbank herstellen können, und anschließend auf **OK**, um fortzufahren.
5. Klicken Sie auf **Weiter**.

Der Abschnitt **Serviceparameter** wird angezeigt.

Konfigurieren der Datenbank des Überwachungsmodellrepository-Diensts

Nachdem Sie die Modellrepository-Datenbank konfiguriert haben, können Sie die Eigenschaften der Überwachungsmodellrepository-Datenbank konfigurieren.

1. Wenn Sie die Erstellung eines Überwachungsmodellrepository-Dienst zum Überwachen der Domänenstatistik ausgewählt haben, wird die Seite **Modellrepository-Datenbank für Überwachung** geöffnet.

Informatica 10.5.9

Informatica Model Repository Database - Step 9A of 12

Model Repository Service name:

Enter database information for the Model repository:

Database type:

Database user ID:

Database user password:

☐ Is the database secure?

Database connection

☒ Enter the JDBC URL.

Database address:

Database service name:

☐ JDBC parameters:

☐ Enter the JDBC connection string.

2. Geben Sie auf der Seite **Modellrepository-Datenbank für Überwachung** die Datenbank- und Benutzerkontoinformationen für das Überwachungsmodellrepository ein.

Eigenschaft	Beschreibung
Datenbanktyp	Datenbank für das Repository. Wählen Sie eine der folgenden Datenbanken aus: <ul style="list-style-type: none"> - Oracle - IBM DB2 - Microsoft SQL Server - PostgreSQL
Datenbankbenutzer-ID	Benutzerkonto für die Repository-Datenbank. Sie können den Windows NT-Benutzernamen für eine vertrauenswürdige Verbindung für Microsoft SQL Server eingeben.
Benutzerpasswort	Das Passwort für das Datenbankbenutzerkonto. Sie können das Windows NT-Passwort für eine vertrauenswürdige Verbindung für Microsoft SQL Server eingeben.

Geben Sie bei Auswahl von IBM DB2 den Tablespace für die Repository-Tabellen an:

Eigenschaft	Beschreibung
Tablespace	Der Name des Tablespace, in dem die Tabellen erstellt werden sollen. Geben Sie einen Tablespace an, der die Anforderungen an die Seitengröße (pageSize) von 32768 Byte erfüllt. Wenn Sie in einer Datenbank mit einer einzigen Partition diese Option nicht auswählen, erstellt das Installationsprogramm die Tabellen im Standard-Tablespace. Wählen Sie diese Option in einer Datenbank mit mehreren Partitionen aus und geben Sie den Namen des nicht partitionierten Tablespace an, der sich in der Katalogpartition der Datenbank befindet.

Geben Sie bei Auswahl von Microsoft SQL Server oder PostgreSQL das Schema für die Repository-Tabellen und die Datenbankverbindung an:

Eigenschaft	Beschreibung
Schemaname	Name des Schemas, das die Repository-Tabellen enthält. Ist diese Option nicht aktiviert, erstellt das Installationsprogramm die Tabellen im Standardschema.
Vertrauenswürdige Verbindung	Zeigt an, ob eine vertrauenswürdige Verbindung zu Microsoft SQL Server hergestellt werden soll. Die vertrauenswürdige Authentifizierung verwendet die Sicherheitsanmeldedaten des aktuellen Benutzers zur Herstellung der Verbindung zu Microsoft SQL Server. Ist diese Option nicht aktiviert, wird die Microsoft SQL Server-Authentifizierung verwendet.

3. Geben Sie die Verbindungsinformationen für die Datenbank ein.

Sie können die Verbindungseigenschaften für die JDBC-URL angeben oder die JDBC-Verbindungszeichenfolge bereitstellen.

- Um die Verbindungsdaten mithilfe der JDBC-URL einzugeben, wählen Sie **JDBC-URL** aus und geben Sie die Eigenschaften der Datenbankverbindung ein.
In der folgenden Tabelle werden die JDBC-URL-Eigenschaften beschrieben, die Sie festlegen:

Eigenschaft	Beschreibung
Datenbankadresse	Hostname und Portnummer für die Datenbank im Format <host name>:<port number>.
Datenbankdienstname	Dienst- oder Datenbankname: <ul style="list-style-type: none">- Oracle: Geben Sie den Dienstnamen ein.- Microsoft SQL Server: Geben Sie den Datenbanknamen ein.- IBM DB2: Geben Sie den Dienstnamen ein.- PostgreSQL: Geben Sie den Namen der Datenbank ein.
JDBC-Parameter	Optionale Parameter, die in die Datenbankverbindungszeichenfolge aufgenommen werden können. Mit den Parametern können die Datenbankvorgänge für die Datenbank optimiert werden. Überprüfen Sie die Gültigkeit der Parameterzeichenfolge. Das Installationsprogramm führt vor dem Hinzufügen der Parameterzeichenfolge zur JDBC-URL keine Überprüfung der Zeichenfolge durch. Ist diese Option nicht aktiviert, erstellt das Installationsprogramm die JDBC-URL ohne zusätzliche Parameter.

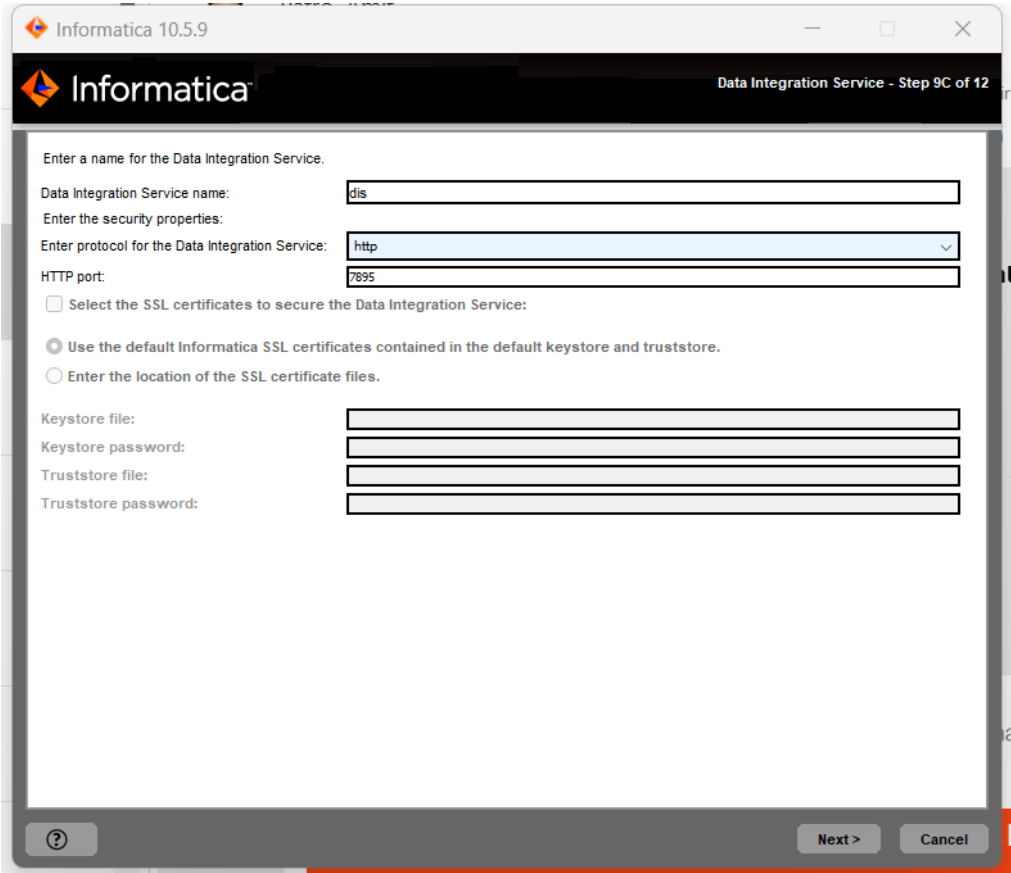
- Um die Verbindungsinformationen mithilfe einer benutzerdefinierten JDBC-Verbindungszeichenfolge einzugeben, wählen Sie **Benutzerdefinierte JDBC-Verbindungszeichenfolge** aus und geben Sie die Verbindungszeichenfolge ein.
4. Klicken Sie auf **Verbindung testen**, um zu überprüfen, ob Sie eine Verbindung zur Datenbank herstellen können, und anschließend auf **OK**, um fortzufahren.
 5. Klicken Sie auf **Weiter**.

Der Abschnitt **Serviceparameter** wird angezeigt.

Datenintegrationsdienst

Nachdem Sie die Modellrepository-Datenbank konfiguriert haben, können Sie die Dienstparameter für die Anwendungsdienste konfigurieren.

- 1. Konfigurieren Sie auf der Seite **Datenintegrationsdienst** die Eigenschaften des Datenintegrationsdiensts.



In der folgenden Tabelle werden die einzurichtenden Dienstparameter beschrieben:

Port	Beschreibung
Name des Datenintegrationsdiensts	Der Name des Datenintegrationsdiensts, der in der Informatica-Domäne erstellt werden soll.
HTTP-Protokolltyp	Der Typ der Verbindung zum Datenintegrationsdienst. Wählen Sie eine der folgenden Optionen aus: <ul style="list-style-type: none">- HTTP. Für Anfragen an den Dienst wird eine HTTP-Verbindung verwendet.- HTTPS. Für Anfragen an den Dienst wird eine sichere HTTP-Verbindung verwendet.- HTTP&HTTPS. Für Anfragen an den Dienst kann eine HTTP- oder HTTPS-Verbindung verwendet werden.
HTTP-Port	Die Portnummer für den Datenintegrationsdienst. Der Standardwert ist 6030.

2. Geben Sie bei Auswahl einer HTTPS-Verbindung an, ob die SSL-Standardzertifikate von Informatica oder Ihre SSL-Zertifikate verwendet werden sollen, um eine sichere Verbindung zum Datenintegrationsdienst herzustellen.

In der folgenden Tabelle werden die SSL-Zertifikatsoptionen zum Sichern des Datenintegrationsdiensts beschrieben:

Option	Beschreibung
SSL-Standardzertifikatsdateien von Informatica verwenden	Verwenden Sie die von Informatica bereitgestellten SSL-Standardzertifikate. Hinweis: Wenn Sie kein SSL-Zertifikat bereitstellen, verwendet Informatica denselben privaten Standardschlüssel für alle Informatica-Installationen. Wenn Sie die standardmäßigen Schlüsselspeicherdateien und Truststore-Dateien von Informatica verwenden, ist die Sicherheit Ihrer Domäne unter Umständen gefährdet. Um ein hohes Maß an Sicherheit für die Domäne zu gewährleisten, wählen Sie die Option zum Angeben des Speicherorts der SSL-Zertifikatsdateien aus.
Speicherort der SSL-Zertifikatsdateien eingeben	Geben Sie den Pfad zur Schlüsselspeicher- und zur Truststore-Datei ein, die die SSL-Zertifikate enthalten.

Wenn Sie das Zertifikat bereitstellen, geben Sie den Speicherort und die Passwörter der Schlüsselspeicher- und der Truststore-Dateien an.

In der folgenden Tabelle werden die Parameter beschrieben, die für die SSL-Zertifikatsdateien eingegeben werden müssen:

Eigenschaft	Beschreibung
Schlüsselspeicherdatei	Obligatorisch. Pfad und Dateiname der Schlüsselspeicherdatei, die die privaten Schlüssel und SSL-Zertifikate für die Datenbank enthält.
Schlüsselspeicher-Passwort	Obligatorisch. Passwort der Schlüsselspeicherdatei für die gesicherte Datenbank.
Truststore-Datei	Obligatorisch. Pfad und Dateiname der Truststore-Datei, die den öffentlichen Schlüssel für die Datenbank enthält.
Truststore-Passwort	Obligatorisch. Passwort der Truststore-Datei für die gesicherte Datenbank.

3. Klicken Sie auf **Weiter**.

Das Installationsprogramm erstellt den Datenintegrationsdienst.

Parameter und Datenbank des Content-Management-Diensts

Nach der Konfiguration des Datenintegrationsdiensts können Sie die Parameter für den Content-Management-Dienst konfigurieren.

- 1. Wenn Sie während der Installation die Erstellung eines Content-Management-Diensts ausgewählt haben, wird die Seite **Content-Management-Dienst** geöffnet.

Informatica 10.5.9

Content Management Service - Step 90 of 12

Enter a name for the Content Management Service.

Content Management Service name:

Enter the security properties:

Select the protocol for the Content Management Service:

HTTP port:

☐ Select a keystore for the Content Management Service.

☒ Use the default Informatica SSL certificates contained in the default keystore and truststore.

☐ Use custom SSL certificates. Specify the path, file name, and password for the keystore file that contain SSL certificates.

Keystore file:

Keystore password:

? Next > Cancel

- 2. Geben Sie die Parameter des Content-Management-Diensts ein.

In der folgenden Tabelle werden die einzurichtenden Dienstparameter beschrieben:

Port	Beschreibung
Name des Content-Management-Diensts	Name des Content-Management-Diensts, der in der Informatica-Domäne erstellt werden soll.
HTTP-Protokoll	Typ der Verbindung des Content-Management-Diensts. Wählen Sie eine der folgenden Optionen aus: <ul style="list-style-type: none">- HTTP. Erfordert, dass der Dienst eine HTTP-Verbindung benutzt.- HTTPS. Erfordert, dass der Dienst eine sichere HTTP-Verbindung benutzt.
HTTP-Port	Portnummer für den Content-Management-Dienst. Standardwert ist 8105.

- 3. Geben Sie bei Auswahl einer HTTPS-Verbindung an, ob die SSL-Standardzertifikate von Informatica oder Ihre SSL-Zertifikate verwendet werden sollen, um eine sichere Verbindung zum Content-Management-Dienst herzustellen.

In der folgenden Tabelle werden die SSL-Zertifikatsoptionen zum Sichern des Content-Management-Diensts beschrieben:

Option	Beschreibung
SSL-Standardzertifikatsdateien von Informatica verwenden	Verwenden Sie die von Informatica bereitgestellten SSL-Standardzertifikate. Hinweis: Wenn Sie kein SSL-Zertifikat bereitstellen, verwendet Informatica denselben privaten Standardschlüssel für alle Informatica-Installationen. Wenn Sie die von Informatica bereitgestellten standardmäßigen Schlüsselspeicherdateien verwenden, wird die Sicherheit Ihrer Domäne unter Umständen gefährdet. Um ein hohes Maß an Sicherheit für die Domäne zu gewährleisten, wählen Sie die Option zum Angeben des Speicherorts der SSL-Zertifikatsdateien aus.
Speicherort der SSL-Zertifikatsdateien eingeben	Verwenden Sie von Ihnen bereitgestellte SSL-Zertifikate. Sie müssen den Speicherort der Schlüsselspeicherdateien angeben.

Wenn Sie das Zertifikat bereitstellen, geben Sie den Speicherort und die Passwörter der Schlüsselspeicherdateien an.

In der folgenden Tabelle werden die Parameter beschrieben, die für die SSL-Zertifikatsdateien eingegeben werden müssen:

Eigenschaft	Beschreibung
Schlüsselspeicherdatei	Erforderlich. Pfad und Dateiname für die Schlüsselspeicherdatei, die die privaten Schlüssel und SSL-Zertifikate für die Datenbank enthält.
Schlüsselspeicherpasswort	Erforderlich. Passwort der Schlüsselspeicherdatei für die sichere Datenbank.

Die Schlüsselspeicherzertifikatstypen für den Content-Management-Dienst richten sich nach den Zertifikatstypen, die vom Administrator Tool verwendet werden:

- Bei Verwendung des standardmäßigen Schlüsselspeicherzertifikats für das Administrator Tool können Sie entweder das standardmäßige oder ein benutzerdefiniertes Schlüsselspeicherzertifikat für den Content-Management-Dienst verwenden.
- Bei Verwendung eines benutzerdefinierten Schlüsselspeicherzertifikats für das Administrator Tool müssen Sie ein benutzerdefiniertes Schlüsselspeicherzertifikat für den Content-Management-Dienst verwenden.

4. Klicken Sie auf **Weiter**.

Informatica 10.5.9

Informatica Content Management Service - Step 90 of 12

Enter reference data warehouse database information for the Content Management Service:

Database type: Oracle

Database user ID: Satish15

Database user password: ●●●●●●●●

Data access connection string: QA18C1.informatica.com

Configure the database connection:

☒ Enter the JDBC URL.

Database address: invb74rmd02.informatica.com:1521

Database service name: QA18C1.informatica.com

☐ JDBC parameters:

MaxPooledStatements=20;CatalogOptions=0;BatchPerformanceWorkaround=true

☐ Enter the JDBC connection string.

jdbc:informatica:oracle://host_name:port_no;ServiceName=

Test Connection

< Previous Next > Cancel

5. Geben Sie auf der Seite **Content-Management-Dienst** die Datenbank- und Benutzerkontoinformationen für die Datenbank des Referenz-Data-Warehouse ein.

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

Eigenschaft	Beschreibung
Datenbanktyp	Die Datenbank für das Referenz-Data-Warehouse. Wählen Sie eine der folgenden Datenbanken aus. <ul style="list-style-type: none"> - Oracle - IBM DB2 - Microsoft SQL Server - Microsoft Azure SQL-Datenbank - PostgreSQL mit JDBC
Datenbankbenutzer-ID	Benutzerkonto für die Datenbank des Referenz-Data-Warehouse.
Benutzerpasswort	Das Passwort für das Datenbankbenutzerkonto.

Geben Sie bei Auswahl von IBM DB2 den Tablespace für die Repository-Tabellen an:

Eigenschaft	Beschreibung
Tablespace	<p>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.</p> <p>Wenn Sie in einer Datenbank mit einer einzigen Partition diese Option nicht auswählen, erstellt das Installationsprogramm die Tabellen im Standard-Tablespace.</p> <p>Wählen Sie diese Option in einer Datenbank mit mehreren Partitionen aus und geben Sie den Namen des nicht partitionierten Tablespace an, der sich in der Katalogpartition der Datenbank befindet.</p>

Geben Sie bei Auswahl von Microsoft SQL Server oder PostgreSQL das Schema für die Repository-Tabellen und die Datenbankverbindung an:

Eigenschaft	Beschreibung
Schemaname	Name des Schemas, das die Repository-Tabellen enthält. Ist diese Option nicht aktiviert, erstellt das Installationsprogramm die Tabellen im Standardschema.
Vertrauenswürdige Verbindung	Zeigt an, ob eine vertrauenswürdige Verbindung zu Microsoft SQL Server hergestellt werden soll. Die vertrauenswürdige Authentifizierung verwendet die Sicherheitsanmeldedaten des aktuellen Benutzers zur Herstellung der Verbindung zu Microsoft SQL Server. Ist diese Option nicht aktiviert, wird die Microsoft SQL Server-Authentifizierung verwendet.

6. Geben Sie die Verbindungsinformationen für die Datenbank ein.

Sie können die Verbindungseigenschaften für die JDBC-URL angeben oder die JDBC-Verbindungszeichenfolge bereitstellen.

- Um die Verbindungsdaten mithilfe der JDBC-URL einzugeben, wählen Sie **JDBC-URL** aus und geben Sie die Eigenschaften der Datenbankverbindung ein.

Eigenschaft	Beschreibung
Datenbankadresse	Hostname und Portnummer für die Datenbank im Format <host name>:<port number>.
Datenbankdienstname	<p>Dienst- oder Datenbankname:</p> <ul style="list-style-type: none"> - Oracle: Geben Sie den Dienstnamen ein. - Microsoft SQL Server: Geben Sie den Datenbanknamen ein. - IBM DB2: Geben Sie den Dienstnamen ein.
JDBC-Parameter	Optionale Parameter, die in die Datenbankverbindungszeichenfolge aufgenommen werden können. Mit den Parametern können die Datenbankvorgänge für die Datenbank optimiert werden. Überprüfen Sie die Gültigkeit der Parameterzeichenfolge. Das Installationsprogramm führt vor dem Hinzufügen der Parameterzeichenfolge zur JDBC-URL keine Überprüfung der Zeichenfolge durch. Ist diese Option nicht aktiviert, erstellt das Installationsprogramm die JDBC-URL ohne zusätzliche Parameter.

- Um die Verbindungsinformationen mithilfe einer benutzerdefinierten JDBC-Verbindungszeichenfolge einzugeben, wählen Sie **Benutzerdefinierte JDBC-Verbindungszeichenfolge** aus und geben Sie die Verbindungszeichenfolge ein.
7. Klicken Sie auf **Verbindung testen**, um zu überprüfen, ob Sie eine Verbindung zur Datenbank herstellen können, und anschließend auf **OK**, um fortzufahren.
 8. Klicken Sie auf **Weiter**.

Profiling Warehouse Connection Database

After you configure the Content Management Service, you can configure the data profiling warehouse database.

1. Select the database type for the data profiling warehouse.

The following table lists the databases for the data profiling warehouse.

Prompt	Description
Database type	Type of database for the data profiling warehouse. Select from the following options: <ul style="list-style-type: none"> - Oracle - Microsoft SQL Server - IBM DB2 - PostgreSQL

2. Enter the properties for the database user account.

The following table lists the properties for the database user account:

Property	Description
Database user ID	Name for the data profiling warehouse user account.
Database user password	Password for the data profiling warehouse user account.

Geben Sie bei Auswahl von IBM DB2 den Tablespace für die Repository-Tabellen an:

Eigenschaft	Beschreibung
Tablespace	<p>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.</p> <p>Wenn Sie in einer Datenbank mit einer einzigen Partition diese Option nicht auswählen, erstellt das Installationsprogramm die Tabellen im Standard-Tablespace.</p> <p>Wählen Sie diese Option in einer Datenbank mit mehreren Partitionen aus und geben Sie den Namen des nicht partitionierten Tablespace an, der sich in der Katalogpartition der Datenbank befindet.</p>

3. To specify the schema name, press **1**. If you do not want to specify a schema name, press **2**. Default is **2**. If you select Microsoft SQL Server, specify the schema for the repository tables and database connection. If you do not specify a schema name, the installer creates the tables in the default schema.

4. To enter the JDBC connection information using the JDBC URL information, press **1**. To enter the JDBC connection information using a custom JDBC connection string, press **2**.

a. 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
Hostname der Datenbank	Hostname für die Datenbank
Portnummer der Datenbank	Die Portnummer für die Datenbank.
Datenbankdienstname	Dienst- oder Datenbankname: <ul style="list-style-type: none">- Oracle: Geben Sie den Dienstnamen ein.- Microsoft SQL Server: Geben Sie den Datenbanknamen ein.- IBM DB2: Geben Sie den Dienstnamen ein.
Konfigurieren von JDBC-Parametern	Geben Sie an, ob der Verbindungszeichenfolge weitere JDBC-Parameter hinzugefügt werden sollen: 1 – Ja 2 – Nein Geben Sie bei Auswahl von „Ja“ die Parameter ein oder drücken Sie die Eingabetaste, um die Standardparameter zu übernehmen. Bei Auswahl von „Nein“ wird die JDBC-Verbindungszeichenfolge ohne Parameter erstellt.

- Um die Verbindungsdaten mithilfe einer benutzerdefinierten JDBC-Verbindungszeichenfolge einzugeben, geben Sie die Verbindungszeichenfolge ein.
Verwenden Sie die folgende Syntax in der JDBC-Verbindungszeichenfolge:

IBM DB2

```
jdbc:Informatica:db2://<hostname>:<portnummer>;DatabaseName=
```

Oracle

```
jdbc:Informatica:oracle://<hostname>:<portnummer>;ServiceName=
```

Verwenden Sie die folgende Verbindungszeichenfolge, um eine Verbindung zur Oracle-Datenbank über den Oracle Connection Manager herzustellen:

```
jdbc:Informatica:oracle:TNSNamesFile=<vollqualifizierter Pfad zur Datei  
tnsnames.ora>;TNSServerName=<TNS-Name>;
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://  
<hostname>:<portnummer>;SelectMethod=cursor;DatabaseName=
```

Microsoft Azure SQL

```
jdbc:Informatica:sqlserver://  
<hostname>:<portnummer>;SelectMethod=cursor;DatabaseName=<datenbankname>;Snap  
shotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.win  
dows.net;ValidateServerCertificate=false
```

PostgreSQL

```
jdbc:Informatica:postgresql://<hostname>:<portnummer>;DatabaseName=
```

Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database  
name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersio  
n=TLSv1.2;
```

Stellen Sie sicher, dass die Verbindungszeichenfolge alle vom Datenbanksystem benötigten Verbindungsparameter enthält.

5. Enter the data access connection string.

PowerCenter-Repository-Dienst und PowerCenter-Integrationsdienst

Sie können den PowerCenter-Repository-Dienst und den PowerCenter-Integrationsdienst konfigurieren.

- 1. Wenn Sie gewählt haben, während der Installation einen PowerCenter-Repository-Dienst und einen PowerCenter-Integrationsdienst zu erstellen, wird die Seite **PowerCenter-Repository-Dienst und PowerCenter-Integrationsdienst** geöffnet.

- 2. Wählen Sie die Datenbank aus, die für das PowerCenter-Repository konfiguriert werden soll.
In der folgenden Tabelle werden die Datenbanken aufgelistet, die Sie für das PowerCenter-Repository konfigurieren können:

Eingabeaufforderung	Beschreibung
Datenbanktyp	Datenbanktyp für das PowerCenter-Repository. Wählen Sie eine der folgenden Optionen aus: 1 – Oracle 2 – Microsoft SQL Server 3 – PostgreSQL 4 – IBM DB2 5 – Sybase ASE

- 3. 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 für das Konto des Benutzers der PowerCenter-Repository-Datenbank.
Benutzerpasswort	Das Passwort für das PowerCenter-Datenbankbenutzerkonto.
Datenbankdienstname	Dienst- oder Datenbankname für PowerCenter: <ul style="list-style-type: none"> - Oracle: Geben Sie den Dienstnamen ein. - Microsoft SQL Server: Geben Sie den Datenbanknamen ein. - PostgreSQL: Geben Sie den Namen der Datenbank ein. - IBM DB2: Geben Sie den Datenbanknamen ein. - Sybase ASE: Geben Sie den Datenbanknamen ein.
Hostname der Datenbank	Geben Sie die Datenbank des PowerCenter-Repositorys ein.

- Geben Sie den Namen des zu erstellenden PowerCenter-Repository-Diensts ein.
- Geben Sie den Namen des zu erstellenden PowerCenter-Integrationsdiensts ein.
- Wählen Sie die Codepage des PowerCenter-Repository-Diensts aus. Der Standardwert ist 7-Bit-ASCII.
- Wählen Sie die Codepage des PowerCenter-Integrationsdiensts aus. Der Standardwert ist 7-Bit-ASCII.
- Klicken Sie auf **Weiter**.
- Klicken Sie zum Beenden des Installationsprogramms auf **Fertig**.

Das Installationsprogramm erstellt den PowerCenter-Repository-Dienst sowie den PowerCenter-Integrationsdienst und startet die Dienste.

In der **Installationsübersicht** wird angezeigt, ob die Installation erfolgreich abgeschlossen wurde. Die Übersicht zeigt außerdem den Status der installierten Komponenten und ihre Konfiguration an.

In der **Installationsübersicht** wird angezeigt, ob die Installation erfolgreich abgeschlossen wurde. Der Bericht zeigt außerdem den Status der installierten Komponenten und deren Konfiguration an.

Beitreten zu einer Domäne

Sie können eine Verknüpfung zu einer Domäne herstellen, wenn Sie eine Installation auf mehreren Computern vornehmen und eine Domäne auf einem anderen Computer erstellt haben.

Ausführen des Installationsprogramms

Führen Sie die folgenden Schritte aus, um das Installationsprogramm auszuführen:

- Melden Sie sich mit einem Systembenutzerkonto am Computer an.
- Schließen Sie alle anderen Anwendungen.

3. Wechseln Sie in das Stammverzeichnis für die Installationsdateien und führen Sie die Datei „install.bat“ als Administrator aus.

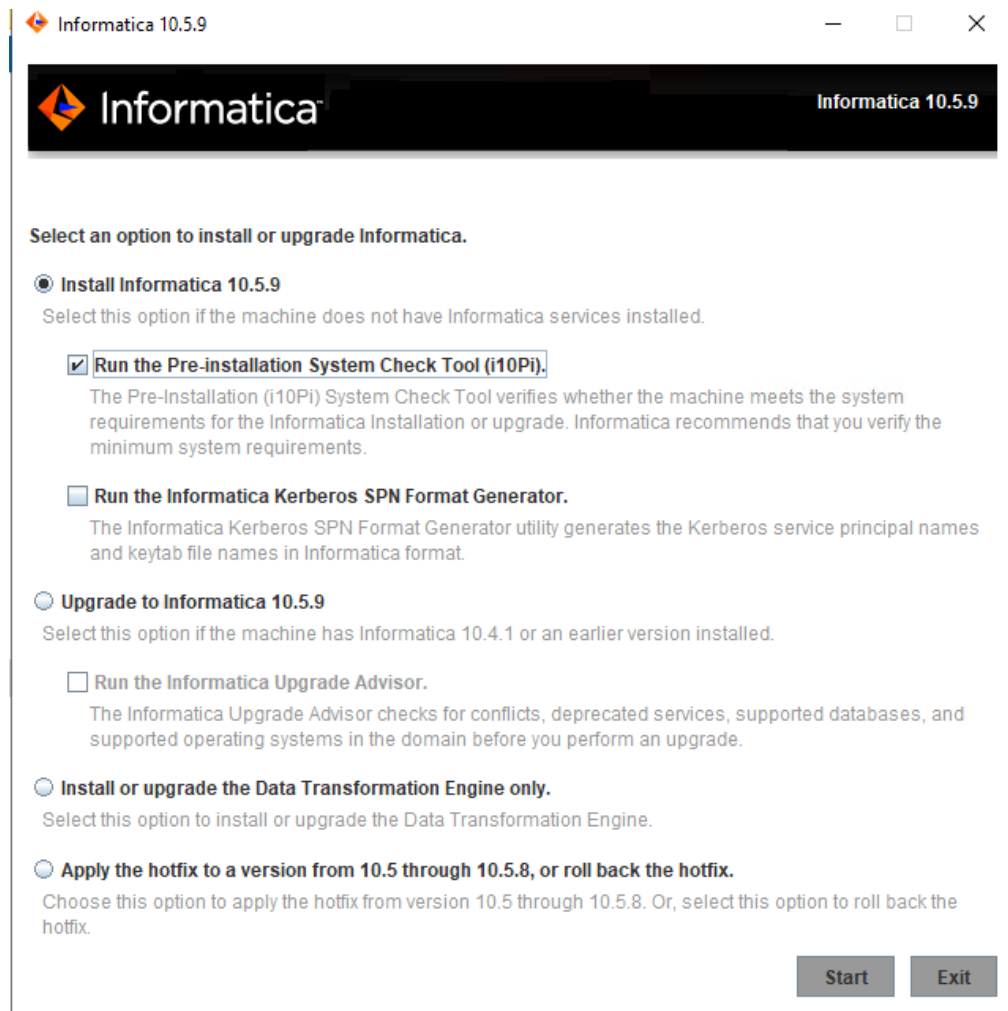
Klicken Sie zum Ausführen der Datei als Administrator mit der rechten Maustaste auf die Datei „install.bat“ und wählen Sie **Als Administrator ausführen** aus.

Hinweis: Wenn Sie das Installationsprogramm nicht als Administrator ausführen, meldet der Windows-Systemadministrator möglicherweise Probleme, wenn Sie auf die Dateien im Informatica-Installationsverzeichnis zugreifen.

Die Seite Informatica 10.5.9 wird geöffnet.

Willkommen beim Informatica-Installationsprogramm

1. Wählen Sie **Informatica 10.5.9** aus.



Informatica stellt Dienstprogramme bereit, um die Installation der Informatica-Dienste zu vereinfachen. Führen Sie die folgenden Dienstprogramme vor der Installation von Informatica-Diensten aus:

- Vorinstallations-Systemprüfungstool (i10Pi). Stellt sicher, dass der Computer, auf dem die Informatica-Dienste installiert werden, die Systemanforderungen für die Installation erfüllt.
Weitere Informationen zum Ausführen des Vorinstallations-Systemprüfungstools (i10Pi) finden Sie unter [“Ausführen des Vorinstallations-Systemprüfungstools \(i10Pi\) im Grafikmodus” auf Seite 115](#).
- Kerberos SPN-Formatgenerator von Informatica. Erstellt eine Liste der Kerberos-Dienstprinzipalnamen und Keytab-Dateinamen, die zum Ausführen von Informatica-Diensten in einem Netzwerk mit Kerberos-Authentifizierung benötigt werden.

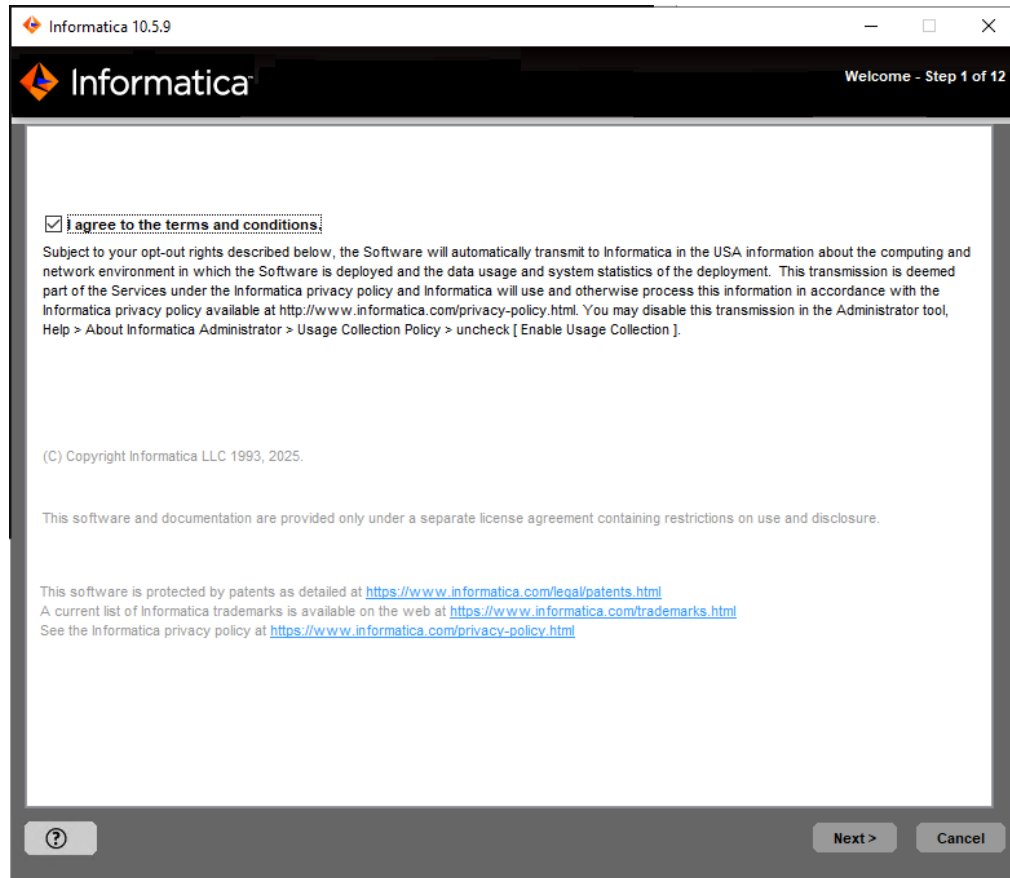
Sie können das Installationsprogramm zum Ausführen der Dienstprogramme verwenden, bevor Sie die Informatica-Dienste installieren. Starten Sie nach dem Beenden eines Dienstprogramms das Installationsprogramm erneut, um das nächste Dienstprogramm auszuführen oder die Informatica-Dienste zu installieren.

2. Klicken Sie auf **Start**.

Der Abschnitt **Willkommen** wird angezeigt.

Willkommen – Akzeptieren der allgemeinen Geschäftsbedingungen

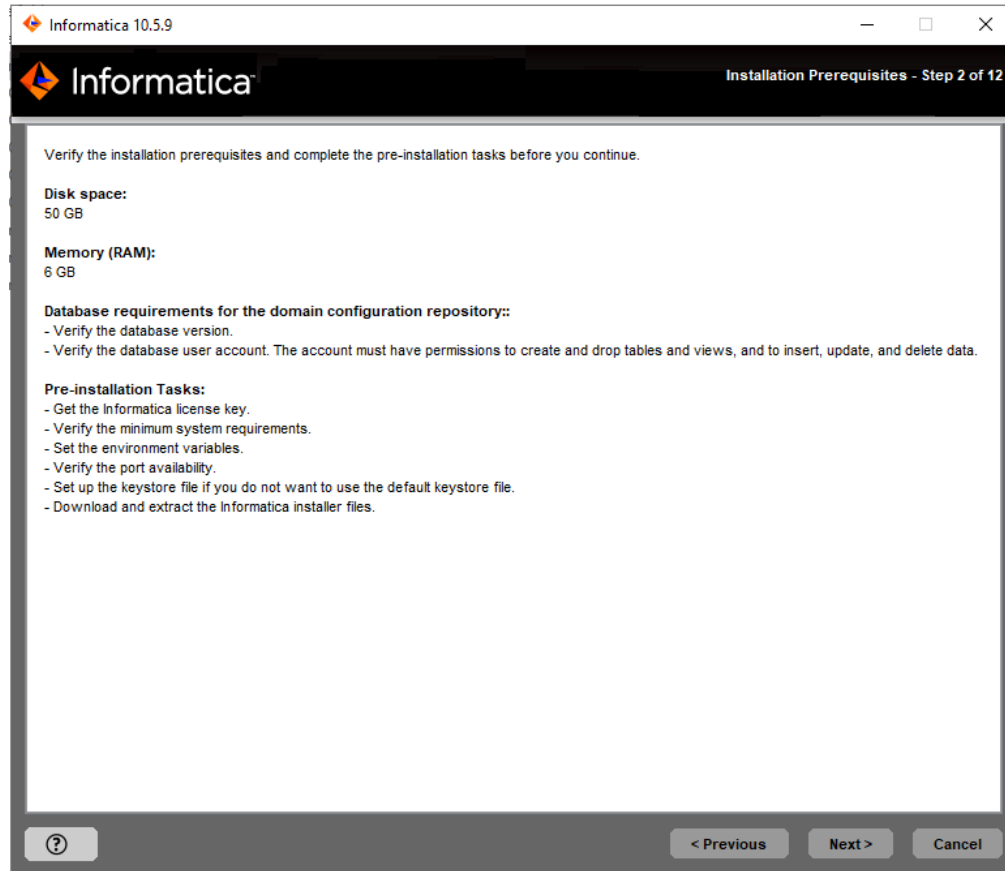
1. Lesen Sie die Bedingungen für die Informatica-Installation und das Toolkit zur Produktverwendung und wählen Sie **Ich stimme den Bedingungen zu** aus.



Informatica DiscoveryIQ ist ein Produktnutzungstool, das Routineberichte über Datennutzung und Systemstatistiken an Informatica sendet. Nach der Installation und Konfiguration der Informatica-Domäne lädt Informatica DiscoveryIQ alle 15 Minuten Daten an Informatica hoch. Danach sendet die Domäne die Daten alle 30 Tage. Sie können die Verwendung von Statistiken im Administrator Tool deaktivieren.

2. Klicken Sie auf **Weiter**.

Auf der Seite **Installationsvoraussetzungen** werden die Installationsanforderungen angezeigt. Stellen Sie sicher, dass alle Voraussetzungen erfüllt sind, bevor Sie die Installation fortsetzen.



3. Klicken Sie auf „Weiter“.

Der Abschnitt **Lizenz- und Installationsverzeichnis** wird angezeigt.

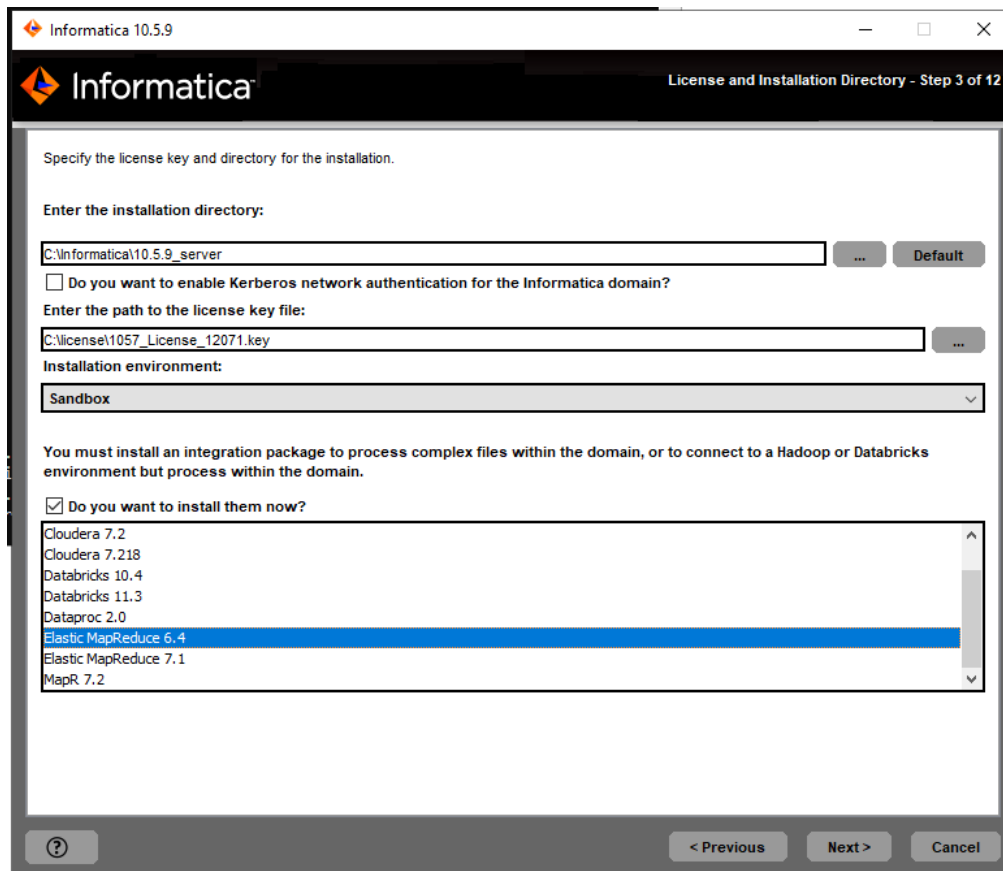
Lizenz und Installationsverzeichnis

Nachdem Sie die Installationsvoraussetzungen überprüft haben, können Sie das Installationsverzeichnis angeben.

1. Geben Sie auf der Seite **Lizenz und Installationsverzeichnis** den Informatica-Lizenzschlüssel, das Installationsverzeichnis, die Installationsumgebung und die Verteilungspakete ein.

In der folgenden Tabelle werden der Lizenzschlüssel und das Verzeichnis beschrieben, die für die Installation der Informatica-Dienste und die Installation der Integrationspakete angegeben werden:

Eigenschaft	Beschreibung
Lizenzschlüsseldatei	Pfad und Dateinamen des Informatica-Lizenzschlüssels.
Installationsverzeichnis	<p>Absoluter Pfad für das Installationsverzeichnis. Das Installationsverzeichnis muss sich auf dem Computer befinden, auf dem Informatica installiert wird. Die Verzeichnisnamen im Pfad dürfen weder Leerzeichen noch die folgenden Sonderzeichen enthalten: @ * \$ # ! % () { } []</p> <p>Hinweis: Informatica empfiehlt die Verwendung alphanumerischer Zeichen im Installationsverzeichnispfad. Wenn Sie ein Sonderzeichen wie á oder € verwenden, können zur Laufzeit unerwartete Ergebnisse auftreten.</p>
Installationsumgebung	<p>Umgebungstyp, der der Installation der Informatica-Dienste zugeordnet ist.</p> <ul style="list-style-type: none"> - Legen Sie die Sandbox-Umgebung für eine Basisumgebung fest, die für Machbarkeitsstudien mit minimaler Benutzerzahl verwendet wird. - Legen Sie die Entwicklungsumgebung für die Designumgebung fest. - Legen Sie die Testumgebung für die Verarbeitung großer Datenmengen ähnlich der in einer Produktionsumgebung fest. - Legen Sie die Produktionsumgebung für die massiv parallele Verarbeitung großer Datenmengen für Endbenutzer fest. Bei erweiterten Produktionsumgebungen handelt es sich in der Regel um Setups mit mehreren Knoten.
Verteilungspakete	<p>Sie können auswählen, ob die Verteilungspakete über das Informatica-Installationsprogramm installiert werden sollen.</p> <p>Wenn Sie Verteilungspakete installieren möchten, wählen Sie ein oder mehrere Pakete aus der Liste aus, die Sie installieren möchten.</p>



2. Klicken Sie auf **Weiter**.

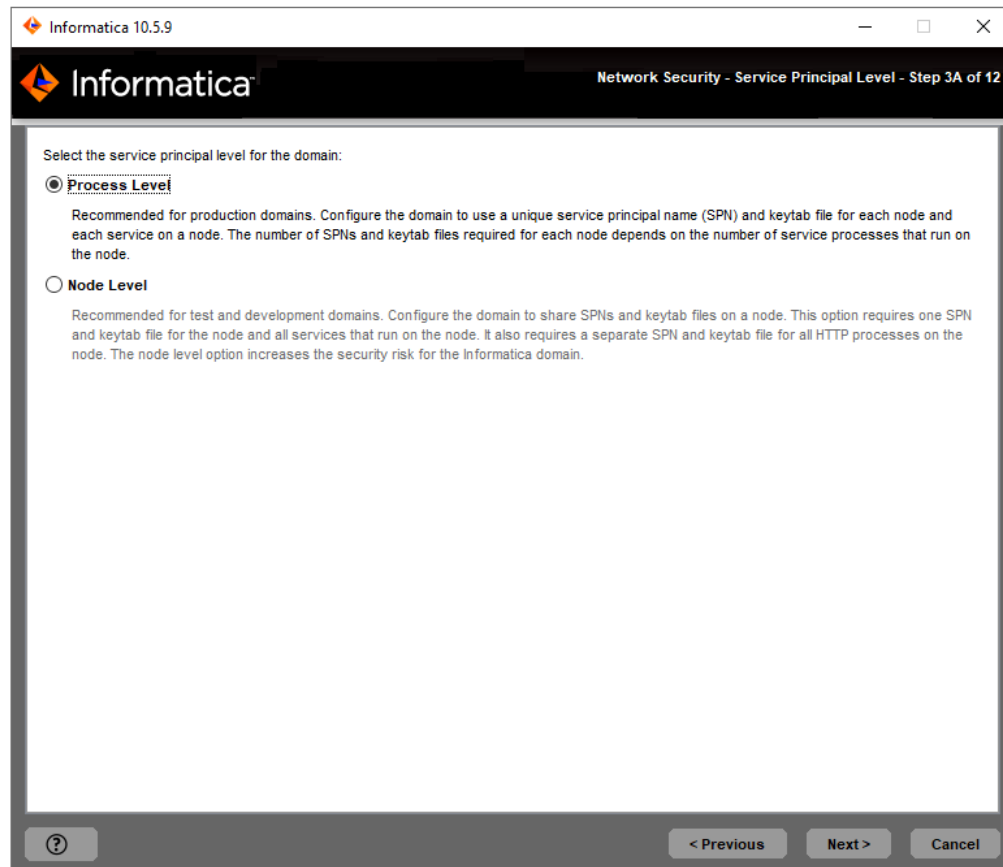
Wenn Sie die Kerberos-Netzwerkauthentifizierung aktiviert haben, wird der Abschnitt **Dienstprinzipalebene** angezeigt.

Wenn Kerberos-Netzwerkauthentifizierung nicht aktiviert wurde, wird der Abschnitt **Vorinstallationsübersicht** angezeigt. Überprüfen Sie die Installationsinformationen und drücken Sie die **Eingabetaste**, um fortzufahren. Fahren Sie mit ["Domänenauswahl" auf Seite 127](#) fort.

Netzwerksicherheit – Dienstprinzipalebene

Nachdem Sie das Installationsverzeichnis angegeben haben, können Sie die Sicherheitsstufe konfigurieren.

1. Wenn Sie die Kerberos-Netzwerkauthentifizierung aktiviert haben, wird die Seite **Netzwerksicherheit – Dienstprinzipalebene** angezeigt.



2. Wählen Sie auf der Seite **Netzwerksicherheit - Dienstprinzipalebene** die Ebene aus, auf die Sie die Kerberos-Dienstprinzipale für die Domäne festlegen möchten.

In der folgenden Tabelle werden die Dienstprinzipalebenen beschrieben, die Sie auswählen können:

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

3. Klicken Sie auf **Weiter**.

Der Abschnitt **Netzwerksicherheit – Kerberos-Authentifizierung** wird angezeigt.

Network Security - Kerberos Authentication

After you configure the security level, you can configure Kerberos authentication.

- 1. The **Network Security - Kerberos Authentication** page, enter the domain and keytab information required for Kerberos authentication.

Informatica 10.5.9

Informatica

Network Security - Kerberos Authentication - Step 3B of 12

Specify the Kerberos network authentication parameters.

Domain name:

Installer_Domain

Node name:

Installer_Node_1

Node host name:

INinstwin201901.informatica.com

Service realm name:

ISPPLATFORMKRB.COM

User realm name:

ISPPLATFORMKRB.COM

Keytab directory:

E:\keytabs\master

...

Fully qualified path to the Kerberos configuration file:

E:\keytabs\master\krb5.conf

...

?

< Previous

Next >

Cancel

The following table describes the Informatica domain and node information that you must provide:

Property	Description
Domain name	Name of the domain to create. Der Name darf maximal 128 Zeichen umfassen und muss im 7-Bit-ASCII-Format vorliegen. Der Name darf weder Leerzeichen noch eines der folgenden Zeichen enthalten: ` % * + ; " ? , < > \ /
Node name	Name des zu erstellenden Knotens.
Node host name	Fully qualified host name or IP address of the machine on which to create the node. Hinweis: Der Hostname des Knotens darf keine Unterstriche (_) enthalten. Verwenden Sie nicht localhost. Der Hostname muss den Computer eindeutig kennzeichnen.

In der folgenden Tabelle werden der Kerberos-Bereich und die Keytab-Informationen beschrieben, die Sie angeben müssen:

Eigenschaft	Beschreibung
Dienstbereichsname	<p>Name des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird. Der Bereichsname muss in Großbuchstaben angegeben werden und unterliegt der Groß-/Kleinschreibung.</p> <p>Zum Konfigurieren von bereichsübergreifender Kerberos-Authentifizierung geben Sie den Namen des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird, getrennt durch Kommas ein. Beispiel: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM</p> <p>Verwenden Sie ein Sternchen als Platzhalterzeichen vor dem Bereichsnamen, um alle Bereiche mit diesem Namen einzuschließen. Beispiel: *EAST.COMPANY.COM</p>
Benutzerbereichsname	<p>Name des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird. Der Bereichsname muss in Großbuchstaben angegeben werden und unterliegt der Groß-/Kleinschreibung.</p> <p>Zum Konfigurieren von bereichsübergreifender Kerberos-Authentifizierung geben Sie den Namen des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird, getrennt durch Kommas ein. Beispiel: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM</p> <p>Verwenden Sie ein Sternchen als Platzhalterzeichen vor dem Bereichsnamen, um alle Bereiche mit diesem Namen einzuschließen. Beispiel: *EAST.COMPANY.COM</p>
Keytab-Verzeichnis	<p>Verzeichnis, in dem alle Keytab-Dateien für die Informatica-Domäne gespeichert werden. Der Name einer Keytab-Datei in der Informatica-Domäne muss einem von Informatica festgelegten Format entsprechen.</p>
Kerberos-Konfigurationsdatei	<p>Pfad und Dateiname der Kerberos-Konfigurationsdatei. Informatica benötigt folgenden Namen für die Kerberos-Konfigurationsdatei: <i>krb5.conf</i></p>

Wichtig: Wenn Sie die Domäne zur Ausführung mit Kerberos-Authentifizierung konfigurieren, müssen der Domänen- und Knotenname sowie der Knoten-Hostname mit den Namen übereinstimmen, die bei Ausführung des Kerberos SPN-Formatgenerators von Informatica zum Erzeugen der SPNs und Keytab-Dateinamen angegeben wurden. Wenn Sie einen anderen Domänen-, Knoten- oder Hostnamen verwenden, erzeugen Sie den SPN und die Keytab-Dateinamen neu und bitten Sie den Kerberos-Administrator, den neuen SPN der Kerberos-Prinzipaldatenbank hinzuzufügen und die Keytab-Dateien zu erstellen.

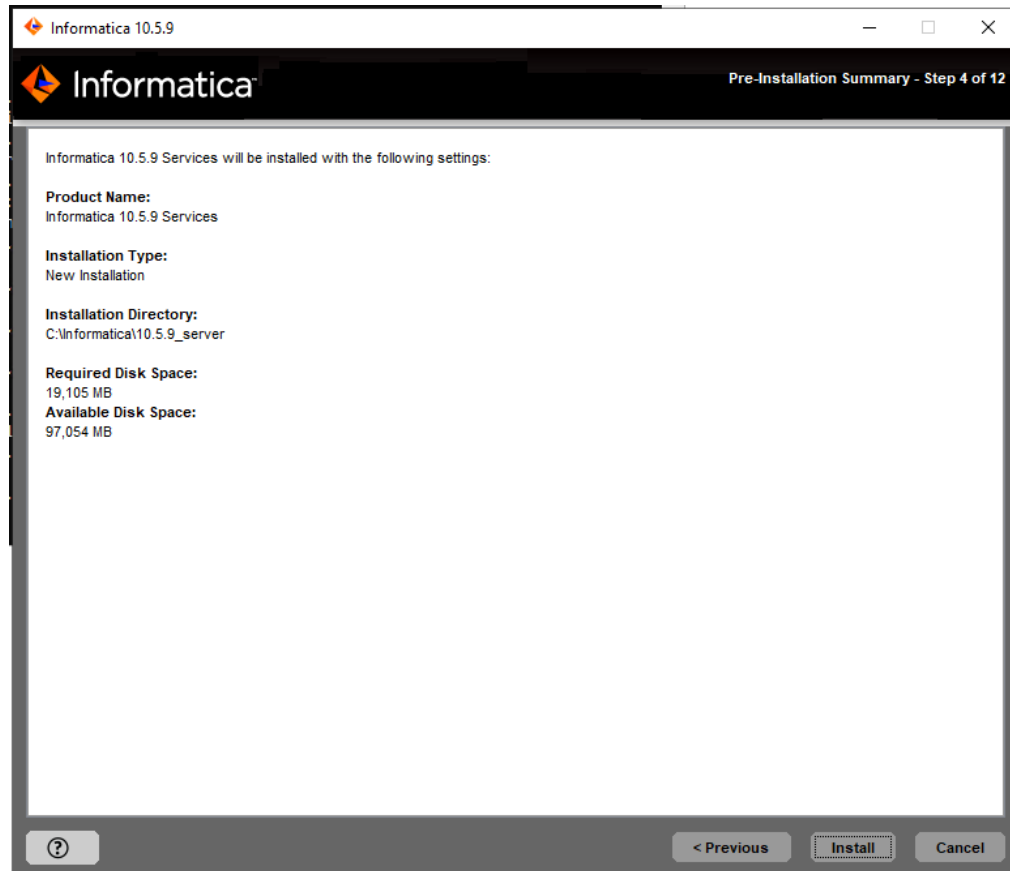
2. Click **Next**.

The **Pre-Installation Summary** section appears. Review the installation information.

Domänenauswahl

Nachdem Sie sich die Vorinstallationszusammenfassung durchgesehen haben, können Sie die Domäneninformationen eingeben.

1. Überprüfen Sie die Seite **Vor der Installation – Zusammenfassung**.



2. Überprüfen Sie die Installationsinformationen und klicken Sie auf **Installieren**, um fortzufahren.

Der Installer kopiert die Informatica-Dateien in das Installationsverzeichnis. Nach dem Kopieren der Dateien durch das Installationsprogramm wird die Seite **Domänenauswahl** angezeigt.

3. Wählen Sie **Domäne hinzufügen** aus.
Das Installationsprogramm fügt einen Knoten auf dem Computer an, auf dem die Installation erfolgt.
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.
4. Geben Sie an, ob für die anzufügende Domäne die Option zur sicheren Kommunikation aktiviert wurde.
Drücken Sie **1**, um eine ungesicherte Domäne anzufügen, oder **2**, um eine sichere Domäne anzufügen.
5. Wählen Sie den Knotentyp aus, den Sie erstellen möchten.
Drücken 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.
6. Wenn Sie eine HTTPS-Verbindung für den Informatica Administrator aktivieren, geben Sie die zum Sichern der Verbindung zu verwendende HTTPS-Portnummer ein.
7. Legen Sie fest, ob Sie zum Aktivieren der SAML-Authentifizierung in der Domäne SSL-Standardzertifikate von Informatica oder eigene SSL-Zertifikate verwenden möchten.

In der folgenden Tabelle werden die SSL-Zertifikatsoptionen für die SAML-Authentifizierung beschrieben:

Option	Beschreibung
Standardmäßige SSL-Zertifikatsdatei von Informatica verwenden	Wählen Sie diese Option aus, um für die SAML-Authentifizierung die Truststore-Standarddatei von Informatica zu verwenden.
Speicherort der SSL-Zertifikatsdatei eingeben	Wählen Sie diese Option, um für die SAML-Authentifizierung eine benutzerdefinierte Truststore-Datei zu verwenden. Geben Sie das Verzeichnis an, das die benutzerdefinierte Truststore-Datei auf Gateway-Knoten in der Domäne enthält. Geben Sie nur das Verzeichnis an, nicht den vollständigen Pfad zur Datei.

8. Zur Konfiguration der Unterstützung von Single Sign-On (SSO) auf der Basis der Security Assertion Markup Language (SAML) für webbasierte Informatica-Anwendungen in einer Informatica-Domäne aktivieren Sie das Kontrollkästchen, um die SAML-Authentifizierung zu aktivieren.

Hinweis: Wenn Sie die Kerberos-Netzwerkauthentifizierung aktivieren, können Sie die SAML-Authentifizierung nicht konfigurieren.

9. Klicken Sie auf **Weiter**.

Wenn Sie die sichere Kommunikation für die Domäne nicht aktivieren, wird die Seite **Domänenkonfiguration** angezeigt. Fahren Sie mit dem Schritt fort, der die Seite „Domänenkonfigurations-Repository“ beschreibt. Wenn Sie das Kontrollkästchen zum Aktivieren der sicheren Kommunikation für die Domäne aktiviert haben, wird die Seite **Domänensicherheit – Sichere Kommunikation** angezeigt.

Domänensicherheit – Sichere Verbindung

Nachdem Sie die Domänen konfiguriert haben, können Sie die Domänensicherheit konfigurieren.

1. Geben Sie auf der Seite **Domänensicherheit – Sichere Kommunikation** an, ob die standardmäßigen SSL-Zertifikate von Informatica oder eigene SSL-Zertifikate zum Aktivieren sicherer Kommunikation in der Domäne verwendet werden sollen.

The screenshot shows the 'Domain Security - Secure Communication' configuration window in Informatica 10.5.9. The window title is 'Informatica 10.5.9'. The Informatica logo is in the top left, and the title 'Domain Security - Secure Communication - Step 5B of 12' is in the top right. The main content area has the heading 'Select the SSL certificates to enable secure communication within the domain:'. There are two radio buttons: the first is selected and labeled 'Use the default Informatica SSL certificates contained in the default keystore and truststore.'; the second is labeled 'Use custom SSL certificates. Specify the path, file name, and passwords for the keystore and truststore files that contain the certificates'. Below the radio buttons are four input fields: 'Keystore file directory:' with 'c:\temp', 'Keystore password:', 'Truststore file directory:' with 'c:\temp', and 'Truststore password:'. At the bottom, there is a navigation bar with a question mark icon, '< Previous', 'Next >', and 'Cancel' buttons.

In der folgenden Tabelle werden die SSL-Zertifikatsoptionen zum Sichern der Informatica-Domäne beschrieben:

Option	Beschreibung
SSL-Standardzertifikate 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 standardmäßigen Schlüsselspeicherdateien und Truststore-Dateien von Informatica verwenden, ist 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.
Benutzerdefinierte SSL-Zertifikate verwenden	Geben Sie den Pfad zur Schlüsselspeicher- und zur Truststore-Datei ein, die die SSL-Zertifikate enthalten. Sie können ein selbstsigniertes Zertifikat oder ein von einer Zertifizierungsstelle ausgegebenes Zertifikat angeben. 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-Dateien und Schlüsselspeicherdateien in einem Verzeichnis, auf das alle Knoten in der Domäne zugreifen können, und geben Sie für alle Knoten in derselben Domäne dasselbe Verzeichnis für Schlüsselspeicherdateien und Truststore-Dateien an. Um die privaten Truststore-Dateien festzulegen, müssen Sie die Zertifikate manuell importieren. Führen Sie den keytool-Befehl im Verzeichnis <INFA_JDK_HOME> aus, um die privaten Truststore-Zertifikate zu importieren. Verwenden Sie beispielsweise den folgenden keytool-Befehl: keytool -noprompt -importkeystore -srckeystore <source truststore file path> -srcstorepass <source truststore file password> -srcalias <alias> -srcstoretype JKS -destkeystore <destination truststore file path> -deststorepass <destination truststore file password> -keypass <private key password> -deststoretype JKS

- Wenn Sie die Sicherheitszertifikate bereitstellen, geben Sie den Speicherort und die Passwörter der KeyStore- und Truststore-Dateien an.

In der folgenden Tabelle werden die Parameter beschrieben, die für die SSL-Zertifikatsdateien eingegeben werden müssen:

Eigenschaft	Beschreibung
Verzeichnis der Schlüsselspeicherdatei	Das Verzeichnis, das die Schlüsselspeicherdateien enthält. Das Verzeichnis muss Dateien namens infa_keystore.jks und infa_keystore.pem enthalten.
Schlüsselspeicher-Passwort	Das Passwort für den Schlüsselspeicher infa_keystore.jks.
Verzeichnis der Truststore-Datei	Das Verzeichnis, das die Truststore-Dateien enthält. Das Verzeichnis muss Dateien namens infa_truststore.jks und infa_truststore.pem enthalten.
Truststore-Passwort	Das Passwort für die Datei infa_truststore.jks.

3. Klicken Sie auf **Weiter**.

Der Abschnitt **Domänenkonfiguration** wird angezeigt.

Domänenkonfiguration

Nachdem Sie die Domänensicherheit konfiguriert haben, können Sie die Verbindungsdetails für das Domänen-Repository konfigurieren.

- Geben Sie die Informationen für die Domäne ein, die Sie anfügen möchten.

In der folgenden Tabelle werden die Eigenschaften beschrieben, die Sie für die Domäne festlegen:

Eigenschaft	Beschreibung
Domänenname	Der Name der zu verknüpfenden Domäne.
Host des Gateway-Knotens	Der Hostname des Computers, der den Gateway-Knoten für die Domäne hostet.
Port des Gateway-Knotens	Die Portnummer des Gateway-Knotens.
Domänenbenutzername	Der Benutzername des Administrators der Domäne, zu der Sie eine Verknüpfung herstellen möchten.
Domänenpasswort	Das Passwort für den Domänenadministrator.
Sicherheitsdomänenname	Name der gesicherten Domäne.

Der Abschnitt **Domänensicherheit – Verschlüsselungsschlüssel** wird angezeigt.

Domänensicherheit – Verschlüsselungsschlüssel

Nachdem Sie das Domänen-Repository konfiguriert haben, können Sie den Verschlüsselungsschlüssel konfigurieren.

1. Geben Sie im Abschnitt **Domänensicherheit – Verschlüsselungsschlüssel** die Verschlüsselungsschlüsselparameter ein, die Sie beim Erstellen einer Domäne angeben müssen.

The screenshot shows the 'Domain Security - Encryption Key - Step 3C of 12' window in Informatica 10.5.9. The window title bar says 'Informatica 10.5.9'. The Informatica logo is in the top left, and the title 'Domain Security - Encryption Key - Step 3C of 12' is in the top right. The main content area has the instruction 'Enter the encryption key information.' and four input fields:

- Encryption key directory:** A text box containing 'C:\Informatica\10.5.9_server\isplconfig\keys' with a browse button ('...') and a 'Default' button to its right.
- Domain user name:** A text box containing 'Administrator'.
- Domain password:** A password field with 10 dots.
- Confirm password:** A password field with 10 dots.

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

Eigenschaft	Beschreibung
Verzeichnis des Verschlüsselungsschlüssels	Verzeichnis, in dem der Verschlüsselungsschlüssel für die Domäne gespeichert werden soll. Standardmäßig wird der Verschlüsselungsschlüssel im folgenden Verzeichnis erstellt: <Informatica-Installationsverzeichnis>/isp/config/keys.
Geben Sie an, ob Sie den vom Installationsprogramm generierten Site-Schlüssel sichern möchten oder nicht:	<p>Ein eindeutiger Site-Schlüssel wird generiert. Wenn Sie den Site-Schlüssel verlieren, können Sie ihn nicht erneut generieren. Speichern Sie unbedingt eine Kopie dieses Schlüssels und teilen Sie den eindeutigen Site-Schlüssel nicht mit anderen.</p> <p>Geben Sie an, ob Sie den vom Installationsprogramm generierten Site-Schlüssel sichern möchten oder nicht:</p> <ul style="list-style-type: none"> - Wählen Sie 1 für Nein. Wenn Sie Nein wählen, wird das Installationsprogramm beendet. - Wählen Sie 2 für JA. Wenn Sie Ja wählen, stimmen Sie zu, die Datei manuell zu sichern.

Das Installationsprogramm legt verschiedene Berechtigungen für das Verzeichnis und die Dateien im Verzeichnis fest. Weitere Informationen über die Berechtigungen für die Verschlüsselungsschlüsseldatei und das Verzeichnis finden Sie unter ["Sichere Dateien und Verzeichnisse" auf Seite 110](#).

2. Klicken Sie auf **Weiter**.

Der Abschnitt **Domänen- und Knotenkonfiguration** wird angezeigt.

Knotenkonfiguration der hinzuzufügenden Domäne

Nachdem Sie den Verschlüsselungsschlüssel konfiguriert haben, können Sie die Domäne und den Knoten konfigurieren, die angefügt werden.

1. Geben Sie die Informationen für die Domäne und den Knoten ein, die Sie anfügen möchten.

In der folgenden Tabelle werden die Eigenschaften beschrieben, die Sie für den aktuellen Knoten festlegen:

Eigenschaft	Beschreibung
Hostname des Knotens	<p>Hostname oder IP-Adresse des Computers, auf dem der Knoten angefügt werden soll.</p> <p>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.</p> <p>Hinweis: Der Hostname des Knotens darf keine Unterstriche (_) enthalten. Verwenden Sie nicht localhost. Der Hostname muss den Computer eindeutig kennzeichnen.</p>
Knotenname	Der Name des Knotens, den Sie anfügen möchten.
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.

- Legen Sie fest, ob die vom Installationsprogramm zugewiesenen erweiterten Portkonfigurationen für die Domänen- und Knotenkomponenten angezeigt werden sollen.

Wenn Sie die Option für Port-Konfigurationen deaktivieren, zeigt das Installationsprogramm die Port-Konfigurationen nicht an. Wenn Sie die Option für Port-Konfigurationen aktivieren, wird der Abschnitt **Port-Konfiguration** angezeigt. Das Installationsprogramm zeigt 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.

- Wählen Sie aus, ob Sie den Modellrepository-Dienst und den Datenintegrationsdienst erstellen möchten.

Wenn Sie die Dienste erstellen möchten, werden die Abschnitte **Modellrepository-Dienst** und **Datenintegrationsdienst** angezeigt.

- Wählen Sie aus, ob Sie den PowerCenter-Repository-Dienst und den PowerCenter-Integrationsdienst erstellen möchten.

Wenn Sie die Dienste erstellen möchten, werden die Abschnitte **PowerCenter-Repository-Dienst** und **PowerCenter-Integrationsdienst** angezeigt.

In der **Installationsübersicht** wird angezeigt, ob die Installation erfolgreich abgeschlossen wurde. Die Übersicht zeigt außerdem den Status der installierten Komponenten und ihre Konfiguration an.

Port-Konfiguration

Sie können die Portnummern für Dienstmanager und Informatica Administrator aktualisieren.

1. Wenn Sie angegeben haben, dass die Seite für die Port-Konfiguration angezeigt werden soll, wird die Seite **Port-Konfiguration** geöffnet.

Informatica 10.5.9

Port Configuration - Step 8A of 12

Enter the port numbers for the Service Manager and Informatica Administrator.

Service Manager port:	7561
Service Manager shutdown port:	7562
Informatica Administrator port:	7563
Informatica Administrator shutdown port:	7564

Enter a range of port numbers for service processes in the node.

Minimum port number:	7569
Maximum port number:	7669

Default

< Previous Next > Cancel

2. Geben Sie auf der Seite **Portkonfiguration** die Portnummern für den Dienstmanager der Domäne und die Dienstprozesse ein, die auf dem Knoten ausgeführt werden.

Stellen Sie sicher, dass die von Ihnen eingegebenen Portnummern nicht von anderen Anwendungen verwendet werden.

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

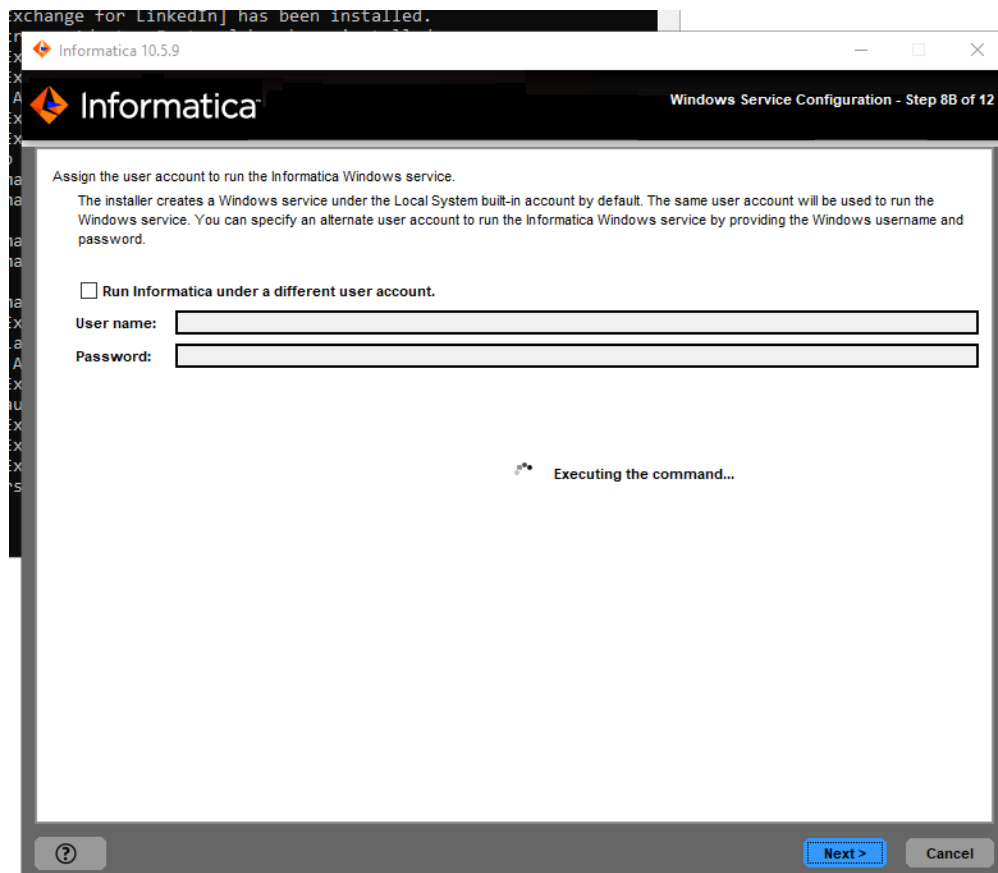
Port	Beschreibung
Dienstmanager-Port	Die vom Dienstmanager auf dem Knoten verwendete Portnummer. Der Dienstmanager überwacht eingehende Verbindungsanfragen an diesem Port. Clientanwendungen verwenden diesen Port zur Kommunikation mit den Diensten in dieser Domäne. Die Informatica-Befehlszeilenprogramme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

- Klicken Sie auf **Weiter**.

Die Seite **Windows-Dienstkonfiguration** wird angezeigt.

Windows-Dienstkonfiguration

1. Wenn Sie nicht angegeben haben, dass die Seite für die Port-Konfiguration angezeigt werden soll, zeigt das Installationsprogramm die Seite **Windows-Dienstkonfiguration** an.



2. Geben Sie auf der Seite **Windows-Dienstkonfiguration** an, ob der Windows-Dienst unter einem anderen Benutzerkonto ausgeführt werden soll.

Das Installationsprogramm erstellt einen Dienst zum Starten von Informatica. Der Dienst wird standardmäßig unter demselben Benutzerkonto ausgeführt wie dem, das für die Installation verwendet wurde. Sie können den Windows-Dienst unter einem anderen Benutzerkonto ausführen.

In der folgenden Tabelle werden die Eigenschaften beschrieben, die zum Ausführen von Informatica unter einem anderen Benutzerkonto eingerichtet werden:

Eigenschaft	Beschreibung
Informatica unter einem anderen Benutzerkonto ausführen	Zeigt die Option an, den Windows-Dienst unter einem anderen Benutzerkonto auszuführen.
Benutzername	Das Benutzerkonto, unter dem der Informatica-Windows-Dienst ausgeführt werden soll. Verwenden Sie das folgende Format: <Domänenname>\<Benutzerkonto> Dieses Benutzerkonto muss „Aktion“ als Betriebssystemberechtigung haben.
Passwort	Das Passwort zum Benutzerkonto, unter dem der Informatica-Windows-Dienst ausgeführt werden soll.

3. Klicken Sie auf **Weiter**.

Wenn Sie die Dienste nicht erstellen möchten, wird im Installationsprogramm die Seite **Installationsabschlussbericht** angezeigt. Auf der Seite **Nach der Installation – Zusammenfassung** wird angezeigt, ob die Installation erfolgreich abgeschlossen wurde.

Wenn Sie die Informatica-Anwendungsdienste konfiguriert haben, wird im Installationsprogramm die Seite **Datenbank des Modellrepository-Diensts** angezeigt.

Konfigurieren der Datenbank des Modellrepository-Diensts

Nachdem Sie die Domäne und den Knoten konfiguriert haben, können Sie die Eigenschaften der Modellrepository-Datenbank konfigurieren.

1. Geben Sie auf der Seite **Datenbank des Modellrepository-Diensts** die Datenbank- und Benutzerkontoinformationen für das Modellrepository ein.

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

Eigenschaft	Beschreibung
Datenbanktyp	Datenbank für das Repository. Wählen Sie eine der folgenden Datenbanken aus: <ul style="list-style-type: none"> - Oracle - IBM DB2 - Microsoft SQL Server - PostgreSQL
Datenbankbenutzer-ID	Benutzerkonto für die Repository-Datenbank.
Benutzerpasswort	Das Passwort für das Konto des Datenbankbenutzers.

Geben Sie bei Auswahl von IBM DB2 den Tablespace für die Repository-Tabellen an:

Eigenschaft	Beschreibung
Tablespace	<p>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.</p> <p>Wenn Sie in einer Datenbank mit einer einzigen Partition diese Option nicht auswählen, erstellt das Installationsprogramm die Tabellen im Standard-Tablespace.</p> <p>Wählen Sie diese Option in einer Datenbank mit mehreren Partitionen aus und geben Sie den Namen des nicht partitionierten Tablespace an, der sich in der Katalogpartition der Datenbank befindet.</p>

Geben Sie bei Auswahl von Microsoft SQL Server oder PostgreSQL das Schema für die Repository-Tabellen und die Datenbankverbindung an:

Eigenschaft	Beschreibung
Schemaname	Name des Schemas, das die Repository-Tabellen enthält. Ist diese Option nicht aktiviert, erstellt das Installationsprogramm die Tabellen im Standardschema.
Vertrauenswürdige Verbindung	Zeigt an, ob eine vertrauenswürdige Verbindung zu Microsoft SQL Server hergestellt werden soll. Die vertrauenswürdige Authentifizierung verwendet die Sicherheitsanmeldedaten des aktuellen Benutzers zur Herstellung der Verbindung zu Microsoft SQL Server. Ist diese Option nicht aktiviert, wird die Microsoft SQL Server-Authentifizierung verwendet.

Wenn Sie sichere Kommunikation für die Domäne aktivieren, können Sie das Modellrepository in einer mit dem SSL-Protokoll gesicherten Datenbank erstellen. Zum Erstellen eines sicheren Modellrepositorys fahren Sie mit Schritt [3](#) fort.

2. Geben Sie die Verbindungsinformationen für die Datenbank ein.

Wenn Sie kein sicheres Modellrepository erstellen, können Sie die Verbindungseigenschaften für die JDBC-URL angeben oder die JDBC-Verbindungszeichenfolge bereitstellen.

- Um die Verbindungsdaten mithilfe der JDBC-URL einzugeben, wählen Sie **JDBC-URL** aus und geben Sie die Eigenschaften der Datenbankverbindung ein.

In der folgenden Tabelle werden die JDBC-URL-Eigenschaften beschrieben, die Sie festlegen:

Eigenschaft	Beschreibung
Datenbankadresse	Der Hostname und die Portnummer für die Datenbank im Format <code>host_name:port</code> .
Datenbankdienstname	Dienst- oder Datenbankname: <ul style="list-style-type: none">- Oracle: Geben Sie den Dienstnamen ein.- Microsoft SQL Server: Geben Sie den Datenbanknamen ein.- IBM DB2: Geben Sie den Dienstnamen ein.- PostgreSQL: Geben Sie den Namen der Datenbank ein.
JDBC-Parameter	Optionale Parameter, die in die Datenbankverbindungszeichenfolge aufgenommen werden können. Mit den Parametern können die Datenbankvorgänge für die Datenbank optimiert werden. Überprüfen Sie die Gültigkeit der Parameterzeichenfolge. Das Installationsprogramm führt vor dem Hinzufügen der Parameterzeichenfolge zur JDBC-URL keine Überprüfung der Zeichenfolge durch. Ist diese Option nicht aktiviert, erstellt das Installationsprogramm die JDBC-URL ohne zusätzliche Parameter.

- Um die Verbindungsdaten mithilfe einer benutzerdefinierten JDBC-Verbindungszeichenfolge einzugeben, wählen Sie **Benutzerdefinierte JDBC-Verbindungszeichenfolge** aus und geben Sie die Verbindungszeichenfolge ein.

IBM DB2

```
jdbc:Informatica:db2://<Hostname>:<Portnummer>;DatabaseName=
```

Oracle

```
jdbc:Informatica:oracle://<Hostname>:<Portnummer>;ServiceName=
```

Verwenden Sie die folgende Verbindungszeichenfolge, um eine Verbindung zur Oracle-Datenbank über den Oracle Connection Manager herzustellen:

```
jdbc:Informatica:oracle:TNSNamesFile=<vollqualifizierter Pfad zur Datei  
tnsnames.ora>;TNSServerName=<TNS-Name>;
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://  
<Hostname>:<Portnummer>;SelectMethod=cursor;DatabaseName=
```

Microsoft Azure SQL

```
jdbc:Informatica:sqlserver://  
<hostname>:<portnummer>;SelectMethod=cursor;DatabaseName=<datenbankname>;SnapshotS  
erializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net  
;ValidateServerCertificate=false
```

Azure SQL-Datenbank mit Active Directory-Authentifizierung

```
"jdbc:informatica: sqlserver://  
<host_name>:<port_number>;database=<database_name>;encrypt=true;AuthenticationMeth  
od=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertificate=*.da  
tabase.windows.net;loginTimeout=<seconds>"
```

PostgreSQL

```
jdbc:Informatica:postgresql://<hostname>:<portnummer>;DatabaseName=
```

Azure PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database  
name>;EncryptionMethod=SSL;ValidateServerCertificate=true;CryptoProtocolVersion=TL  
Sv1.2;
```

Stellen Sie sicher, dass die Verbindungszeichenfolge alle vom Datenbanksystem benötigten Verbindungsparameter enthält.

3. Wählen Sie, ob ein sicheres Modellrepository erstellt werden soll.

Wenn Sie das Repository in einer gesicherten Datenbank erstellen, müssen Sie die Truststore-Informationen für die Datenbank angeben. Außerdem müssen Sie eine JDBC-Verbindungszeichenfolge angeben, die die Sicherheitsparameter für die Datenbank enthält.

In der folgenden Tabelle werden die Eigenschaften beschrieben, die für eine sichere Datenbank eingerichtet werden müssen:

Eigenschaft	Beschreibung
Datenbank-Truststore-Datei	Pfad und Dateiname der Truststore-Datei für die gesicherte Datenbank.
Datenbank-Truststore-Passwort	Passwort für die Truststore-Datei.
Benutzerdefinierte JDBC-Verbindungszeichenfolge	JDBC-Verbindungszeichenfolge zum Herstellen einer Verbindung mit der gesicherten Datenbank, einschließlich Hostname, Portnummer und Sicherheitsparameter für die Datenbank.

Informationen zu den Sicherheitsparametern, die in die JDBC-Verbindung für eine sichere Datenbank aufgenommen werden müssen, finden Sie unter [“Verbindungszeichenfolge für eine sichere Datenbank” auf Seite 105](#).

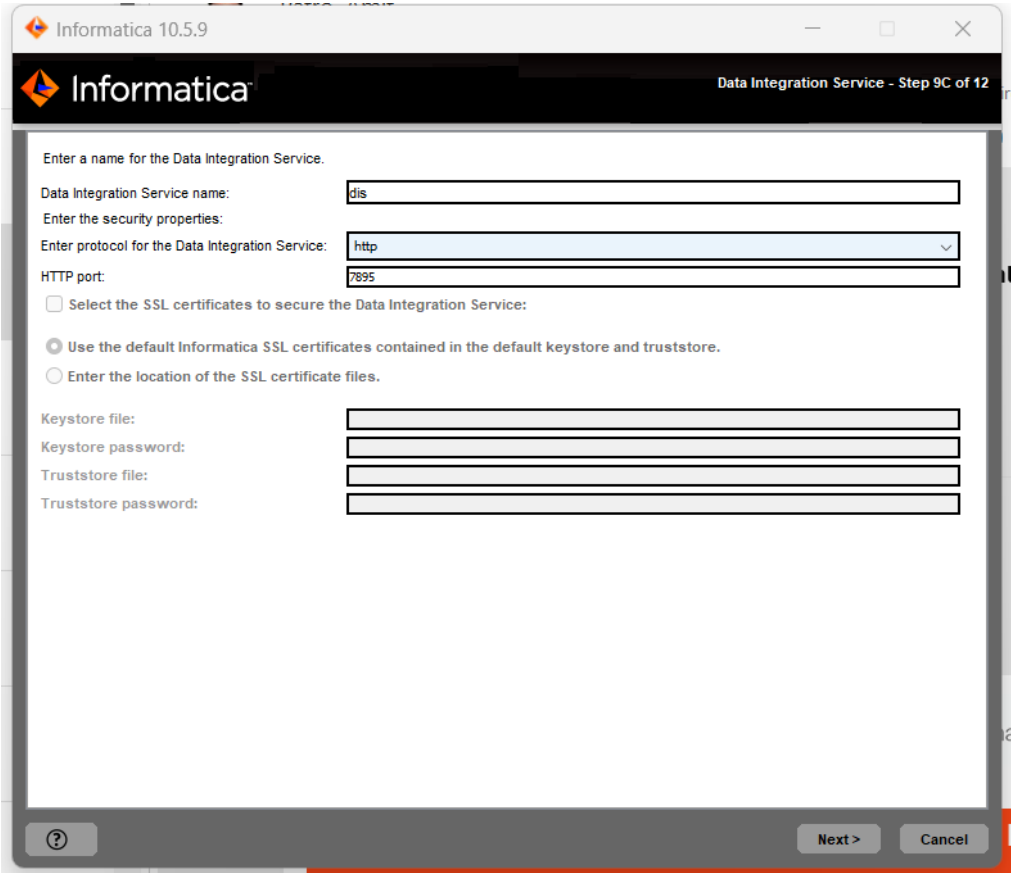
4. Klicken Sie auf **Verbindung testen**, um zu überprüfen, ob Sie eine Verbindung zur Datenbank herstellen können, und anschließend auf **OK**, um fortzufahren.
5. Klicken Sie auf **Weiter**.

Der Abschnitt **Serviceparameter** wird angezeigt.

Datenintegrationsdienst

Nachdem Sie die Modellrepository-Datenbank konfiguriert haben, können Sie die Dienstparameter für die Anwendungsdienste konfigurieren.

- 1. Konfigurieren Sie auf der Seite **Datenintegrationsdienst** die Eigenschaften des Datenintegrationsdiensts.



In der folgenden Tabelle werden die einzurichtenden Dienstparameter beschrieben:

Port	Beschreibung
Name des Datenintegrationsdiensts	Der Name des Datenintegrationsdiensts, der in der Informatica-Domäne erstellt werden soll.
HTTP-Protokolltyp	Der Typ der Verbindung zum Datenintegrationsdienst. Wählen Sie eine der folgenden Optionen aus: <ul style="list-style-type: none">- HTTP. Für Anfragen an den Dienst wird eine HTTP-Verbindung verwendet.- HTTPS. Für Anfragen an den Dienst wird eine sichere HTTP-Verbindung verwendet.- HTTP&HTTPS. Für Anfragen an den Dienst kann eine HTTP- oder HTTPS-Verbindung verwendet werden.
HTTP-Port	Die Portnummer für den Datenintegrationsdienst. Der Standardwert ist 6030.

2. Geben Sie bei Auswahl einer HTTPS-Verbindung an, ob die SSL-Standardzertifikate von Informatica oder Ihre SSL-Zertifikate verwendet werden sollen, um eine sichere Verbindung zum Datenintegrationsdienst herzustellen.

In der folgenden Tabelle werden die SSL-Zertifikatsoptionen zum Sichern des Datenintegrationsdiensts beschrieben:

Option	Beschreibung
SSL-Standardzertifikatsdateien von Informatica verwenden	Verwenden Sie die von Informatica bereitgestellten SSL-Standardzertifikate. Hinweis: Wenn Sie kein SSL-Zertifikat bereitstellen, verwendet Informatica denselben privaten Standardschlüssel für alle Informatica-Installationen. Wenn Sie die standardmäßigen Schlüsselspeicherdateien und Truststore-Dateien von Informatica verwenden, ist die Sicherheit Ihrer Domäne unter Umständen gefährdet. Um ein hohes Maß an Sicherheit für die Domäne zu gewährleisten, wählen Sie die Option zum Angeben des Speicherorts der SSL-Zertifikatsdateien aus.
Speicherort der SSL-Zertifikatsdateien eingeben	Geben Sie den Pfad zur Schlüsselspeicher- und zur Truststore-Datei ein, die die SSL-Zertifikate enthalten.

Wenn Sie das Zertifikat bereitstellen, geben Sie den Speicherort und die Passwörter der Schlüsselspeicher- und der Truststore-Dateien an.

In der folgenden Tabelle werden die Parameter beschrieben, die für die SSL-Zertifikatsdateien eingegeben werden müssen:

Eigenschaft	Beschreibung
Schlüsselspeicherdatei	Obligatorisch. Pfad und Dateiname der Schlüsselspeicherdatei, die die privaten Schlüssel und SSL-Zertifikate für die Datenbank enthält.
Schlüsselspeicher-Passwort	Obligatorisch. Passwort der Schlüsselspeicherdatei für die gesicherte Datenbank.
Truststore-Datei	Obligatorisch. Pfad und Dateiname der Truststore-Datei, die den öffentlichen Schlüssel für die Datenbank enthält.
Truststore-Passwort	Obligatorisch. Passwort der Truststore-Datei für die gesicherte Datenbank.

3. Klicken Sie auf **Weiter**.

Das Installationsprogramm erstellt den Datenintegrationsdienst.

PowerCenter-Repository-Dienst und PowerCenter-Integrationsdienst

Sie können den PowerCenter-Repository-Dienst und den PowerCenter-Integrationsdienst konfigurieren.

- 1. Wenn Sie gewählt haben, während der Installation einen PowerCenter-Repository-Dienst und einen PowerCenter-Integrationsdienst zu erstellen, wird die Seite **PowerCenter-Repository-Dienst und PowerCenter-Integrationsdienst** geöffnet.

Informatica 10.5.9

PowerCenter Repository Service and the PowerCenter Integration Service - Step 11 of 12

Enter the required information to configure the PowerCenter Repository Service and the PowerCenter Integration Service.

Database type: Oracle

Database user ID: Satish14

Database user password: [masked]

Database service name for PowerCenter: orcl19c.informatica.com

PowerCenter Repository Service name: PCRS

PowerCenter Integration Service name: IS

Select PowerCenter Repository Service code page: UTF-8 encoding of Unicode

Select PowerCenter Integration Service code page: MS Windows Latin 1 (ANSI), superset of Latin1

Next > Cancel

- 2. Wählen Sie die Datenbank aus, die für das PowerCenter-Repository konfiguriert werden soll.
In der folgenden Tabelle werden die Datenbanken aufgelistet, die Sie für das PowerCenter-Repository konfigurieren können:

Eingabeaufforderung	Beschreibung
Datenbanktyp	Datenbanktyp für das PowerCenter-Repository. Wählen Sie eine der folgenden Optionen aus: 1 – Oracle 2 – Microsoft SQL Server 3 – IBM DB2 4 – Sybase ASE 5 – PostgreSQL

- 3. 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 für das Konto des Benutzers der PowerCenter-Repository-Datenbank.
Benutzerpasswort	Das Passwort für das PowerCenter-Datenbankbenutzerkonto.
Datenbankdienstname	Dienst- oder Datenbankname für PowerCenter: <ul style="list-style-type: none">- Oracle: Geben Sie den Dienstnamen ein.- Microsoft SQL Server: Geben Sie den Datenbanknamen ein.- PostgreSQL: Geben Sie den Namen der Datenbank ein.
Hostname der Datenbank	Geben Sie die Datenbank des PowerCenter-Repositorys ein.

4. Geben Sie den Namen des zu erstellenden PowerCenter-Repository-Diensts ein.
5. Geben Sie den Namen des zu erstellenden PowerCenter-Integrationsdiensts ein.
6. Wählen Sie die Codepage des PowerCenter-Repository-Diensts aus. Der Standardwert ist 7-Bit-ASCII.
7. Wählen Sie die Codepage des PowerCenter-Integrationsdiensts aus. Der Standardwert ist 7-Bit-ASCII.
8. Klicken Sie auf **Weiter**.
9. Klicken Sie zum Beenden des Installationsprogramms auf **Fertig**.

Das Installationsprogramm erstellt den PowerCenter-Repository-Dienst sowie den PowerCenter-Integrationsdienst und startet die Dienste.

In der **Installationsübersicht** wird angezeigt, ob die Installation erfolgreich abgeschlossen wurde. Die Übersicht zeigt außerdem den Status der installierten Komponenten und ihre Konfiguration an.

In der **Installationsübersicht** wird angezeigt, ob die Installation erfolgreich abgeschlossen wurde. Der Bericht zeigt außerdem den Status der installierten Komponenten und deren Konfiguration an.

KAPITEL 10

Ausführen des automatischen Installationsprogramms

Dieses Kapitel umfasst die folgenden Themen:

- [Automatische Installation, 257](#)
- [Verschlüsseln von Passwörtern in der Eigenschaftendatei, 259](#)

Automatische Installation

Verwenden Sie den automatischen Modus, um ohne Benutzereingriff zu installieren. Geben Sie die Installationsoptionen mithilfe einer Eigenschaftendatei an. Das Installationsprogramm liest die Datei, um die Installationsoptionen zu ermitteln. Mit der automatischen Installation können Sie die Dienste auf mehreren Computern im Netzwerk installieren oder die Installation auf den verschiedenen Computern standardisieren.

Kopieren Sie die Installationsdateien auf die Festplatte des Computers, auf dem Sie die Dienste installieren möchten. Stellen Sie bei der Installation auf einem Remotecomputer sicher, dass Sie darauf zugreifen und Dateien erstellen können.

Gehen Sie für die automatische Installation wie folgt vor:

1. Führen Sie das Dienstprogramm zur Passwortverschlüsselung aus, um die Passwörter in der Installationseigenschaftendatei zu verschlüsseln.
2. Konfigurieren Sie die Installationseigenschaftendatei und geben Sie darin die Installationsoptionen an.
3. Führen Sie das Installationsprogramm mit der Installationseigenschaftendatei aus.

Konfigurieren der Eigenschaftendatei

Konfigurieren Sie die Eigenschaftendatei, die die Konfigurationseigenschaften enthält, die für die Installation der Informatica-Dienste im automatischen Modus erforderlich sind.

Informatica stellt zwei Versionen der Eigenschaftendatei bereit. Sie können eine der beiden Dateien verwenden, um die Optionen für Ihre Installation anzugeben.

Eigenschaftendatei für die automatische Eingabe

Konfigurieren Sie die Eigenschaftendatei für die automatische Eingabe, die die Konfigurationseigenschaften enthält, die für die Installation der Informatica-Dienste im automatischen Modus erforderlich sind. Verwenden Sie die Datei, wenn Sie den entsprechenden Wert für jede Eigenschaft in der Datei festlegen möchten.

Standardmäßige Eigenschaftendatei für die automatische Eingabe

Die standardmäßige Eigenschaftendatei für die automatische Eingabe enthält Standardwerte für viele Konfigurationseigenschaften. Die Eigenschaften sind im unteren Teil der Datei aufgeführt. Verwenden Sie die Datei, wenn Sie planen, die Informatica-Dienste mit den Standardeigenschaftswerten zu installieren.

Die Datei enthält Eigenschaften, die bei den folgenden Optionen auf den Standardwert festgelegt sind:

- Anwendungsdienstnamen.
- Secure Sockets Layer-Authentifizierung.
- Kerberos-Authentifizierung.
- Portnummernzuweisung für Domänen- und Knotenkomponenten.

Um die Eigenschaftendatei zu konfigurieren, die die Konfigurationseigenschaften enthält, die für die Installation der Informatica-Dienste im automatischen Modus erforderlich sind, führen Sie die folgenden Schritte aus:

1. Wechseln Sie zum Root-Verzeichnis, das die Installationsdateien enthält.
2. Führen Sie optional das Dienstprogramm zur Passwortverschlüsselung aus, um Passwörter in der `.properties`-Datei zu verschlüsseln.
3. Erstellen Sie eine Sicherungskopie der Datei `SilentInput.properties`.
4. Öffnen Sie entweder die Datei `SilentInput.properties` oder die Datei `SilentInput_Default.properties`.
5. Konfigurieren Sie die Eigenschaften in der Datei.
6. Speichern Sie die Datei unter dem Namen `SilentInput.properties`.

Ausführen des Installationsprogramms

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

1. Öffnen Sie die Eingabeaufforderung.
2. Wechseln Sie zum Root-Verzeichnis, das die Installationsdateien enthält.
3. Stellen Sie sicher, dass das Verzeichnis die Datei `SilentInput.properties` enthält, die Sie bearbeitet und erneut gespeichert haben.
4. Führen Sie die automatische Installation aus. Führen Sie unter Linux `silentInstall.sh` aus.

Die automatische Installation wird im Hintergrund ausgeführt. Der Vorgang kann eine Weile dauern. Die automatische Installation ist abgeschlossen, wenn die Datei `Informatica_<Version>_Services_InstallLog<timestamp>.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.

Verschlüsseln von Passwörtern in der Eigenschaftendatei

Das Installationsprogramm enthält ein Dienstprogramm, mit dem Sie Passwörter verschlüsseln können, die Sie in der Eigenschaftendatei festlegen. Diese Datei wird zur Angabe von Optionen genutzt, wenn Sie das Installationsprogramm im automatischen Modus ausführen. Informatica verwendet die AES-Verschlüsselung mit mehreren 256-Bit-Schlüsseln, um Passwörter zu verschlüsseln.

Sie führen das Dienstprogramm für jedes Passwort aus, das Sie verschlüsseln möchten. Wenn Sie das Dienstprogramm ausführen, geben Sie den Wert des Passworts in Klartext an der Eingabeaufforderung an. Das Dienstprogramm generiert das Passwort im verschlüsselten Format als Ausgabe. Die Ausgabe enthält das folgende Präfix: `=INSTALLER:CIPHER:AES:256=`

Kopieren Sie die komplette Ausgabezeichenfolge, einschließlich des Präfixes, und fügen Sie sie dann in die Eigenschaftendatei als Wert für die Passworteigenschaft ein. Wenn Sie das Installationsprogramm im automatischen Modus ausführen, entschlüsselt das Installationsframework das Passwort.

1. Wechseln Sie zum Dienstprogrammverzeichnis:

```
<Installationsprogrammverzeichnis>/properties/utils/passwd_encryption
```

2. Führen Sie das Dienstprogramm aus. Geben Sie das Klartextpasswort an, das Sie als Wert für `<Passwort>` verschlüsseln möchten.

- Führen Sie unter Linux und UNIX den folgenden Befehl aus:

```
sh install.sh <Passwort>
```

- Führen Sie unter Windows den folgenden Befehl aus:

```
install.bat <Passwort>
```

3. Kopieren Sie die Zeichenfolge des verschlüsselten Passworts aus der Ausgabe und fügen Sie sie dann in die `.properties`-Datei als Wert für das entsprechende Passwort ein.

Das folgende Beispiel zeigt das verschlüsselte Passwort, das als Wert für die Eigenschaft `DOMAIN_PSSWD` festgelegt wurde:

```
DOMAIN_PSSWD==INSTALLER:CIPHER:AES:256=mjkjmDR2kzFJiizfRWIOPg==
```

KAPITEL 11

Fehlerbehebung

Dieses Kapitel umfasst die folgenden Themen:

- [Behebung von Problemen bei der Installation - Übersicht, 260](#)
- [Fortsetzen eines fehlgeschlagenen Installationsprogrammprozesses, 260](#)
- [Fehlerbehebung bei Installationsprotokolldateien, 262](#)
- [Fehlerbehebung von Domänen und Knoten, 263](#)
- [Fehlerbehebung bei Informatica Developer, 265](#)

Behebung von Problemen bei der Installation - Übersicht

Die Themen in diesem Abschnitt enthalten Informationen zur Fehlerbehebung bei möglichen Problemen, die während der Installation von Informatica auftreten können. Die Beispiele in diesen Themen beschreiben allgemeine Strategien zur Fehlerbehebung und stellen keine vollständige Liste der möglichen Ursachen von Installationsproblemen dar.

Fortsetzen eines fehlgeschlagenen Installationsprogrammprozesses

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

Wenn der Dienstinstallationsvorgang unter UNIX oder Linux fehlschlägt, können Sie die vorherige Dienstkonfiguration fortsetzen und die zuletzt eingegebenen Details für diese Dienstinstallation wiederherstellen. Der Installationsvorgang kann aus Gründen wie Netzwerkausfall, beim Beenden der Installation vor Abschluss des gesamten Installationsvorgangs oder aufgrund falsch eingegebener Informationen fehlschlagen.

Beachten Sie die folgenden Richtlinien für die Fortsetzung der Installation:

Sie können das Installationsprogramm fortsetzen

Wenn ein Dienst ausfällt oder beim Installationsprozess während einer Diensterstellung ein Fehler auftritt, können Sie den Installationsprozess über das Installationsprogramm des Servers fortsetzen. Stellen Sie zum Fortsetzen des Installationsvorgangs anhand des Installationsprotokolls sicher, dass

mindestens einer der Dienste erstellt wurde und dass die Domäne in Betrieb ist und läuft. Wenn Sie beispielsweise überprüfen möchten, ob der Modellrepository-Dienst erstellt wurde, schauen Sie im Serverprotokoll nach, ob ein Eintrag über das erfolgreiche Erstellen des Diensts im folgenden Format vorliegt:

```
SUCCESS: MRS Service [mrs_name] wird erstellt. Befehl wurde erfolgreich ausgeführt.
```

Um die Installation fortzusetzen, führen Sie das Installationsprogramm erneut aus.

Wenn Sie das Installationsprogramm fortsetzen, während Sie einen Dienst erstellen, werden alle dienst- und datenbankspezifischen Informationen, z. B. der Status in Bezug auf das Erstellen des Diensts, der Dienstname, der Status, ob der Dienst aktiviert oder deaktiviert ist, beibehalten. Sie können die zuvor eingegebenen Werte bestätigen und verwenden oder neue Werte für den Dienst angeben und den Installationsvorgang fortsetzen.

Sie können das Installationsprogramm nicht fortsetzen

Sie können das Installationsprogramm in folgenden Situationen nicht fortsetzen:

- Sie führen das Installationsprogramm aus, um Dienste zu konfigurieren, nachdem die Dienste erstellt wurden.
- Sie führen den Assistenten zur Dienstkonfiguration aus.
- Sie treten einer Domäne bei.

Vor dem Fortsetzen des Installationsprogramms

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:

1. Überprüfen Sie in der im Installationsverzeichnis befindlichen Installationsprotokolldatei, ob mindestens die Domäne und ein Dienst erstellt wurden. Der Name der Installationsprotokolldatei hat folgende Syntax: Informatica_<Version>_Services_<Zeitstempel>.log
2. Stellen Sie sicher, dass Sie die ObjektdateninstallInst.obj nicht löschen, die sich im Tools-Ordner des Benutzerinstallationsverzeichnisses befindet.
3. Falls Sie den Installationsvorgang über das automatische Installationsprogramm fortsetzen, stellen Sie sicher, dass RESUME_INSTALLATION in der Datei SilentInput.properties auf true gesetzt ist.

Fortsetzung des Installationsprogramms

Nachdem Sie die Vorinstallationsaufgaben abgeschlossen haben, können Sie das Installationsprogramm fortsetzen.

1. Öffnen Sie eine Eingabeaufforderung und navigieren Sie zum Speicherort der Installationsdateien.
2. Führen Sie das Konsoleninstallationsprogramm oder das automatische Installationsprogramm aus.
3. Wenn das reguläre Installationsprogramm ausgeführt wird, werden Sie möglicherweise gefragt, ob Sie das vorherige Installationsprogramm fortsetzen möchten oder nicht.
 - Wenn Sie die Installation nicht fortsetzen möchten, geben Sie 1 für „Nein“ ein. Der Standardwert ist 1.
 - Wenn Sie die Installation fortsetzen möchten, geben Sie 2 für „Ja“ ein.

Bevor Sie die Installation fortsetzen können, werden die Dienste validiert.

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.

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.

In der nachstehenden Tabelle sind die Eigenschaften der Debug-Protokolldatei beschrieben:

Eigenschaft	Beschreibung
Name der Protokolldatei	<ul style="list-style-type: none">- Informatica_<Version>_Services_<Zeitstempel>.log- Informatica_<Version>_Client_<Zeitstempel>.log- Informatica_<Version>_Services_Upgrade_<Zeitstempel>.log- Informatica_<Version>_Client_Upgrade_<Zeitstempel>.log
Speicherort	Installationsverzeichnis.
Verwendung	Weitere 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.

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 Protokolldatei	<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.

Protokolldateien des Dienstmanagers

Das Installationsprogramm startet den Informatica-Dienst. Der Informatica-Dienst startet den Dienstmanager für den Knoten. Der Dienstmanager erzeugt 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 Protokolldateien des Dienstmanagers werden auf jedem Knoten erstellt.

In der nachstehenden Tabelle werden die vom Dienstmanager erzeugten Dateien beschrieben:

Eigenschaft	Beschreibung
catalina.out	<p>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 Dienstmanagers in Gebrauch. In diesem Protokoll finden Sie weitere Informationen dazu, welcher Port während des Starts des Dienstmanagers nicht verfügbar war.</p> <p>Die catalina.out-Datei befindet sich im folgenden Verzeichnis: <Informatica-Installationsverzeichnis>/logs/< Knotenname>/catalina.out</p>
node.log	<p>Zeichnet Ereignisse auf, die während des Starts des Dienstmanagers 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 Dienstmanagers fehl. Die Datei node.log befindet sich im Verzeichnis /tomcat/logs.</p>

Hinweis: Der Dienstmanager verwendet die Datei „node.log“ außerdem zum Aufzeichnen von Ereignissen, bei denen der Protokollmanager nicht verfügbar ist. Beispiel: Wenn der Computer, auf dem der Dienstmanager ausgeführt wird, nicht über genügend Speicherplatz zum Schreiben von Protokollereignisdateien verfügt, ist der Protokollmanager 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.

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. Sie brauchen ODBC oder die native Konnektivität auf dem Rechner, auf dem Sie die Informatica-Dienste installieren, 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 Erstellungsberechtigung in der Datenbank verfügen. Jede Domäne muss über ein separates Domänenkonfigurations-Repository verfügen.

Erstellen oder Anfügen einer Domäne

Je nachdem, ob Sie eine Domäne erstellen oder anfügen, führt das Installationsprogramm unterschiedliche Aufgaben durch.

- **Erstellen einer Domäne** Das Installationsprogramm führt auf dem aktuellen Rechner den Befehl `infasetup DefineDomain` aus, um die Domäne und den Gateway-Knoten für die Domäne entsprechend den im Fenster „Domäne konfigurieren“ eingegebenen Daten zu erstellen.
- **Anfügen einer Domäne** Das Installationsprogramm führt den Befehl `infasetup DefineWorkerNode` zum Erstellen eines Knotens auf dem aktuellen Rechner und den Befehl `infacmd AddDomainNode` zum Hinzufügen des Knotens zur Domäne aus. Die im Fenster „Domäne konfigurieren“ 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 ist und der Hostname richtig ist, und wiederholen Sie den Vorgang.

Wenn der Befehl `AddDomainNode` fehlschlägt, überprüfen Sie, ob der Informatica-Dienst auf dem Knoten ausgeführt wird, und wiederholen Sie den Vorgang.

Starten von Informatica

Das Installationsprogramm führt `infaservice` aus, um die Informatica-Dienste zu starten. Wenn sich Informatica nicht starten lässt, verwenden Sie die Informationen im Informatica-Debug-Log, um Fehler zu beheben, und die Protokolldateien `node.log` und `catalina.out` des Dienstmanagers, um die Ursache des Fehlers zu identifizieren.

Wenn Sie eine Domäne erstellen, melden Sie sich bei Informatica Administrator an, nachdem der Informatica-Dienst die Verfügbarkeit der Domäne überprüft hat. Wenn Sie eine Domäne anfügen, melden Sie sich bei Informatica Administrator an, nachdem der Informatica-Dienst geprüft hat, ob der Knoten erfolgreich erstellt und gestartet wurde.

Wenn sich Informatica nicht starten lässt, kann das die folgenden Ursachen haben:

- **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. Setzen Sie die Umgebungsvariable `INFA_JAVA_OPTS`, um die Größe des von Informatica verwendeten Systemspeichers zu konfigurieren. Unter UNIX können Sie die Speicherkonfiguration beim Starten von Informatica festlegen.

- **Die Domänenkonfigurationsdatenbank ist nicht verfügbar.** Informatica 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.

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 Informatica auf dem Gateway-Knoten.

Hinzufügen einer Lizenz

Das Installationsprogramm führt den Befehl *infacmd AddLicense* aus, mit dem die Informatica-Lizenzschlüsseldatei gelesen und ein Lizenzobjekt in der Domäne erstellt wird. Zum Ausführen der Anwendungsdienste in Informatica Administrator muss in der Domäne ein gültiges Lizenzobjekt vorliegen.

Wenn Sie eine inkrementelle Lizenz verwenden und eine Domäne anfügen, muss die Seriennummer der inkrementellen Lizenz mit der Seriennummer eines vorhandenen Lizenzobjekts in der Domäne übereinstimmen. Stimmen die Seriennummern nicht überein, schlägt der Befehl *AddLicense* fehl.

Weitere Informationen zum Inhalt der für die Installation verwendeten Lizenzschlüsseldatei einschließlich Seriennummer, Version, Ablaufdatum, Betriebssystemen und Konnektivitätsoptionen finden Sie im Installations-Debug-Log. In Informatica Administrator finden Sie weitere Informationen zu vorhandenen Lizenzen für die Domäne.

Fehlerbehebung bei Informatica Developer

Beachten Sie die folgenden Tipps, wenn Sie mit Informatica Developer arbeiten:

Informatica Developer kann nicht gestartet werden

Dieses Problem kann auftreten, wenn die *jvm.dll* von Java die *MSVCR100.dll* erfordert.

Um dieses Problem zu beheben, laden Sie das Microsoft Visual C++ Studio 2010 Redistributable Package von der Microsoft-Website herunter.

Teil IV: Nach der Installation der Dienste

Dieser Teil enthält die folgenden Kapitel:

- [Durchführen der Domänenkonfiguration, 267](#)
- [Vorbereiten zum Erstellen der Anwendungsdienste, 273](#)
- [Erstellen und Konfigurieren von Anwendungsdiensten, 283](#)

KAPITEL 12

Durchführen der Domänenkonfiguration

Dieses Kapitel umfasst die folgenden Themen:

- [Checkliste zum Abschließen der Domänenkonfiguration, 267](#)
- [Durchführen der Domänenkonfiguration - Übersicht, 268](#)
- [Überprüfen der Gebietsschemaeinstellungen und der Codepage-Kompatibilität, 268](#)
- [Konfigurieren von Umgebungsvariablen unter UNIX oder Linux, 269](#)

Checkliste zum Abschließen der Domänenkonfiguration

Dieses Kapitel enthält Informationen über Aufgaben zur Domänenkonfiguration, die Sie nach der Installation ausführen müssen. Verwenden Sie diese Checkliste zur Überwachung der Aufgaben zur Domänenkonfiguration.

☐ Überprüfen der Gebietsschemaeinstellungen und der Codepage-Kompatibilität:

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

☐ Konfigurieren der folgenden Umgebungsvariablen:

- Informatica-Umgebungsvariablen zum Speichern der Einstellungen für Speicherplatz, Domänen und Speicherort.
- Bibliothekspfad-Umgebungsvariablen auf den Computern, auf denen der Datenintegrationsdienst ausgeführt wird.
- Kerberos-Umgebungsvariablen, wenn Sie die Informatica-Domäne so konfigurieren, dass sie in einem Netzwerk mit Kerberos-Authentifizierung ausgeführt wird.

Durchführen der Domänenkonfiguration - Übersicht

Nach der Installation der Informatica-Dienste und vor dem Erstellen der Anwendungsdienste führen Sie die Konfiguration für die Domänen-Dienste durch.

Zu den Aufgaben der Domänenkonfiguration gehören das Überprüfen der Codepages, das Konfigurieren der Umgebungsvariablen für die Domäne und das Konfigurieren der Firewall.

Überprüfen der Gebietsschemaeinstellungen und der Codepage-Kompatibilität

Die Codepages für Anwendungsdienste müssen mit den Codepages in der Domäne kompatibel sein.

Überprüfen und konfigurieren Sie die Gebietsschemaeinstellungen und Codepages:

Stellen Sie sicher, dass die Domänen-Konfigurationsdatenbank mit den Codeseiten der Anwendungsdienste, die Sie in der Domäne erstellen, kompatibel ist.

Der Dienstmanager synchronisiert die Liste der Benutzer in der Domäne mit der Liste der Benutzer und Gruppen in allen Anwendungsdiensten. Wenn ein Benutzername in der Domäne Zeichen enthält, die die Codepage des Anwendungsdiensts nicht erkennt, werden diese Zeichen nicht ordnungsgemäß umgewandelt, was zu Inkonsistenzen führt.

Stellen Sie sicher, dass die Gebietsschemaeinstellungen auf Computern mit Zugriff auf das Administrator-Tool und die Informatica-Client-Tools mit den Codepages der Repositories in der Domäne kompatibel sind.

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

Konfigurieren der Gebietsschema-Umgebungsvariablen

Stellen Sie sicher, dass die Gebietsschemaeinstellung mit der Codepage für das Repository kompatibel ist. Ist die Gebietsschemaeinstellung nicht mit der Codepage für das Repository kompatibel, kann kein Anwendungsdienst erstellt werden.

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

Für unterschiedliche Betriebssysteme sind unterschiedliche Werte für ein und dasselbe Gebietsschema erforderlich. Beim Wert für die Gebietsschemavariablen muss auf Groß- und Kleinschreibung geachtet werden.

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 unter Betriebssystemen installierten Sprachen und die vorhandenen Gebietsschemaeinstellungen zurück.

Richten Sie die folgenden Gebietsschema-Umgebungsvariablen ein:

Gebietsschema unter Linux

Zu allen UNIX-Betriebssystemen mit Ausnahme von Linux gibt es zu jedem Gebietsschema einen einmaligen Wert. Unter Linux können unterschiedliche Werte dasselbe Gebietsschema darstellen. So

stellen beispielsweise "utf8," "UTF-8," "UTF8" und "utf-8" auf einem Linux-Rechner ein und dasselbe Gebietsschema dar. Für Informatica müssen Sie einen speziellen Wert für jedes Gebietsschema auf einem Linux-Rechner verwenden. Achten Sie darauf, die Umgebungsvariable LANG entsprechend auf allen Linux-Rechnern einzustellen.

Gebietsschema für Oracle-Datenbank-Clients

Stellen Sie NLS_LANG bei Oracle-Datenbank-Clients auf das Gebietsschema ein, das der Datenbank-Client und -Server bei der Anmeldung verwenden soll. Eine Gebietsschemaeinstellung besteht aus der Sprache, der Region und dem Zeichensatz. Der Wert von NLS_LANG hängt von der Konfiguration ab.

Wenn der Wert beispielsweise american_america.UTF8 lautet, legen Sie die Variable mit dem folgenden Befehl in einer C-Shell fest:

```
setenv NLS_LANG american_america.UTF8
```

Um Multibyte-Zeichen in der Datenbank zu lesen, legen Sie die Variable mit dem folgenden Befehl fest:

```
setenv NLS_LANG=american_america.AL32UTF8
```

Sie müssen die richtige Variable auf dem Rechner des Datenintegrationsdiensts festlegen, damit der Datenintegrationsdienst die Oracle-Daten korrekt lesen kann.

Konfigurieren von Umgebungsvariablen unter UNIX oder Linux

Informatica verwendet Umgebungsvariablen zum Speichern von Konfigurationsinformationen bei der Ausführung der Anwendungsdienste und beim Herstellen einer Verbindung zu den Clients. 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.

Melden Sie sich zum Konfigurieren von Umgebungsvariablen mit dem Systembenutzerkonto an, mit dem Sie Informatica installiert haben.

Konfigurieren der Informatica-Umgebungsvariablen

Sie können Informatica-Umgebungsvariablen zum Speichern von Speicher-, Domänen- und Speicherorteinstellungen konfigurieren.

Richten Sie die folgenden Umgebungsvariablen ein:

INFA_JAVA_OPTS

Standardmäßig verwendet Informatica maximal 512 MB Systemspeicher.

Die folgende Tabelle listet die Minimalanforderungen für die maximalen Heap-Größeneinstellungen auf, basierend auf der Anzahl der Benutzer und Dienste in der Domäne:

Anzahl der Domänenbenutzernamen	Maximale Heap-Größe (1-5 Dienste)	Maximale Heap-Größe (6-10 Dienste)
Bis zu 1.000	512 MB (Standard)	1024 MB
5,000	2048 MB	3072 MB
10,000	3072 MB	5120 MB
20,000	5120 MB	6144 MB
30,000	5120 MB	6144 MB

Hinweis: Die Einstellungen für die maximale Heap-Größe in der Tabelle basieren auf der Anzahl der Anwendungsdienste in der Domäne.

Wenn die Domäne mehr als 1.000 Benutzer hat, aktualisieren Sie die maximale Heap-Größe basierend auf der Anzahl der Benutzer in der Domäne.

Sie können die Umgebungsvariable `INFA_JAVA_OPTS` verwenden, um die Größe des von Informatica verwendeten Systemspeichers zu konfigurieren. Um zum Beispiel 1 GB Systemspeicher für den Informatica-Daemon 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 Informatica-Installationsverzeichnis die Datei `domains.infa`. Die Datei `domains.infa` enthält die Konnektivitätsinformationen der Gateway-Knoten in einer Domäne, einschließlich 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 Variable `INFA_DOMAINS_FILE` auf dem Computer, auf dem Sie die Informatica-Dienste installieren.

INFA_HOME

Verwenden Sie `INFA_HOME`, um das Informatica-Installationsverzeichnis zu bestimmen. Wenn Sie die Informatica-Verzeichnisstruktur verändern, dann müssen Sie die Umgebungsvariable so setzen, dass sie auf den Speicherort des Informatica-Installationsverzeichnisses verweist oder auf das Verzeichnis, in dem sich die installierten Informatica-Dateien befinden.

Beispiel: Sie verwenden einen Softlink für alle Informatica-Verzeichnisse. Um `INFA_HOME` so zu konfigurieren, dass alle Informatica-Anwendungen und -Dienste die auszuführenden anderen Informatica-Komponenten finden, müssen Sie `INFA_HOME` so setzen, dass es auf das Informatica-Installationsverzeichnis verweist.

INFA_TRUSTSTORE

Wenn Sie sichere Kommunikation für die Domäne aktivieren, legen Sie die Variable `INFA_TRUSTSTORE` mit dem Verzeichnis fest, das die Truststore-Dateien für die SSL-Zertifikate enthält. Das Verzeichnis muss Truststore-Dateien namens `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 zum Verschlüsseln des Passworts das Befehlszeilenprogramm `pmpasswd`.

Konfigurieren von Bibliothekspfad-Umgebungsvariablen

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}"
Informix	<Datenbankpfad>/lib
Teradata	<Datenbankpfad>/lib
ODBC	<CLOSEDODBCHOME>/lib
PostgreSQL	\$PGHOME/lib:\${LD_LIBRARY_PATH}

Konfigurieren der Kerberos-Umgebungsvariablen

Wenn Sie die Informatica-Domäne zur Ausführung in einem Netzwerk mit Kerberos-Authentifizierung konfigurieren, müssen Sie die Umgebungsvariablen für die Kerberos-Konfiguration und den Zugangsdaten-Cache einrichten.

Richten Sie die folgenden Umgebungsvariablen ein:

KRB5_CONFIG

Verwenden Sie die Umgebungsvariable `KRB5_CONFIG`, um den Pfad und Dateinamen der Kerberos-Konfigurationsdatei zu speichern. Der Name der Kerberos-Konfigurationsdatei lautet `krb5.conf`. Sie müssen die Umgebungsvariable `KRB5_CONFIG` auf jedem Knoten in der Informatica-Domäne einrichten.

KRB5CCNAME

Richten Sie die Umgebungsvariable `KRB5CCNAME` mit dem Pfad und Dateinamen des Kerberos-Benutzerzugangsdaten-Cache ein. Kerberos-SSO (Single Sign-On, einmalige Anmeldung) erfordert einen Kerberos-Zugangsdaten-Cache für Benutzerkonten.

Wenn Sie die Benutzerzugangsdaten zwischenspeichern, müssen Sie die Option *Weiterleitbar* verwenden. Wenn Sie beispielsweise mithilfe von *kinit* Benutzerzugangsdaten abrufen und zwischenspeichern, müssen Sie die Option *-f* zum Anfordern weiterleitbarer Tickets verwenden.

KAPITEL 13

Vorbereiten zum Erstellen der Anwendungsdienste

Dieses Kapitel umfasst die folgenden Themen:

- [Checkliste zum Vorbereiten der Erstellung von Anwendungsdiensten, 273](#)
- [Erstellen von Verzeichnissen für den Analyst-Dienst, 274](#)
- [Erstellen eines Schlüsselspeichers für eine sichere Verbindung zu einem Web-Anwendungsdienst, 274](#)
- [Anmelden Sie bei Informatica Administrator, 275](#)
- [Erstellen von Verbindungen, 276](#)

Checkliste zum Vorbereiten der Erstellung von Anwendungsdiensten

Dieses Kapitel enthält Aufgaben, die Sie vor der Erstellung oder Konfiguration des Analyst-Diensts, Datenintegrationsdiensts und Content-Management-Diensts ausführen müssen. Bei der Konfiguration der Dienste konfigurieren Sie Eigenschaften abhängig von den Verbindungen und Verzeichnissen, die Sie erstellen. Verwenden Sie diese Checkliste zur Überwachung der Konfigurationsaufgaben.

☐ Erstellen der folgenden Verzeichnisse für den Analyst-Dienst:

- Einfachdatei-Caches
- Temporäre Business-Glossar-Dateien
- Glossarobjekte

☐ Erstellen der folgenden Verbindungen für den Datenintegrationsdienst:

- Datenobjekt-Cache-Datenbank
- Arbeitsablauf-Datenbank
- Profiling-Warehouse

☐ Erstellen der folgenden Verbindungen für den Content-Management-Dienst:

- Referenzdaten-Warehouse

Erstellen von Verzeichnissen für den Analyst-Dienst

Vor dem Erstellen des Analyst-Diensts müssen Sie Verzeichnisse für das Analyst Tool zum Speichern temporärer Dateien erstellen.

Erstellen Sie die folgenden Verzeichnisse auf dem Knoten, auf dem der Analyst-Dienst ausgeführt wird:

Verzeichnis des Einfachdatei-Cache

Erstellen Sie ein Verzeichnis für den Einfachdatei-Cache, in dem das Analyst Tool hochgeladene Einfachdateien speichert. Der Datenintegrationsdienst muss auch in der Lage sein, auf dieses Verzeichnis zuzugreifen. Wenn der Analyst-Dienst und der Datenintegrationsdienst auf verschiedenen Knoten ausgeführt werden, konfigurieren Sie das Einfachdateiverzeichnis zur Verwendung eines freigegebenen Verzeichnisses. Wenn der Datenintegrationsdienst auf primären und Backup-Knoten oder auf einem Gitter läuft, muss jeder Prozess des Datenintegrationsdiensts auf die Dateien im freigegebenen Verzeichnis zugreifen können.

Sie können beispielsweise ein Verzeichnis namens „flatfilecache“ auf dem folgenden zugeordneten Laufwerk erstellen, auf das alle Analyst-Dienst- und Datenintegrationsdienstprozesse zugreifen können:

```
F:\shared\<Informatica installation directory>\server
```

Wenn Sie eine Referenztabelle oder eine Einfachdatei-Quelle importieren, verwendet das Analyst Tool die Dateien aus diesem Verzeichnis, um eine Referenztabelle oder ein Einfachdatei-Datenobjekt zu erstellen.

Temporäres Verzeichnis für Exportdateien

Erstellen Sie ein Verzeichnis zum Speichern der temporären Unternehmensglossardateien, die der Unternehmensglossar-Exportprozess erstellt. Erstellen Sie das Verzeichnis auf dem Knoten, auf dem der Analyst-Dienst ausgeführt wird.

Beispiel: Sie können ein Verzeichnis namens "exportfiledirectory" an dem folgenden Speicherort erstellen: <Informatica-Installationsverzeichnis>/server

Verzeichnis für Objekthänge

Erstellen Sie ein Verzeichnis, um die Dateien zu speichern, die von Content-Managern als Anhänge zu Glossarobjekten hinzugefügt werden können. Erstellen Sie das Verzeichnis auf dem Knoten, auf dem der Analyst-Dienst ausgeführt wird.

Beispiel: Sie können ein Verzeichnis namens "attachmentdirectory" an dem folgenden Speicherort erstellen: <Informatica-Installationsverzeichnis>/server.

Erstellen eines Schlüsselspeichers für eine sichere Verbindung zu einem Web-Anwendungsdienst

Sie können eine sichere Verbindung zwischen der Informatica-Domäne und einem Web-Anwendungsdienst wie Analyst-Dienst herstellen. Informatica verwendet das SSL/TLS-Protokoll zum Verschlüsseln von Netzwerkverkehr. Um die Verbindung zu sichern, müssen Sie die erforderlichen Dateien erstellen.

Bevor Sie die Verbindung zu einem Web-Anwendungsdienst sichern, überprüfen Sie, ob die folgenden Anforderungen erfüllt sind:

Sie haben eine Zertifikatssignieranfrage und einen privaten Schlüssel erstellt.

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

Beachten Sie, dass für die RSA-Verschlüsselung mehr als 512 Bit erforderlich sind.

Sie haben ein signiertes SSL-Zertifikat.

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

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

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

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

Der Schlüsselspeicher befindet sich in einem Verzeichnis, auf das zugegriffen werden kann.

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

Anmelden Sie bei Informatica Administrator

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

Wenn die Informatica-Domäne in einem Netzwerk mit Kerberos-Authentifizierung ausgeführt wird, müssen Sie den Browser so konfigurieren, dass der Zugriff auf die Informatica-Webanwendungen möglich ist. Fügen Sie in Microsoft Internet Explorer, Microsoft Edge und Google Chrome die URL der Informatica-Webanwendung zur Liste der vertrauenswürdigen Sites hinzu. Fügen Sie in Safari das Zertifikat der Informatica-Webanwendung zum Schlüsselbund hinzu. Wenn Sie Chrome Version 86.0.42x oder höher unter Windows verwenden, müssen Sie auch die Richtlinien `AuthServerWhitelist` und `AuthNegotiateDelegateWhitelist` festlegen.

1. Starten Sie Microsoft Internet Explorer oder Google Chrome.
2. Geben Sie in der **Adresszeile** die URL für das Administrator-Tool ein:
 - Wenn das Administrator-Tool nicht für die Verwendung einer sicheren Verbindung konfiguriert wurde, geben Sie die folgende URL ein:

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

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

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

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

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

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

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

Fehlerbehebung bei der Anmeldung bei Informatica Administrator

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

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

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

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

Wenn nach Ihrer Anmeldung beim Administrator-Tool eine leere Seite angezeigt wird, überprüfen Sie, ob Sie die Delegierung für alle Benutzerkonten mit in der Informatica-Domäne verwendeten Dienstprinzipalen aktiviert haben. Zum Aktivieren der Delegierung legen Sie im Microsoft Active Directory Service die Option **Benutzer bei Delegierungen aller Dienste vertrauen (nur Kerberos)** für jedes Benutzerkonto fest, für das Sie einen SPN festgelegt haben.

Erstellen von Verbindungen

Erstellen Sie im Administrator Tool Verbindungen zu den Datenbanken, die die Anwendungsdienste verwenden. Sie müssen die Verbindungsdetails beim Konfigurieren des Anwendungsdiensts angeben.

Wenn Sie die Datenbankverbindung erstellen, geben Sie die Eigenschaften der Datenbankverbindung an, und testen Sie die Verbindung.

Die folgende Tabelle beschreibt die Datenbankverbindungen, die Sie erstellen müssen, bevor die Anwendungsdienste auf die zugehörigen Datenbanken zugreifen können.

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	<p>Zum Erstellen und Ausführen von Profilen und Scorecards erstellen Sie die Profiling-Warehouse-Datenbankverbindung für den Datenintegrationsdienst.</p> <p>Verwenden Sie diese Instanz des Datenintegrationsdiensts bei der Konfiguration der Laufzeiteigenschaften des Analyst-Diensts.</p> <p>Hinweis: Wenn Sie die Microsoft SQL Server-Datenbank als Profiling-Warehouse verwenden möchten, wählen Sie ODBC als Provider-Typ aus und deaktivieren Sie bei der Konfiguration der Microsoft SQL Server-Verbindung die Option DSN verwenden im Dialogfeld Microsoft SQL Server-Verbindungseigenschaften.</p>
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	Benutzername für die Datenbank
Passwort	Das Passwort für den Benutzernamen.
Verbindungszeichenfolge für den Metadatenzugriff	Die Verbindungszeichenfolge für das Importieren von physischen Datenobjekten. Verwenden Sie die folgende Verbindungszeichenfolge: jdbc:informatica:db2://<host>:50000;databaseName=<dbname>
Verbindungszeichenfolge für den Datenzugriff	Die Verbindungszeichenfolge für die Datenvorschau und das Ausführen von Zuordnungen. Geben Sie den dbname aus dem im DB2-Client konfigurierten Alias ein.
Codepage	Datenbank-Codepage
Umgebungs-SQL	Optional. Geben Sie die SQL-Befehle zum Einrichten der Datenbankumgebung ein, wenn Sie eine Verbindung zur Datenbank herstellen. Der Datenintegrationsdienst führt 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 Transaktionsumgebungs-SQL am Anfang jeder Transaktion aus.

Eigenschaft	Beschreibung
Wiederholungszeitraum	Diese Eigenschaft ist für die zukünftige Verwendung reserviert.
Tablespace	Tablespace-Name der DB2 für LUW-Datenbank.
SQL-Bezeichnerzeichen	Der Zeichentyp, der zur Kennzeichnung von Sonderzeichen und reservierten SQL-Schlüsselwörtern, wie WHERE, verwendet wird. Der Datenintegrationsdienst schließt mit dem ausgewählten Zeichen Sonderzeichen und reservierte SQL-Schlüsselwörter ein. Außerdem nutzt der Datenintegrationsdienst dieses Zeichen für die Eigenschaft „Bezeichner mit gemischter Groß-/Kleinschreibung unterstützen“.
Bezeichner mit gemischter Groß-/Kleinschreibung unterstützen	Sofern aktiviert, schließt der Datenintegrationsdienst Tabellen-, Ansichts-, Schema-, Synonym- und Spaltennamen in Bezeichnerzeichen ein, wenn SQL für diese Objekte in der Verbindung erzeugt und ausgeführt wird. Zu verwenden, wenn Objekte Namen mit gemischter Groß-/Kleinschreibung oder kleingeschriebene Namen haben. Diese Option ist standardmäßig deaktiviert.

Verbindungseigenschaften der Microsoft Azure SQL-Datenbank

Verwenden Sie eine Azure SQL Data Warehouse-Verbindung, um auf Tabellen in einer Microsoft Azure SQL-Datenbank zuzugreifen.

In der folgenden Tabelle werden die Verbindungseigenschaften der Microsoft Azure SQL-Datenbank beschrieben:

Eigenschaft	Beschreibung
Azure DW-JDBC-URL	Verbindungszeichenfolge für die Verbindung zur Microsoft Azure SQL-Datenbank.
Azure DW-JDBC-Benutzername	Benutzername für die Datenbank.
Azure DW-JDBC-Passwort	Das Passwort für den Benutzernamen.
Azure DW-JDBC-Schemaname	Name des Schemas in der Datenbank.
Azure-Speichertyp	
Azure Blob-Kontoname	
Azure Blob-Kontoschlüssel	
Name des ADLS Gen2-Speicherkontos	
Schlüssel des ADLS Gen2-Kontos	
Blob-Endpunkt	
VNet-Regel	

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 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
Eigentümername	Der Name des Eigentümers des Schemas. Geben Sie ihn für die Verbindungen zur Profiling Warehouse-Datenbank oder zur Datenobjekt-Cache-Datenbank an.
Schemaname	Der Name des Schemas in der Datenbank. Geben Sie ihn für die Verbindungen zum Profiling Warehouse oder zur Datenobjekt-Cache-Datenbank an. Sie müssen den Schemanamen für das Profiling Warehouse angeben, wenn der Schemaname anders lautet als der Benutzername der Datenbank. Sie müssen den Schemanamen für die Datenobjekt-Cache-Datenbank angeben, wenn der Schemaname anders lautet als der Benutzername für die Datenbank und Sie den Cache mit einem externen Tool verwalten.
Umgebungs-SQL	Optional. Geben Sie die SQL-Befehle zum Einrichten der Datenbankumgebung ein, wenn Sie eine Verbindung zur Datenbank herstellen. Der Datenintegrationsdienst führt die SQL-Befehle zur Verbindungsumgebung jedes Mal aus, wenn er eine Verbindung zur Datenbank herstellt.
Transaktions-SQL	Optional. Geben Sie die SQL-Befehle zum Einrichten der Datenbankumgebung ein, wenn Sie eine Verbindung zur Datenbank herstellen. Der Datenintegrationsdienst führt die SQL-Befehle zur Transaktionsumgebung am Anfang jeder Transaktion aus.

Eigenschaft	Beschreibung
Wiederholungsperiode	Diese Eigenschaft ist für die zukünftige Verwendung reserviert.
SQL-Kennungszeichen	Der Zeichentyp, der verwendet wird, um Sonderzeichen und reservierte SQL-Schlüsselwörter wie WHERE zu kennzeichnen. Der Datenintegrationsdienst schließt mit dem ausgewählten Zeichen Sonderzeichen und reservierte SQL-Schlüsselwörter ein. Außerdem nutzt der Datenintegrationsdienst dieses Zeichen zur Unterstützung der ID-Eigenschaft für gemischte Groß- und Kleinschreibung.
Unterstützte IDs für gemischte Groß-/Kleinschreibung	Sofern aktiviert, umgibt der Datenintegrationsdienst Tabellen-, Ansichts-, Schema-, Synonym- und Spaltennamen beim Generieren und Ausführen von SQL für diese Objekte in der Verbindung mit ID-Zeichen. Zu verwenden, wenn Objekte Namen mit gemischter Groß-/Kleinschreibung oder kleingeschriebene Namen haben. Diese Option ist standardmäßig deaktiviert.

Hinweis: Wenn Sie eine Microsoft SQL Server-Verbindung verwenden, um auf Tabellen in einer Microsoft SQL Server-Datenbank zuzugreifen, zeigt das Developer-Tool nicht die Synonyme für die Tabellen an.

Eigenschaften für Oracle-Verbindungen

Verwenden Sie eine Oracle-Verbindung, um auf Tabellen in einer Oracle-Datenbank zuzugreifen.

In der folgenden Tabelle werden die Eigenschaften von Oracle-Verbindungen erläutert.

Eigenschaft	Beschreibung
Benutzername	Benutzername für die Datenbank.
Passwort	Das Passwort für den Benutzernamen.
Verbindungszeichenfolge für den Metadatenzugriff	<p>Verbindungszeichenfolge für das Importieren von physischen Datenobjekten.</p> <p>Verwenden Sie die folgende Verbindungszeichenfolge:</p> <pre>jdbc:informatica:oracle://<host>:1521;SID=<sid></pre> <p>Verwenden Sie die folgende Verbindungszeichenfolge, um eine Verbindung zu Oracle über den Oracle Connection Manager herzustellen:</p> <pre>jdbc:Informatica:oracle:TNSNamesFile=<vollqualifizierter Pfad zur Datei tnsnames.ora>;TNSServerName=<TNS-Servername>;</pre>
Verbindungszeichenfolge für den Datenzugriff	Die Verbindungszeichenfolge für die Datenvorschau und das Ausführen von Zuordnungen. 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 die SQL-Befehle zur Verbindungsumgebung jedes Mal aus, wenn er eine Verbindung zur Datenbank herstellt.

Eigenschaft	Beschreibung
Transaktions-SQL	Optional. Geben Sie die SQL-Befehle zum Einrichten der Datenbankumgebung ein, wenn Sie eine Verbindung zur Datenbank herstellen. Der Datenintegrationsdienst führt die Transaktionsumgebungs-SQL 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 Massenmodus. Der Standardwert ist „Deaktiviert“.
SQL-Bezeichnerzeichen	Der Zeichentyp, der zur Kennzeichnung von Sonderzeichen und reservierten SQL-Schlüsselwörtern, wie WHERE, verwendet wird. Der Datenintegrationsdienst schließt mit dem ausgewählten Zeichen Sonderzeichen und reservierte SQL-Schlüsselwörter ein. Außerdem nutzt der Datenintegrationsdienst dieses Zeichen zur Unterstützung der ID-Eigenschaft für gemischte Groß- und Kleinschreibung.
Unterstützte IDs für gemischte Groß-/Kleinschreibung	Sofern aktiviert, schließt der Datenintegrationsdienst Tabellen-, Ansichts-, Schema-, Synonym- und Spaltennamen in Bezeichnerzeichen ein, wenn SQL für diese Objekte in der Verbindung erzeugt und ausgeführt wird. Zu verwenden, wenn Objekte Namen mit gemischter Groß-/Kleinschreibung oder kleingeschriebene Namen haben. Diese Option ist standardmäßig deaktiviert.

Eigenschaften von PostgreSQL-Verbindungen

Verwenden Sie eine JDBC-Verbindung für den Zugriff auf Tabellen in einer PostgreSQL-Datenbank.

In der folgenden Tabelle werden die Eigenschaften von Oracle-Verbindungen erläutert.

Eigenschaft	Beschreibung
Benutzername	Benutzername für die Datenbank.
Passwort	Das Passwort für den Benutzernamen.
JDBC-Treiberklassenname	
Verbindungszeichenfolge	Verbindungszeichenfolge für das Auslesen von Daten und Metadaten aus der Datenbank. Definieren Sie die Verbindungszeichenfolge im folgenden Format: <code>jdbc:informatica:postgresql://<host>:<port>;Database=<id></code>
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 Transaktionsumgebungs-SQL am Anfang jeder Transaktion aus.

Eigenschaft	Beschreibung
Unterstützte IDs für gemischte Groß-/Kleinschreibung	Sofern aktiviert, schließt der Datenintegrationsdienst Tabellen-, Ansichts-, Schema-, Synonym- und Spaltennamen in Bezeichnerzeichen ein, wenn SQL für diese Objekte in der Verbindung erzeugt und ausgeführt wird. Zu verwenden, wenn Objekte Namen mit gemischter Groß-/Kleinschreibung oder kleingeschriebene Namen haben. Diese Option ist standardmäßig deaktiviert.
SQL-Bezeichnerzeichen	Der Zeichentyp, der zur Kennzeichnung von Sonderzeichen und reservierten SQL-Schlüsselwörtern, wie WHERE, verwendet wird. Der Datenintegrationsdienst schließt mit dem ausgewählten Zeichen Sonderzeichen und reservierte SQL-Schlüsselwörter ein. Außerdem nutzt der Datenintegrationsdienst dieses Zeichen zur Unterstützung der ID-Eigenschaft für gemischte Groß- und Kleinschreibung.
Sqoop-Connector verwenden	
Sqoop-Argumente	

Erstellen einer Verbindung

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

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie auf die Ansicht **Verbindungen**.
3. Wählen Sie die Domäne im Navigator aus.
4. Klicken Sie im Navigator auf **Aktionen > Neu > Datenbankverbindung**.
Das Dialogfeld **Neue Datenbankverbindung** wird eingeblendet.
5. Wählen Sie im Dialogfeld **Neue Verbindung** den Verbindungstyp aus, und klicken Sie dann auf **OK**.
Die **Neue Verbindung** wird angezeigt.
6. Geben Sie die Verbindungseigenschaften ein.
Die Verbindungseigenschaften, die Sie eingeben, richten sich nach dem Verbindungstyp. Klicken Sie auf **Weiter**, um zur nächsten Seite im Assistenten **Neue Verbindung** zu wechseln.
7. Klicken Sie nach der Eingabe der Verbindungseigenschaften auf **Verbindung testen**, um die Verbindung zu testen.
8. Klicken Sie auf **Fertig stellen**.

KAPITEL 14

Erstellen und Konfigurieren von Anwendungsdiensten

Dieses Kapitel umfasst die folgenden Themen:

- [Checkliste zum Erstellen und Konfigurieren von Anwendungsdiensten, 283](#)
- [Erstellen und Konfigurieren von Anwendungsdiensten – Übersicht, 284](#)
- [Erstellen und Konfigurieren des Modellrepository-Diensts, 284](#)
- [Erstellen und Konfigurieren des Datenintegrationsdiensts, 289](#)
- [Erstellen und Konfigurieren des PowerCenter-Repository-Dienstes, 293](#)
- [Erstellen und Konfigurieren des PowerCenter-Integrationsdienstes, 297](#)
- [Erstellen und Konfigurieren des Metadata Manager-Dienstes, 299](#)
- [Erstellen und Konfigurieren des Content-Management-Diensts, 304](#)
- [Erstellen und Konfigurieren des Analyst-Diensts, 306](#)
- [Erstellen und Konfigurieren des Suchdiensts, 308](#)

Checkliste zum Erstellen und Konfigurieren von Anwendungsdiensten

Dieses Kapitel enthält Anweisungen zur Erstellung und Konfiguration von Anwendungsdiensten. Selbst wenn Sie Dienste während der Installation erstellt haben, müssen Sie einige Dienste möglicherweise noch konfigurieren. Verwenden Sie diese Checkliste, um die Konfiguration der Anwendungsdienste zu überwachen.

- ☐ Prüfen Ihrer Notizen zur Planung der Anwendungsdienste.
- ☐ Identifizieren der Dienste, die Sie während der Installation erstellt haben, und führen Sie zusätzliche Konfigurationsaufgaben für den Dienst aus.
- ☐ Erstellen und Konfigurieren anderer in der Domäne erwünschter Dienste.

Erstellen und Konfigurieren von Anwendungsdiensten – Übersicht

Falls Sie bei der Ausführung des Installationsprogramms keine Dienste erstellt haben, verwenden Sie das Administrator Tool zum Erstellen der Anwendungsdienste.

Einige Anwendungsdienste sind von anderen Anwendungsdiensten abhängig. Beim Erstellen dieser abhängigen Anwendungsdienste müssen Sie die Namen anderer ausgeführter Anwendungsdienste angeben. Überprüfen Sie die Anwendungsdienst-Abhängigkeiten, um die Reihenfolge zu ermitteln, in der die Dienste erstellt werden müssen. Sie müssen beispielsweise vor dem Erstellen eines Datenintegrationsdiensts zunächst einen Modellrepository-Dienst erstellen.

Stellen Sie vor dem Erstellen der Anwendungsdienste sicher, dass Sie die erforderlichen Aufgaben für die Installation und Konfiguration abgeschlossen haben.

Erstellen und Konfigurieren des Modellrepository-Diensts

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 einem Informatica-Client-Tool oder Anwendungsdienst auf ein Modellrepository-Objekt zugreifen, sendet der Client oder der Dienst eine Anfrage an den Modellrepository-Dienst. Der Modellrepository-Dienst-Prozess ruft Metadaten aus den Modellrepository-Datenbanktabellen ab, fügt sie dort ein und aktualisiert sie.

Erstellen des Modellrepository-Dienstes

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

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie auf **Aktionen > Neu > Modellrepository-Dienst**.

Das Dialogfeld **Neuer Modellrepository-Dienst** wird angezeigt.

3. Geben Sie auf der Seite **Neuer Modellrepository-Dienst – Schritt 1 von 2** die folgenden Eigenschaften ein:

Eigenschaft	Beschreibung
Name	Name des Diensts. Beachten Sie die folgenden Richtlinien, wenn Sie den Dienst benennen: <ul style="list-style-type: none"> - Es wird nicht zwischen Groß- und Kleinschreibung unterschieden. - Der Name muss in der Domäne eindeutig sein. - Er darf nicht mehr als 128 Zeichen umfassen. - Er darf nicht mit @ beginnen. - Er darf die folgenden Sonderzeichen nicht enthalten: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! ()] [- Sie können den Namen des Diensts nach dessen Erstellung nicht mehr ändern.
Beschreibung	Beschreibung des Diensts. Er darf nicht mehr als 765 Zeichen umfassen.
Speicherort	Domäne und Ordner, in denen der Dienst erstellt wird. 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 dieser 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. Sie können den Windows NT-Benutzernamen für eine vertrauenswürdige Verbindung für Microsoft SQL Server eingeben.
Passwort	Passwort der Repository-Datenbank für den Datenbankbenutzer. Sie können das Windows NT-Passwort für eine vertrauenswürdige Verbindung für Microsoft SQL Server eingeben.
Datenbankschema	Verfügbar für Microsoft SQL Server und PostgreSQL. Name des Schemas, das die Modellrepository-Tabellen enthält.
Datenbank-Tablespace	Für IBM DB2 verfügbar. Der Name des Tablespace, in dem die Tabellen erstellt werden sollen. Bei einer IBM DB2-Datenbank mit mehreren Partitionen muss der Tablespace einen einzelnen Knoten und eine einzelne Partition umfassen.

6. Geben Sie die JDBC-Verbindungszeichenfolge ein, mit der der Dienst eine Verbindung zur Modellrepository-Datenbank herstellt.

Verwenden Sie die folgende Syntax für die Verbindungszeichenfolge für den ausgewählten Datenbanktyp:

Datenbanktyp	Syntax der Verbindungszeichenfolge
IBM DB2	"jdbc:informatica:db2://<host name>:<port number>;DatabaseName=<database name>;BatchPerformanceWorkaround=true;DynamicSections=3000"
Microsoft SQL Server	<div> <ul style="list-style-type: none"> - Microsoft SQL Server, der die Standardinstanz verwendet "jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database name>;SnapshotSerializable=true" - Microsoft SQL Server, der eine benannte Instanz verwendet "jdbc:informatica:sqlserver://<host name>\<named instance name>;DatabaseName=<database name>;SnapshotSerializable=true" - Microsoft Azure. jdbc:informatica:sqlserver://<host_name>:<port_number>;DatabaseName=<database_name>;SnapshotSerializable=true;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.<hostnameincertificate>;ValidateServerCertificate=true - Azure SQL Database mit Active Directory-Authentifizierung. "jdbc:informatica: sqlserver://<host_name>:<port_number>;database=<database_name>;encrypt=true;AuthenticationMethod=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=<seconds>" </div> <div> <p>Hinweis: Wenn Sie die Windows NT-Anmeldeinformationen für die Modellrepository-Datenbank in Microsoft SQL Server angegeben haben, schließen Sie die Authentifizierungsmethode mithilfe der Syntax der Verbindungszeichenfolge als NTLM ein.</p> <ul style="list-style-type: none"> - Microsoft SQL Server, der die Standardinstanz mit Windows NT-Anmeldeinformationen verwendet: "jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM" - Microsoft SQL Server, der eine benannte Instanz mit Windows NT-Anmeldeinformationen verwendet: "jdbc:informatica:sqlserver://<host name>\<named instance name>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM" </div>
Oracle	"jdbc:informatica:oracle://<host name>:<port number>;SID=<database name>;MaxPooledStatements=20;CatalogOptions=0;BatchPerformanceWorkaround=true"
PostgreSQL	"jdbc:informatica:postgresql://<host name>:<port number>;DatabaseName= "

- 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	Obligatorisch. Gibt an, ob Daten bei der Netzwerkübertragung verschlüsselt werden. Dieser Parameter muss auf <code>SSL</code> festgelegt werden.
ValidateServerCertificate	Optional. Gibt an, ob Informatica das Zertifikat validiert, das der Datenbankserver sendet. Wenn dieser Parameter auf <code>TRUE</code> gesetzt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat. Wenn Sie den Parameter <code>HostNameInCertificate</code> angeben, validiert Informatica auch den Hostnamen im Zertifikat. Wenn dieser Parameter auf <code>FALSE</code> 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 gesicherte Datenbank gehostet wird. Wenn Sie einen Hostnamen angeben, validiert Informatica den Hostnamen in der Verbindungszeichenfolge mit dem Hostnamen im SSL-Zertifikat.
cryptoProtocolVersion	Obligatorisch. Gibt das Kryptografieprotokoll an, das für die Verbindung mit einer gesicherten 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.
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: <code><Informatica-Installationsverzeichnis>/tomcat/bin</code>
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.

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

Nach dem Erstellen des Modellrepository-Dienstes

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

- Erstellen des Modellrepository-Benutzers, wenn die Domäne keine Kerberos-Authentifizierung verwendet

- Erstellen anderer Anwendungsdienste

Erstellen des Modellrepository-Benutzers

Wenn Sie einen Anwendungsdienst erstellen, der vom Modellrepository-Dienst abhängig ist, geben Sie den Namen des Modellrepository-Diensts und dieses Modellrepository-Benutzers an.

Wenn die Domäne keine Kerberos-Authentifizierung verwendet, erfolgt die Authentifizierung anderer Anwendungsdienste, die Anfragen an den Modellrepository-Dienst stellen, in der Domäne mit einem Benutzerkonto. Sie müssen ein Benutzerkonto erstellen und dem Benutzer die Administratorrolle für den Modellrepository-Dienst zuweisen.

1. Klicken Sie im Administrator-Tool auf die Registerkarte **Sicherheit**.
2. Klicken Sie im Menü „Sicherheitsaktionen“ auf **Benutzer erstellen**, um ein natives Benutzerkonto zu erstellen.

Hinweis: Wenn Sie die LDAP-Authentifizierung in der Domäne einrichten, können Sie ein LDAP-Benutzerkonto für den Modellrepository-Benutzer verwenden.

3. Geben Sie folgende Eigenschaften für den Benutzer ein:

Eigenschaft	Beschreibung
Anmeldename	Der Anmeldename für das Benutzerkonto. Der Anmeldename für ein Benutzerkonto muss innerhalb der Sicherheitsdomäne, zu der er gehört, eindeutig sein. Beim Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden. Er darf nicht länger als 128 Zeichen sein. Er darf weder einen Tabulator noch ein Zeilenende-Zeichen noch folgende Sonderzeichen enthalten: „ + " \ < > ; / * % ? & Der Name kann ein ASCII-Leerzeichen enthalten, jedoch nicht als erstes oder letztes Zeichen. Alle anderen Leerzeichen sind nicht zulässig.
Passwort	Das Passwort für das Benutzerkonto. Das Passwort kann zwischen 1 und 80 Zeichen lang sein.
Passwort bestätigen	Geben Sie das Passwort zur Bestätigung erneut ein. Sie müssen das Passwort noch einmal eingeben. Das Passwort darf nicht mit Kopieren und Einfügen eingegeben werden.
Vollständiger Name	Der vollständige Name für das Benutzerkonto. Der vollständige Name darf folgende Sonderzeichen nicht enthalten: < > "
Beschreibung	Die Beschreibung des Benutzerkontos. Die Beschreibung darf nicht länger als 765 Zeichen sein und keines der folgenden Sonderzeichen enthalten: < > "

4. Klicken Sie auf **OK**.
Die Benutzereigenschaften werden angezeigt.
5. Klicken Sie auf die Registerkarte **Berechtigungen**.
6. Klicken Sie auf **Bearbeiten**.
Das Dialogfeld **Rollen und Rechte bearbeiten** wird eingeblendet.
7. Erweitern Sie auf der Registerkarte der **Rollen** den Modellrepository-Dienst.
8. Wählen Sie unter **Systemdefinierte Rollen** „Administrator“ aus und klicken Sie auf **OK**.

Erstellen weiterer Dienste

Nach dem Erstellen des Modellrepository-Dienstes erstellen Sie die Anwendungsdienste, die vom Modellrepository-Dienst abhängig sind.

Erstellen Sie die abhängigen Dienste in der folgenden Reihenfolge:

1. Datenintegrationsdienst
2. Analyst-Dienst
3. Content-Management-Dienst
4. Suchdienst

Erstellen und Konfigurieren des Datenintegrationsdiensts

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

Erstellen des Datenintegrationsdiensts

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

Stellen Sie vor dem Erstellen des Datenintegrationsdiensts sicher, dass Sie die folgenden Dienste erstellt haben:

Modell-Repository Service

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. Beachten Sie die folgenden Richtlinien, wenn Sie den Dienst benennen: <ul style="list-style-type: none"> - Es wird nicht zwischen Groß- und Kleinschreibung unterschieden. - Der Name muss in der Domäne eindeutig sein. - Er darf nicht mehr als 128 Zeichen umfassen. - Er darf nicht mit @ beginnen. - Er darf die folgenden Sonderzeichen nicht enthalten: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! ()] [- Sie können den Namen des Diensts nach dessen Erstellung nicht mehr ändern.
Beschreibung	Beschreibung des Diensts. Er darf nicht mehr als 765 Zeichen umfassen.
Speicherort	Domäne und Ordner, in denen der Dienst erstellt wird. 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 dieser Dienst ausgeführt wird.
Backup-Knoten	Wenn die Lizenz hohe Verfügbarkeit einschließt, sind dies die Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist.
Modellrepository-Dienst	Modellrepository-Dienst zum Zuweisen zum Dienst.
Benutzername	Benutzername, den der Dienst für den Zugriff auf den Modellrepository-Dienst verwendet. Geben Sie den Modellrepository-Benutzer ein, den Sie erstellt haben.
Passwort	Passwort für den Modellrepository-Benutzer.
Sicherheitsdomäne	LDAP-Sicherheitsdomäne für den Benutzer des Modellrepository. Das Feld wird angezeigt, wenn die Informatica-Domäne eine LDAP-Sicherheitsdomäne enthält. Nicht verfügbar für eine Domäne mit Kerberos-Authentifizierung.

6. Klicken Sie auf **Weiter**.
Die Seite **Neuer Datenintegrationsdienst - Schritt 2 von 14** wird angezeigt.
7. Geben Sie die HTTP-Portnummer für den Datenintegrationsdienst ein.
8. Akzeptieren Sie für die restlichen Sicherheitseigenschaften die Standardwerte. Sie können die Sicherheitseigenschaften nach dem Erstellen des Datenintegrationsdiensts konfigurieren.
9. Wählen Sie **Dienst aktivieren** aus.
Zum Aktivieren des Datenintegrationsdiensts muss der Modellrepository-Dienst ausgeführt werden.
10. Stellen Sie sicher, dass **Zur Plugin-Konfigurationsseite wechseln** nicht ausgewählt ist.
11. Klicken Sie auf **Weiter**.

Die Seite **Neuer Datenintegrationsdienst - Schritt 3 von 14** wird angezeigt.

12. Stellen Sie die Eigenschaft **Joboptionen starten** auf einen der folgenden Werte ein:

- Im Dienstprozess. Konfigurieren Sie diesen Wert, wenn Sie SQL-Datendienst- und Webdienstjobs ausführen. Die SQL-Datendienst- und Webdienstjobs erreichen in der Regel eine bessere Leistung, wenn der Datenintegrationsdienst Jobs im Dienstprozess ausführt.
- In separaten lokalen Prozessen. Konfigurieren Sie diesen Wert, wenn Sie Mapping-, Profil- und Arbeitsablaufjobs ausführen. Wenn der Datenintegrationsdienst Jobs in separaten lokalen Prozessen ausführt, erhöht sich die Stabilität, weil eine unerwartete Unterbrechung eines Jobs keine Auswirkungen auf alle anderen Jobs hat.

Wenn Sie den Datenintegrationsdienst nach der Erstellung des Diensts zur Ausführung auf einem Gitter konfigurieren, können Sie den Dienst zur Ausführung von Jobs in separaten Remoteprozessen konfigurieren.

13. Akzeptieren Sie die Standardwerte für die verbleibenden Ausführungsoptionen und klicken Sie auf **Weiter**.

Die Seite **Neuer Datenintegrationsdienst - Schritt 4 von 14** wird angezeigt.

14. Wenn Sie die Datenobjekt-Cache-Datenbank für den Datenintegrationsdienst erstellt haben, klicken Sie auf **Auswählen** und wählen Sie die Cache-Verbindung aus. Wählen Sie die Datenobjekt-Cache-Verbindung aus, die Sie für den Dienst erstellt haben, um auf die Datenbank zuzugreifen.

15. Akzeptieren Sie für die restlichen Eigenschaften auf dieser Seite die Standardwerte und klicken Sie auf **Weiter**.

Die Seite **Neuer Datenintegrationsdienst - Schritt 5 von 14** wird angezeigt.

16. Für eine optimale Leistung aktivieren Sie die Datenintegrationsdienst-Module, die Sie verwenden möchten.

In der folgenden Tabelle werden die Datenintegrationsdienst-Module aufgelistet, die Sie aktivieren können:

Modul	Beschreibung
Webdienstmodul	Führt Vorgangs-Mappings für Webdienste durch.
Zuordnungsdienstmodul	Führt Mappings und Vorschauen aus.
Profilerstellungsdienst-Modul	Führt Profile und Scorecards aus.
SQL-Dienstmodul	Führt SQL-Abfragen von Client-Tools anderer Hersteller an einen SQL-Datendienst aus.
Arbeitsablauf-Orchestration-Dienstmodul	Führt Arbeitsabläufe aus.

17. Klicken Sie auf **Weiter**.

Die Seite **Neuer Datenintegrationsdienst - Schritt 6 von 14** wird angezeigt.

Sie können Sie die HTTP-Proxyservereigenschaften so konfigurieren, dass die HTTP-Anfragen an den Datenintegrationsdienst umgeleitet werden. Sie können Sie die HTTP-Konfigurationseigenschaften so konfigurieren, dass Webdienst-Client-Computer, die Anfragen an den Datenintegrationsdienst senden können, gefiltert werden. Diese Eigenschaften können Sie nach dem Erstellen des Diensts konfigurieren.

18. Akzeptieren Sie die Standardwerte für die HTTP-Proxyserver- und HTTP-Konfigurationseigenschaften und klicken Sie auf **Weiter**.

Die Seite **Neuer Datenintegrationsdienst - Schritt 7 von 14** wird angezeigt.

Der Datenintegrationsdienst nutzt die Ergebnissatz-Cache-Eigenschaften, um zwischengespeicherte Ergebnisse für SQL-Datendienstabfragen und -Webdienstanfragen zu verwenden. Sie können die Eigenschaften nach dem Erstellen des Diensts konfigurieren.

19. Akzeptieren Sie die Standardwerte für die Eigenschaften des Ergebnissatz-Cache und klicken Sie auf **Weiter**.

Die Seite **Neuer Datenintegrationsdienst - Schritt 8 von 14** wird angezeigt.

20. Wenn Sie die Profiling-Warehouse-Datenbank für den Datenintegrationsdienst erstellt haben, wählen Sie das Profilerstellungsdienst-Modul aus.
21. Wenn Sie die Arbeitsablauf-Datenbank für den Datenintegrationsdienst erstellt haben, wählen Sie das Arbeitsablauf-Orchestration-Dienstmodul aus.
22. Stellen Sie sicher, dass die restlichen Module nicht ausgewählt sind.
Sie können die Eigenschaften für die restlichen Module nach dem Erstellen des Diensts konfigurieren.
23. Klicken Sie auf **Weiter**.

Die Seite **Neuer Datenintegrationsdienst - Schritt 11 von 14** wird angezeigt.

24. Wenn Sie die Profiling-Warehouse-Datenbank für den Datenintegrationsdienst erstellt haben, klicken Sie auf **Auswählen**, um die Datenbankverbindung auszuwählen. Wählen Sie die Profiling-Warehouse-Verbindung aus, die Sie für den Dienst erstellt haben, um auf die Datenbank zuzugreifen.
25. Wählen Sie aus, ob die Profiling-Warehouse-Datenbank Inhalt aufweist oder nicht.

Wenn Sie eine neue Profiling-Warehouse-Datenbank erstellt haben, wählen Sie **Die angegebene Verbindungszeichenfolge weist keinen Inhalt auf** aus.

26. Klicken Sie auf **Weiter**.

Die Seite **Neuer Datenintegrationsdienst - Schritt 12 von 14** wird angezeigt.

27. Akzeptieren Sie die Standardwerte für die erweiterten Profiling-Eigenschaften und klicken Sie auf **Weiter**.

Die Seite **Neuer Datenintegrationsdienst - Schritt 14 von 14** wird angezeigt.

28. Wenn Sie die Arbeitsablauf-Datenbank für den Datenintegrationsdienst erstellt haben, klicken Sie auf **Auswählen**, um die Datenbankverbindung auszuwählen. Wählen Sie die Arbeitsablauf-Datenbankverbindung aus, die Sie für den Dienst erstellt haben, um auf die Datenbank zuzugreifen.
29. Klicken Sie auf **Fertig stellen**.

Die Domäne erstellt und aktiviert den Datenintegrationsdienst.

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

Nach dem Erstellen des Datenintegrationsdienstes

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

- Überprüfen der Hostdateikonfiguration
- Erstellen anderer Anwendungsdienste

Hostdateikonfiguration überprüfen

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

Erstellen weiterer Dienste

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

Erstellen Sie die abhängigen Dienste in der folgenden Reihenfolge:

1. Content-Management-Dienst
2. Analyst-Dienst
3. Suchdienst

Erstellen und Konfigurieren des PowerCenter-Repository-Dienstes

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

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

Erstellen des PowerCenter-Repository-Dienstes

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

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie auf **Aktionen > Neu > PowerCenter-Repository-Dienst**.
Das Dialogfeld **Neuer PowerCenter-Repository-Dienst** wird angezeigt.
3. Geben Sie auf der Seite **Neuer PowerCenter-Repository-Dienst – Schritt 1 von 2** die folgenden Eigenschaften ein:

Eigenschaft	Beschreibung
Name	Name des Diensts. Beachten Sie die folgenden Richtlinien, wenn Sie den Dienst benennen: <ul style="list-style-type: none">- Es wird nicht zwischen Groß- und Kleinschreibung unterschieden.- Der Name muss in der Domäne eindeutig sein.- Er darf nicht mehr als 128 Zeichen umfassen.- Er darf nicht mit @ beginnen.- Er darf die folgenden Sonderzeichen nicht enthalten: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! ()] [- Sie können den Namen des Diensts nach dessen Erstellung nicht mehr ändern.
Beschreibung	Beschreibung des Diensts. Er darf nicht mehr als 765 Zeichen umfassen.

Eigenschaft	Beschreibung
Speicherort	Domäne und Ordner, in denen der Dienst erstellt wird. 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 dieser Dienst ausgeführt wird.
Primärer Knoten	Erforderlich, wenn Sie über hohe Verfügbarkeit verfügen. Der Knoten, auf dem der Dienst standardmäßig 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 PowerCenter-Repository-Dienst – Schritt 2 von 2** wird angezeigt.

5. Geben Sie die folgenden Eigenschaften für die PowerCenter-Repository-Datenbank ein:

Eigenschaft	Beschreibung
Datenbanktyp	Der Typ der Repository-Datenbank.
Benutzername	Der Datenbankbenutzername für das Repository.
Passwort	Passwort für den PowerCenter-Repository-Datenbankbenutzer. Muss in 7-Bit-ASCII kodiert sein.
Verbindungszeichenfolge	Native Verbindungszeichenfolge, die der PowerCenter-Repository-Dienst verwendet, um auf die Repository-Datenbank zuzugreifen. Verwenden Sie die folgende native Syntax der Verbindungszeichenfolge für jede unterstützte Datenbank: <ul style="list-style-type: none"> - <code>servername@databasename</code> für Microsoft SQL Server und Sybase. - <code>databasename.world</code> für Oracle - <code>databasename</code> für IBM DB2
Codepage	Codepage der Repository-Datenbank. Der PowerCenter-Repository-Dienst verwendet zum Schreiben von Daten den in der Datenbank kodierten Datensatz. Nachdem Sie den PowerCenter-Repository-Dienst erstellt haben, können Sie die Codepage in den Eigenschaften des PowerCenter-Repository-Dienstes nicht mehr ändern.
Tablespace-Name	Name des Tablespace, in dem alle Repository-Datenbanktabellen erstellt werden sollen. Sie können im Tablespace-Namen keine Leerzeichen verwenden. Für IBM DB2- und Sybase-Datenbanken verfügbar. Um die Repository-Leistung bei IBM DB2 EEE-Repositories zu verbessern, geben Sie einen Tablespace-Namen mit einem Knoten an.

6. Wählen Sie **Die angegebene Verbindungszeichenfolge weist keinen Inhalt auf. Erstellen Sie neue Inhalte**. aus.

7. Optional können Sie ein globales Repository auswählen.

Nachdem Sie den Dienst erstellen, können Sie ein lokales Repository zu einem globalen Repository hochstufen. Ein globales Repository kann jedoch nicht in ein lokales Repository geändert werden

8. Wenn Ihre Lizenz über die teambasierte Entwicklungsoption verfügt, können Sie optional die Versionskontrolle des Repository aktivieren.

Nachdem Sie den Dienst erstellt haben, können Sie ein versionsloses Repository in ein Repository mit Versionsangabe konvertieren. Ein Repository mit Versionsangabe in ein versionsloses Repository zu konvertieren, ist jedoch nicht möglich.

9. Klicken Sie auf **Fertig stellen**.

Die Domäne erstellt den PowerCenter-Repository-Dienst, startet den Dienst und erstellt Inhalt für das PowerCenter-Repository.

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

Nach dem Erstellen des PowerCenter-Repository-Dienstes

Führen Sie nach dem Erstellen des PowerCenter-Repository-Dienstes die folgenden Aufgaben durch:

- Konfigurieren des PowerCenter-Repository-Dienstes zur Ausführung im normalen Modus
- Erstellen des PowerCenter-Repository-Benutzers, wenn die Domäne keine Kerberos-Authentifizierung verwendet
- Erstellen anderer Anwendungsdienste

Führen Sie den PowerCenter-Repository-Dienst im Normalmodus aus.

Nachdem Sie den PowerCenter-Repository-Dienst erstellt haben, wird er im exklusiven Modus gestartet. Der Zugriff ist auf den Administrator beschränkt. Bearbeiten Sie die Diensteigenschaften, um den Dienst im normalen Betriebsmodus auszuführen und anderen Benutzern Zugriff zu gewähren.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten**.
2. Im Navigator wählen Sie den PowerCenter-Repository-Dienst.
3. Klicken Sie auf **Eigenschaften**.
4. Klicken Sie auf **Repository-Eigenschaften bearbeiten**.
5. Wählen Sie „Normal“ im Feld **Betriebsmodus** aus.
6. Klicken Sie auf **OK**.

Sie müssen den PowerCenter-Repository-Dienst recyceln, damit die Änderungen wirksam werden.

7. Wählen Sie **Aktionen > Dienst recyceln**.

Erstellen des PowerCenter-Repository-Benutzers

Wenn die Domäne keine Kerberos-Authentifizierung verwendet, wird die Authentifizierung anderer Anwendungsdienste, die Anfragen an den PowerCenter-Repository-Dienst stellen, mit einem Benutzerkonto durchgeführt. Sie müssen ein Benutzerkonto erstellen und dem Benutzer die Administratorrolle für den PowerCenter-Repository-Dienst zuweisen.

Wenn Sie einen Anwendungsdienst erstellen, der vom PowerCenter-Repository-Dienst abhängig ist, geben Sie den Namen des PowerCenter-Repository-Dienstes und des PowerCenter-Repository-Benutzers an.

1. Klicken Sie im Administrator-Tool auf die Registerkarte **Sicherheit**.
2. Klicken Sie im Menü „Sicherheitsaktionen“ auf **Benutzer erstellen**, um ein natives Benutzerkonto zu erstellen.

Hinweis: Wenn Sie die LDAP-Authentifizierung in der Domäne einrichten, können Sie ein LDAP-Benutzerkonto für den PowerCenter-Repository-Benutzer verwenden.

3. Geben Sie folgende Eigenschaften für den Benutzer ein:

Eigenschaft	Beschreibung
Anmeldename	Der Anmeldename für das Benutzerkonto. Der Anmeldename für ein Benutzerkonto muss innerhalb der Sicherheitsdomäne, zu der er gehört, eindeutig sein. Beim Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden. Er darf nicht länger als 128 Zeichen sein. Er darf weder einen Tabulator noch ein Zeilenende-Zeichen noch folgende Sonderzeichen enthalten: „ + " \ < > ; / * % ? & Der Name kann ein ASCII-Leerzeichen enthalten, jedoch nicht als erstes oder letztes Zeichen. Alle anderen Leerzeichen sind nicht zulässig.
Passwort	Das Passwort für das Benutzerkonto. Das Passwort kann zwischen 1 und 80 Zeichen lang sein.
Passwort bestätigen	Geben Sie das Passwort zur Bestätigung erneut ein. Sie müssen das Passwort noch einmal eingeben. Das Passwort darf nicht mit Kopieren und Einfügen eingegeben werden.
Vollständiger Name	Der vollständige Name für das Benutzerkonto. Der vollständige Name darf folgende Sonderzeichen nicht enthalten: < > "
Beschreibung	Die Beschreibung des Benutzerkontos. Die Beschreibung darf nicht länger als 765 Zeichen sein und keines der folgenden Sonderzeichen enthalten: < > "

4. Klicken Sie auf **OK**.
Die Benutzereigenschaften werden angezeigt.
5. Klicken Sie auf die Registerkarte **Berechtigungen**.
6. Klicken Sie auf **Bearbeiten**.
Das Dialogfeld **Rollen und Rechte bearbeiten** wird eingeblendet.
7. Erweitern Sie auf der Registerkarte **Rollen** den PowerCenter-Repository-Dienst.
8. Wählen Sie unter **Systemdefinierte Rollen** „Administrator“ aus und klicken Sie auf **OK**.

Erstellen weiterer Dienste

Nach dem Erstellen des PowerCenter-Repository-Dienstes erstellen Sie die Anwendungsdienste, die vom PowerCenter-Repository-Dienst abhängig sind.

Sie können die folgenden Anwendungsdienste erstellen:

1. PowerCenter-Integrationsdienst
2. Metadata Manager-Dienst
3. Webdienst-Hub-Dienst

Erstellen und Konfigurieren des PowerCenter-Integrationsdienstes

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

Wenn Sie einen Arbeitsablauf im PowerCenter Client ausführen, sendet der Client die Anfragen an den PowerCenter-Integrationsdienst. Der PowerCenter-Integrationsdienst stellt eine Verbindung zum PowerCenter-Repository-Dienst zum Abrufen von Metadaten aus dem PowerCenter-Repository her und führt anschließend die Sitzungen und Arbeitsabläufe aus und überwacht sie.

Erstellen des PowerCenter-Integrationsdienstes

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

Stellen Sie vor dem Erstellen des PowerCenter-Integrationsdienstes sicher, dass Sie den folgenden Dienst erstellt haben:

PowerCenter Repository Service

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie auf **Aktionen > Neu > PowerCenter-Integrationsdienst**.

Das Dialogfeld **Neuer PowerCenter-Integrationsdienst** wird eingeblendet.

3. Geben Sie auf der Seite **Neuer PowerCenter-Integrationsdienst – Schritt 1 von 2** die folgenden Eigenschaften ein:

Eigenschaft	Beschreibung
Name	Name des Diensts. Beachten Sie die folgenden Richtlinien, wenn Sie den Dienst benennen: <ul style="list-style-type: none">- Es wird nicht zwischen Groß- und Kleinschreibung unterschieden.- Der Name muss in der Domäne eindeutig sein.- Er darf nicht mehr als 128 Zeichen umfassen.- Er darf nicht mit @ beginnen.- Er darf die folgenden Sonderzeichen nicht enthalten: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! ()] [- Sie können den Namen des Diensts nach dessen Erstellung nicht mehr ändern.
Beschreibung	Beschreibung des Diensts. Er darf nicht mehr als 765 Zeichen umfassen.
Speicherort	Domäne und Ordner, in denen der Dienst erstellt wird. 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 dieser Dienst ausgeführt wird.
Zuweisen	Wählen Sie Knoten aus, um den Dienst zur Ausführung auf einem Knoten zu konfigurieren. Wenn die Lizenz Gitter einschließt, können Sie ein Gitter erstellen und den auf dem Gitter auszuführenden Dienst zuweisen, nachdem Sie den Dienst erstellt haben.

Eigenschaft	Beschreibung
Primärer Knoten	Erforderlich, wenn Sie über hohe Verfügbarkeit verfügen. Der Knoten, auf dem der Dienst standardmäßig 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**.
5. Geben Sie auf der Seite **Neuer PowerCenter-Integrationsdienst – Schritt 2 von 2** die folgenden Eigenschaften ein:

Eigenschaft	Beschreibung
PowerCenter-Repository-Dienst	PowerCenter-Repository-Dienst, der dem Dienst zugeordnet werden soll.
Benutzername	Benutzername, den der Dienst für den Zugriff auf den PowerCenter-Repository-Dienst verwendet. Geben Sie den PowerCenter-Repository-Benutzer ein, den Sie erstellt haben. Erforderlich, wenn Sie dem Dienst einen PowerCenter-Repository-Dienst zuordnen. Nicht verfügbar für eine Domäne mit Kerberos-Authentifizierung.
Passwort	Dem PowerCenter-Repository-Benutzer zugeordnetes Passwort. Nicht verfügbar für eine Domäne mit Kerberos-Authentifizierung.
Sicherheitsdomäne	LDAP-Sicherheitsdomäne für den Benutzer des PowerCenter-Repository. Das Feld Sicherheitsdomäne wird eingeblendet, wenn die Informatica-Domäne eine LDAP-Sicherheitsdomäne enthält. Erforderlich, wenn Sie dem Dienst einen PowerCenter-Repository-Dienst zuordnen. Nicht verfügbar für eine Domäne mit Kerberos-Authentifizierung.

6. Wählen Sie den Datenverschiebungsmodus aus, der bestimmt, wie der PowerCenter-Integrationsdienst Zeichendaten verarbeitet. Wählen Sie ASCII oder Unicode aus. Der Standardwert ist ASCII.

Im ASCII-Modus erkennt der PowerCenter-Integrationsdienst 7-Bit-ASCII- und EBCDIC-Zeichen und speichert jedes Zeichen in einem einzelnen Byte. Im Unicode-Modus erkennt der PowerCenter-Integrationsdienst Multibyte-Zeichensätze, wie sie von unterstützten Codepages definiert sind. Verwenden Sie den Unicode-Modus, wenn Quellen oder Targets 8-Bit- oder Multibyte-Zeichensätze verwenden und Zeichendaten enthalten.

7. Klicken Sie auf **Fertig stellen**.
8. Weisen Sie im Dialogfeld **Codepages angeben** einen Code für den PowerCenter-Integrationsdienst zu. Die Codepage für den PowerCenter-Integrationsdienst muss kompatibel sein mit der Codepage des zugeordneten Repository.
9. Klicken Sie auf **OK**.
Die Domäne erstellt den PowerCenter-Integrationsdienst. Die Domäne aktiviert den PowerCenter-Integrationsdienst während der Diensterstellung nicht.
10. Zum Aktivieren des PowerCenter-Integrationsdienstes wählen Sie den Dienst im Navigator aus und klicken Sie auf **Aktionen > Dienst aktivieren**. Der PowerCenter-Repository-Dienst muss ausgeführt werden, um den PowerCenter-Integrationsdienst zu aktivieren.

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

Nach dem Erstellen des PowerCenter-Integrationsdienstes

Nach dem Erstellen des PowerCenter-Integrationsdienstes erstellen Sie den Metadata Manager-Dienst, der vom PowerCenter-Integrationsdienst abhängig ist.

Erstellen und Konfigurieren des Metadata Manager-Dienstes

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

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

Erstellen des Metadata Manager-Dienstes

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

Stellen Sie vor dem Erstellen des Metadata Manager-Dienstes sicher, dass Sie die folgenden Dienste erstellt und aktiviert haben:

PowerCenter-Repository-Dienst

PowerCenter-Integrationsdienst

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie auf **Aktionen > Neu > Metadata Manager-Dienst**.
Das Dialogfeld **Neuer Metadata Manager-Dienst** erscheint.
3. Geben Sie auf der Seite **Neuer Metadata Manager-Dienst – Schritt 1 von 3** die folgenden Eigenschaften ein:

Eigenschaft	Beschreibung
Name	Name des Diensts. Beachten Sie die folgenden Richtlinien, wenn Sie den Dienst benennen: <ul style="list-style-type: none">- Es wird nicht zwischen Groß- und Kleinschreibung unterschieden.- Der Name muss in der Domäne eindeutig sein.- Er darf nicht mehr als 128 Zeichen umfassen.- Er darf nicht mit @ beginnen.- Er darf die folgenden Sonderzeichen nicht enthalten: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! ()] [- Sie können den Namen des Diensts nach dessen Erstellung nicht mehr ändern.
Beschreibung	Beschreibung des Diensts. Er darf nicht mehr als 765 Zeichen umfassen.

Eigenschaft	Beschreibung
Speicherort	Domäne und Ordner, in denen der Dienst erstellt wird. 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 dieser Dienst ausgeführt wird.

4. Geben Sie die folgenden Eigenschaften des zugehörigen Repository-Dienstes:

Eigenschaft	Beschreibung
Zugehöriger Integrationsdienst	Wählen Sie den PowerCenter-Integrationsdienst aus, über den der Metadata Manager Metadaten in das Metadata Manager-Warehouse lädt.
Repository-Benutzername	Benutzername, den der Dienst für den Zugriff auf den PowerCenter-Repository-Dienst verwendet. Geben Sie den PowerCenter-Repository-Benutzer ein, den Sie erstellt haben. Erforderlich, wenn Sie dem Dienst einen PowerCenter-Repository-Dienst zuordnen. Nicht verfügbar für eine Domäne mit Kerberos-Authentifizierung.
Repository-Passwort	Dem PowerCenter-Repository-Benutzer zugeordnetes Passwort. Nicht verfügbar für eine Domäne mit Kerberos-Authentifizierung.
Sicherheitsdomäne	LDAP-Sicherheitsdomäne für den Benutzer des PowerCenter-Repository. Das Feld Sicherheitsdomäne wird eingeblendet, wenn die Informatica-Domäne eine LDAP-Sicherheitsdomäne enthält. Erforderlich, wenn Sie dem Dienst einen PowerCenter-Repository-Dienst zuordnen. Nicht verfügbar für eine Domäne mit Kerberos-Authentifizierung.

5. Klicken Sie auf **Weiter**.

Die Seite **Neuer Metadata Manager-Dienst – Schritt 2 von 3** wird angezeigt.

6. Geben Sie die folgenden Datenbankeneigenschaften für das Metadata Manager-Repository ein:

Eigenschaft	Beschreibung
Datenbanktyp	Der Typ der Repository-Datenbank.
Codepage	Codepage für Metadata Manager-Repository. Der Metadata Manager-Dienst und die Metadata Manager-Anwendung nutzen beim Schreiben von Daten in das Metadata Manager-Repository den Zeichensatz, der in der Repository-Codepage codiert ist. Sie können den Metadata Manager-Dienst erst nach Angabe der Codepage aktivieren.

Eigenschaft	Beschreibung
Verbindungszeichenfolge	<p>Native Verbindungszeichenfolge für die Metadata Manager-Repository-Datenbank. Der Metadata Manager-Dienst verwendet die Verbindungszeichenfolge, um ein Verbindungsobjekt zum Metadata Manager-Repository im PowerCenter-Repository zu erstellen.</p> <p>Verwenden Sie die folgende native Syntax der Verbindungszeichenfolge für jede unterstützte Datenbank:</p> <ul style="list-style-type: none"> - servername@databasename für Microsoft SQL Server - databasename.world für Oracle - databasename für IBM DB2
Datenbankbenutzer	Der Datenbankbenutzername für das Repository.
Datenbankpasswort	Passwort für den Metadata Manager-Repository-Datenbankbenutzer. Muss in 7-Bit-ASCII kodiert sein.
Tablespace-Name	<p>Name des Tablespace, in dem alle Repository-Datenbanktabellen erstellt werden sollen. Sie können im Tablespace-Namen keine Leerzeichen verwenden.</p> <p>Für IBM DB2-Datenbanken.</p> <p>Um die Repository-Leistung bei IBM DB2 EEE-Repositorys zu verbessern, geben Sie einen Tablespace-Namen mit einem Knoten an.</p>
Datenbankhostname	Name des Computers, der als Host für den Datenbankserver dient.
Datenbankport	Die Portnummer, mit der Sie den Listenerdienst für den Datenbankserver konfigurieren.
SID/Dienstname	Für Oracle-Datenbanken. Gibt an, ob die SID oder der Dienstname in der JDBC-Verbindungszeichenfolge verwendet werden soll. Für Oracle RAC-Datenbanken wählen Sie Oracle-SID oder Oracle-Dienstname. Für andere Oracle-Datenbanken wählen Sie die Oracle-SID aus.
Datenbankname	<p>Der Name des Datenbankservers.</p> <p>Geben Sie den vollständigen Dienstnamen oder die SID für Oracle-Datenbanken, den Dienstnamen für IBM DB2-Datenbanken und den Datenbanknamen für Microsoft SQL Server-Datenbanken an.</p>

7. Wenn Sie Parameter an die Datenbankverbindungs-URL anhängen, konfigurieren Sie zusätzliche Parameter im Feld **Zusätzliche JDBC-Parameter**. Geben Sie die Parameter als Name = Wertpaare, getrennt durch ein Semikolon (;) ein. Beispiel: param1=value1;param2=value2

Sie können diese Eigenschaft verwenden, um die folgenden Parameter anzugeben:

Parameter	Beschreibung
Speicherort des Sicherungsservers	Wenn Sie einen hochverfügbaren Datenbankserver wie zum Beispiel Oracle RAC verwenden, geben Sie den Speicherort eines Sicherungsservers ein.
Oracle ASO (Advanced Security Option)-Parameter	<p>Wenn die Metadata Manager-Repository-Datenbank eine Oracle-Datenbank ist, die ASO verwendet, geben Sie die folgenden zusätzlichen Parameter ein:</p> <pre>EncryptionLevel=[encryption level];EncryptionTypes=[encryption types];DataIntegrityLevel=[data integrity level];DataIntegrityTypes=[data integrity types]</pre> <p>Hinweis: Die Parameterwerte müssen den Werten in der Datei <code>sqlnet.ora</code> auf dem Computer entsprechen, auf dem der Metadata Manager-Dienst ausgeführt wird.</p>
Authentifizierungsinformationen für Microsoft SQL Server	<p>Zum Authentifizieren der Benutzeranmeldedaten und Einrichten einer vertrauenswürdigen Verbindung zu einem Microsoft SQL Server-Repository geben Sie den folgenden Text ein:</p> <pre>AuthenticationMethod=ntlm;LoadLibraryPath=[directory containing DDJDBCx64Auth04.dll]. jdbc:informatica:sqlserver://[host]:[port];DatabaseName=[DB name]; AuthenticationMethod=ntlm;LoadLibraryPath=[directory containing DDJDBCx64Auth04.dll]</pre> <p>Wenn Sie eine vertrauenswürdige Verbindung verwenden, um eine Verbindung zu einer Microsoft SQL Server-Datenbank herzustellen, stellt der Metadata Manager-Dienst eine Verbindung zum Repository mit den Anmeldeinformationen des Benutzers her, der auf dem Computer angemeldet ist, auf dem der Dienst ausgeführt wird.</p> <p>Um den Metadata Manager-Dienst als Windows-Dienst mithilfe einer vertrauenswürdigen Verbindung zu starten, konfigurieren Sie die Eigenschaften des Windows-Dienstes so, dass die Anmeldung mit einem vertrauenswürdigen Benutzerkonto erfolgt.</p>

8. Wenn das Metadata Manager-Repository für die sichere Kommunikation konfiguriert ist, können Sie zusätzliche JDBC-Parameter im Feld **Sichere JDBC-Parameter** konfigurieren.

Verwenden Sie diese Eigenschaft, um sichere Verbindungsparameter wie Passwörter anzugeben. Das Administrator Tool zeigt keine sicheren Parameter bzw. die Parameterwerte in den Eigenschaften des Metadata Manager-Diensts an. Geben Sie die Parameter als Name = Wertpaare, getrennt durch ein Semikolon (;) ein. Beispiel: `param1=value1;param2=value2`.

Geben Sie die folgenden sicheren Datenbankparameter ein:

Sicherer Datenbankparameter	Beschreibung
EncryptionMethod	Obligatorisch. Gibt an, ob Daten bei der Netzwerkübertragung verschlüsselt werden. Dieser Parameter muss auf <code>SSL</code> festgelegt werden.
TrustStore	Erforderlich. Pfad und Dateiname der TrustStore-Datei, die das SSL-Zertifikat des Datenbankservers enthält.
TrustStorePassword	Erforderlich. Passwort für den Zugriff auf die Truststore-Datei.

Sicherer Datenbankparameter	Beschreibung
HostNameInCertificate	Hostname des Computers, auf dem die sichere Datenbank gehostet wird. Wenn Sie einen Hostnamen angeben, vergleicht der Metadata Manager-Dienst den Hostnamen in der Verbindungszeichenfolge mit dem Hostnamen im SSL-Zertifikat.
ValidateServerCertificate	Optional. Gibt an, ob Informatica das Zertifikat validiert, das der Datenbankserver sendet. Wenn dieser Parameter auf TRUE gesetzt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat. Wenn Sie den Parameter HostNameInCertificate angeben, validiert Informatica auch den Hostnamen im Zertifikat. Wenn dieser Parameter auf FALSE gesetzt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat nicht. Informatica ignoriert alle Truststore-Informationen, die Sie angeben.
KeyStore	Pfad und Dateiname der Schlüsselspeicherdatei mit den SSL-Zertifikaten, die der Metadata Manager-Dienst an den Datenbankserver sendet.
KeyStorePassword	Passwort für den Zugriff auf die Schlüsselspeicherdatei.

9. Klicken Sie auf **Weiter**.

Die Seite **Neuer Metadata Manager-Dienst – Schritt 3 von 3** wird angezeigt.

10. Geben Sie die HTTP-Portnummer für den Dienst ein.

11. Zum Aktivieren der sicheren Kommunikation mit dem Metadata Manager-Dienst wählen Sie **Secured Socket Layer aktivieren** aus.

Geben Sie die folgenden Eigenschaften ein, um die sichere Kommunikation für den Dienst zu konfigurieren:

Eigenschaft	Beschreibung
HTTPS-Port	Zu verwendende Portnummer für eine sichere Verbindung zum Dienst. Verwenden Sie eine Portnummer, die sich von der HTTP-Portnummer unterscheidet.
Schlüsselspeicherdatei	Pfad und Dateiname der Schlüsselspeicherdatei, die die privaten oder öffentlichen Schlüsselpaare und die zugeordneten Zertifikate enthält. Erforderlich, wenn Sie HTTPS-Verbindungen für den Dienst verwenden.
Schlüsselspeicherpasswort	Klartext-Passwort für die Schlüsselspeicherdatei.

12. Klicken Sie auf **Fertig stellen**.

Die Domäne erstellt den Metadata Manager-Dienst. Die Domäne aktiviert den Metadata Manager-Dienst während der Diensterstellung nicht.

13. Zum Aktivieren des Metadata Manager-Dienstes wählen Sie den Dienst im Navigator aus und klicken Sie auf **Aktionen > Dienst aktivieren**. Der PowerCenter-Repository-Dienst und der PowerCenter-Integrationsdienst müssen ausgeführt werden, um den Metadata Manager-Dienst zu aktivieren.

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

Nach dem Erstellen des Metadata Manager-Dienstes

Führen Sie nach dem Erstellen des Metadata Manager-Dienstes die folgenden Aufgaben durch:

- Erstellen der Inhalte für das Metadata Manager-Repository
- Erstellen anderer Anwendungsdienste

Beim Erstellen des Metadata Manager-Dienstes erstellen Sie die Repository-Tabellen und importieren Modelle für Metadatenquellen.

1. Wählen Sie im Navigator den Metadata Manager-Dienst aus.
2. Klicken Sie auf **Aktionen > Repository-Inhalte > Erstellen**.
3. Klicken Sie auf **OK**.

Nach dem Erstellen des Metadata Manager-Dienstes erstellen Sie die Anwendungsdienste, die vom Metadata Manager-Dienst abhängig sind.

Erstellen und Konfigurieren des Content-Management-Diensts

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-Diensts

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

Stellen Sie vor dem Erstellen des Content-Management-Dienstes sicher, dass Sie die folgenden Dienste erstellt und aktiviert haben:

Modellrepository-Dienst

Datenintegrationsdienst

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. Beachten Sie die folgenden Richtlinien, wenn Sie den Dienst benennen: <ul style="list-style-type: none"> - Es wird nicht zwischen Groß- und Kleinschreibung unterschieden. - Der Name muss in der Domäne eindeutig sein. - Er darf nicht mehr als 128 Zeichen umfassen. - Er darf nicht mit @ beginnen. - Er darf die folgenden Sonderzeichen nicht enthalten: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! ()] [- Sie können den Namen des Diensts nach dessen Erstellung nicht mehr ändern.
Beschreibung	Beschreibung des Diensts. Er darf nicht mehr als 765 Zeichen umfassen.
Speicherort	Domäne und Ordner, in denen der Dienst erstellt wird. 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 dieser Dienst ausgeführt wird.
HTTP-Port	HTTP-Portnummer für den Content-Management-Dienst
Datenintegrationsdienst	Datenintegrationsdienst für die Zuordnung zum Dienst. 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.
Speicherort der Referenzdaten	Die Verbindung des Referenzdaten-Warehouse, die Sie für den Content-Management-Dienst für den Zugriff auf das Referenzdaten-Warehouse erstellt haben. Klicken Sie auf Auswählen , um die Verbindung auszuwählen.

4. Klicken Sie auf **Weiter**.
Die Seite **Neuer Content-Management-Dienst – Schritt 2 von 2** wird angezeigt.
5. Übernehmen Sie die Standardwerte für die Sicherheitseigenschaften.
6. Wählen Sie **Dienst aktivieren** aus.
Der Modellrepository-Dienst und der Datenintegrationsdienst müssen ausgeführt werden, um den Content-Management-Dienst zu aktivieren.
7. Klicken Sie auf **Fertigstellen**.
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.

Erstellen und Konfigurieren des Analyst-Diensts

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

Erstellen des Analyst-Dienstes

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

Stellen Sie vor dem Erstellen des Analyst-Diensts sicher, dass Sie die folgenden Dienste erstellt und aktiviert haben:

Modellrepository-Dienst

Datenintegrationsdienst

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie auf **Aktionen > Neu > Analyst-Dienst**.
Das Dialogfeld **Neuer Analyst-Dienst** wird geöffnet.
3. Geben Sie auf der Seite **Neuer Analyst-Dienst – Schritt 1 von 6** die folgenden Eigenschaften ein:

Eigenschaft	Beschreibung
Name	Name des Diensts. Beachten Sie die folgenden Richtlinien, wenn Sie den Dienst benennen: <ul style="list-style-type: none">- Es wird nicht zwischen Groß- und Kleinschreibung unterschieden.- Der Name muss in der Domäne eindeutig sein.- Er darf nicht mehr als 128 Zeichen umfassen.- Er darf nicht mit @ beginnen.- Er darf die folgenden Sonderzeichen nicht enthalten: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! ()] [- Sie können den Namen des Diensts nach dessen Erstellung nicht mehr ändern.
Beschreibung	Beschreibung des Diensts. Er darf nicht mehr als 765 Zeichen umfassen.
Speicherort	Domäne und Ordner, in denen der Dienst erstellt wird. 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 dieser Dienst ausgeführt wird.

4. Klicken Sie auf **Weiter**.
Die Seite **Neuer Analyst-Dienst – Schritt 2 von 6** wird angezeigt.
5. Geben Sie die HTTP-Portnummer für die Kommunikation des Analyst Tools mit dem Analyst-Dienst ein.

6. Zum Aktivieren der sicheren Kommunikation zwischen dem Analyst Tool und dem Analyst-Dienst wählen Sie **Sichere Kommunikation aktivieren** aus.

Geben Sie folgende Eigenschaften ein, um die sichere Kommunikation für den Analyst-Dienst zu konfigurieren:

Eigenschaft	Beschreibung
HTTPS-Port	Portnummer, auf der das Analyst Tool bei Aktivierung der sicheren Kommunikation ausgeführt wird. Verwenden Sie eine Portnummer, die sich von der HTTP-Portnummer unterscheidet.
Schlüsselspeicherdatei	Verzeichnis, in dem die Schlüsselspeicherdatei gespeichert wird, die die digitalen Zertifikate enthält.
Schlüsselspeicherpasswort	Klartext-Passwort für die Schlüsselspeicherdatei. Wenn diese Eigenschaft nicht festgelegt ist, verwendet der Analyst-Dienst das Standardpasswort <code>changeit</code> .
SSL-Protokoll	Optional. Gibt das zu verwendende Protokoll an. Legen Sie diese Eigenschaft auf <code>SSL</code> fest.

7. Wählen Sie **Dienst aktivieren** aus.

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

8. Klicken Sie auf **Weiter**.

Die Seite **Neuer Analyst-Dienst – Schritt 3 von 6** wird angezeigt.

9. Geben Sie die folgenden Eigenschaften ein, um den Modellrepository-Dienst mit dem Analyst-Dienst zu verbinden:

Beschreibung	Eigenschaft
Modellrepository-Dienst	Modellrepository-Dienst zum Zuweisen zum Dienst.
Benutzername	Benutzername, den der Dienst für den Zugriff auf den Modellrepository-Dienst verwendet. Geben Sie den Modellrepository-Benutzer ein, den Sie erstellt haben.
Passwort	Passwort für den Modellrepository-Benutzer.
Sicherheitsdomäne	LDAP-Sicherheitsdomäne für den Benutzer des Modellrepository. Das Feld wird angezeigt, wenn die Informatica-Domäne eine LDAP-Sicherheitsdomäne enthält. Nicht verfügbar für eine Domäne mit Kerberos-Authentifizierung.

10. Damit Benutzer des Analyst Tool mit Human-Task-Daten arbeiten können, legen Sie die **Datenintegrationsdienst**-Eigenschaft mit dem Datenintegrationsdienst fest, den Sie für das Ausführen von Arbeitsabläufen konfigurieren.

Wenn die Benutzer des Analyst Tools keine Human Task-Datensätze bearbeiten müssen, konfigurieren Sie diese Eigenschaft nicht.

11. Klicken Sie auf **Weiter**.

Die Seite **Neuer Analyst-Dienst – Schritt 4 von 6** wird angezeigt.

12. Geben Sie die folgenden Laufzeiteigenschaften für den Analyst-Dienst ein:

Eigenschaft	Beschreibung
Datenintegrationsdienst	Datenintegrationsdienst für die Zuordnung zum Dienst. Der Analyst-Dienst verwaltet die Verbindung zu einem Datenintegrationsdienst, mit dem Benutzer Datenvorschau-, Mappingspezifikations-, Scorecard- und Profil-Jobs im Analyst Tool durchführen können. Sie können den Analyst-Dienst mit dem Datenintegrationsdienst verbinden, den Sie für die Ausführung von Arbeitsabläufen konfiguriert haben. Oder Sie können den Analyst-Dienst für verschiedene Vorgänge verschiedenen Datenintegrationsdiensten zuordnen.
Verzeichnis des Einfachdatei-Cache	Verzeichnis des Einfachdatei-Cache, in dem das Analyst Tool hochgeladene Einfachdateien speichert. Der Datenintegrationsdienst muss auch in der Lage sein, auf dieses Verzeichnis zuzugreifen. Wenn der Analyst-Dienst und der Datenintegrationsdienst auf verschiedenen Knoten ausgeführt werden, konfigurieren Sie das Einfachdateiverzeichnis zur Verwendung eines freigegebenen Verzeichnisses.

13. Klicken Sie auf **Weiter**.

Die Seite **Neuer Analyst-Dienst – Schritt 6 von 5** wird angezeigt.

14. Geben Sie das Verzeichnis zum Speichern der temporären Unternehmensglossardateien ein, die der Unternehmensglossar-Exportprozess erstellt. Geben Sie außerdem das Verzeichnis ein, in dem Dateien gespeichert werden sollen, die von Content-Managern den Glossarobjekten angehängt werden. Diese Verzeichnisse müssen sich auf dem Knoten befinden, auf dem der Analyst-Dienst ausgeführt wird.

15. Klicken Sie auf **Fertig stellen**.

Die Domäne erstellt und aktiviert den Analyst-Dienst.

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

Nach dem Erstellen des Analyst-Dienstes

Nachdem Sie den Analyst-Dienst erstellt haben, erstellen Sie den Suchdienst, der vom Analyst-Dienst abhängig ist.

Erstellen und Konfigurieren des Suchdiensts

Der Suchdienst führt Suchvorgänge im Analyst-Tool durch. Er gibt Suchergebnisse aus dem Profiling-Warehouse und dem Modellrepository zurück, einschließlich Datenobjekten, Zuordnungsspezifikationen und Scorecards.

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

Erstellen des Suchdienstes

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

Stellen Sie vor dem Erstellen des Suchdienstes sicher, dass Sie die folgenden Dienste erstellt und aktiviert haben:

Modellrepository-Dienst

Datenintegrationsdienst

Analyst-Dienst

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie auf **Aktionen > Neu > Suchdienst**.
Das Dialogfeld **Neuer Suchdienst** wird geöffnet.
3. Geben Sie auf der Seite **Neuer Suchdienst – Schritt 1 von 2** die folgenden Eigenschaften ein:

Eigenschaft	Beschreibung
Name	Name des Diensts. Beachten Sie die folgenden Richtlinien, wenn Sie den Dienst benennen: <ul style="list-style-type: none">- Es wird nicht zwischen Groß- und Kleinschreibung unterschieden.- Der Name muss in der Domäne eindeutig sein.- Er darf nicht mehr als 128 Zeichen umfassen.- Er darf nicht mit @ beginnen.- Er darf die folgenden Sonderzeichen nicht enthalten: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! ()] [- Sie können den Namen des Diensts nach dessen Erstellung nicht mehr ändern.
Beschreibung	Beschreibung des Diensts. Er darf nicht mehr als 765 Zeichen umfassen.
Speicherort	Domäne und Ordner, in denen der Dienst erstellt wird. 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 dieser Dienst ausgeführt wird.

4. Klicken Sie auf **Weiter**.
Die Seite **Neuer Suchdienst – Schritt 2 von 2** wird angezeigt.
5. Geben Sie die folgenden Sucheigenschaften für den Suchdienst ein:

Beschreibung	Eigenschaft
Portnummer	Die Portnummer für den Suchdienst.
Indexspeicherort	Das Verzeichnis, das die Suchindex-Dateien enthält. Geben Sie ein Verzeichnis auf dem Computer ein, auf dem der Suchdienst ausgeführt wird. Wenn das Verzeichnis nicht existiert, erstellt Informatica das Verzeichnis beim Erstellen des Suchdienstes.
Extraktionsintervall	Das Intervall in Sekunden, in dem der Suchdienst aktualisierten Inhalt extrahiert und indiziert. Standardwert ist 60 Sekunden.

Beschreibung	Eigenschaft
Modellrepository-Dienst	Modellrepository-Dienst zum Zuweisen zum Dienst.
Benutzername	Benutzername, den der Dienst für den Zugriff auf den Modellrepository-Dienst verwendet. Geben Sie den Modellrepository-Benutzer ein, den Sie erstellt haben.
Passwort	Passwort für den Modellrepository-Benutzer.
Sicherheitsdomäne	LDAP-Sicherheitsdomäne für den Benutzer des Modellrepository. Das Feld wird angezeigt, wenn die Informatica-Domäne eine LDAP-Sicherheitsdomäne enthält. Nicht verfügbar für eine Domäne mit Kerberos-Authentifizierung.

6. Klicken Sie auf **Fertig stellen**.

Die Domäne erstellt den Suchdienst. Die Domäne aktiviert den Suchdienst während des Diensterstellungsprozesses nicht. Sie müssen den Dienst aktivieren, bevor Benutzer Suchen im Analyst-Tool und im Business Glossary-Desktop durchführen können.

7. Wählen Sie zum Aktivieren des Suchdienstes den Dienst im Navigator aus und klicken Sie auf **Aktionen > Dienst aktivieren**.

Sie können den Suchdienst nur aktivieren, wenn der Modellrepository-Dienst, der Datenintegrationsdienst und der Analyst-Dienst ausgeführt werden.

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

Teil V: Installation des Informatica-Client

Dieser Teil enthält die folgenden Kapitel:

- [Installieren der Clients, 312](#)
- [Installation im automatischen Modus , 320](#)

KAPITEL 15

Installieren der Clients

Dieses Kapitel umfasst die folgenden Themen:

- [Installieren der Clients - Übersicht, 312](#)
- [Vor dem Installieren, 313](#)
- [Installieren der Clients, 314](#)
- [Nach der Installation, 315](#)
- [Starten von PowerCenter Client, 318](#)
- [Starten des Developer Tools, 318](#)

Installieren der Clients - Übersicht

Sie können sie unter Windows im Grafikmodus oder automatisch installieren.

Führen Sie die Vorinstallationsaufgaben zur Vorbereitung auf die Installation durch. Sie können die Informatica-Clients auf mehreren Computern installieren.

Beim Ausführen des Clientinstallationsprogramms können Sie die folgenden Informatica-Client-Tools auswählen:

Informatica Developer

Informatica Developer ist eine Clientanwendung, die Sie zum Erstellen von Datenobjekten und virtuellen Datenbanken sowie zum Erstellen und Ausführen von Zuordnungen verwenden.

PowerCenter Client

Der PowerCenter Client enthält mehrere Tools, die zum Verwalten des PowerCenter-Repositorys sowie von Zuordnungen und Sitzungen verwendet werden können.

Hinweis: Informatica empfiehlt, dass Sie die Informatica-Dienste und den PowerCenter Client in verschiedenen Verzeichnissen installieren. Wenn Sie die Informatica-Dienste und den PowerCenter Client im selben Installationsverzeichnis installieren, werden die Dienstbinärdateien deinstalliert, wenn Sie den PowerCenter Client deinstallieren.

Vor dem Installieren

Stellen Sie vor dem Installieren der Informatica-Clients unter Windows sicher, dass die minimalen System- und Drittanbietersoftware-Anforderungen erfüllt sind. Wenn der Computer, auf dem Sie die Informatica-Clients installieren möchten, nicht ordnungsgemäß konfiguriert ist, kann die Installation fehlschlagen.

Überprüfen der Prüfsumme des Installationspakets

Überprüfen Sie vor der Ausführung des Client-Installationsprogramms mit dem Befehl „cksum“ die Integrität des Installationspakets. Mit dem Befehl „cksum“ wird der Prüfsummenwert für das Installationsprogramm berechnet.

Vergleichen Sie die Prüfsumme für die spezifischen Installationsdateien mit der Prüfsumme der Installationsdateien, die von der Informatica Electronic Software-Download-Site heruntergeladen wurden.

In der folgenden Tabelle werden die Prüfsumme und die Dateigröße für den Informatica-Client unter Windows aufgelistet:

Datei	Prüfsummenwert	Dateigröße
informatica_1059_client_winem-64t.zip	1232188873	4021746298 Byte

Zu einer nicht übereinstimmenden Prüfsumme kann es kommen, wenn während des Downloads aufgrund von Netzwerkproblemen Datenfehler auftreten oder wenn Daten in der Datei auf der Festplatte beschädigt werden. Weitere Informationen zu Prüfsummenfehlern finden Sie unter [HOW TO: Identify file errors after downloading Informatica installation files](#).

Überprüfen der Systemvoraussetzungen

Bevor Sie den Client installieren, überprüfen Sie, ob die folgenden Installationsanforderungen zur Installation und Ausführung des Clients erfüllt sind:

Speicherplatz für die temporären Dateien

Das Installationsprogramm schreibt temporäre Dateien auf die Festplatte. Stellen Sie sicher, dass für die Installation 1 GB Speicherplatz auf dem Computer vorhanden ist. Nach Abschluss der Installation werden die temporären Dateien gelöscht und der Speicherplatz wird freigegeben.

Berechtigungen zur Installation

Stellen Sie sicher, dass das Benutzerkonto, das Sie zum Installieren des Clients verwenden, keine Schreibberechtigung für das Installationsverzeichnis und die Windows-Registrierung hat.

Mindestsystemanforderungen

In der folgenden Tabelle werden die Mindestsystemanforderungen für das Ausführen des Clients aufgelistet:

Prozessor	RAM	Festplattenspeicher
1 CPU	1 GB	6 GB

Überprüfen von Drittanbieteranforderungen für Informatica Developer

Überprüfen Sie vor der Installation des Developer Tools die folgenden Drittanbieter-Installationsanforderungen:

- Installieren Sie .NET Framework 4.0 oder höher. Wenn Sie planen, Datenprozessor- oder Umwandlungen von hierarchisch auf relational zu verwenden, müssen Sie .NET Framework installieren, bevor Sie das Developer Tool installieren.
- Installieren Sie die neueste Version von Microsoft Visual C++ Redistributable Package (x64), bevor Sie das Developer Tool verwenden oder installieren. Sie können es von der Microsoft-Website herunterladen.

Überprüfen von Drittanbieteranforderungen für den PowerCenter Client

Die PowerCenter Client-Installation enthält Mapping Architect for Visio und Mapping Analyst for Excel. Überprüfen Sie Drittanbieteranforderungen sowohl für Mapping Architect for Visio als auch für Mapping Analyst for Excel, bevor Sie den PowerCenter Client installieren.

Überprüfen von Drittanbieteranforderungen für Mapping Architect for Visio

Wenn Sie Mapping Architect for Visio verwenden möchten, installieren Sie die folgende Software von Drittanbietern, bevor Sie den PowerCenter Client installieren:

- Version 2007 oder 2010 von Microsoft Visio
- Microsoft .NET Framework 3.5.1
- Microsoft .NET Framework 4.0

Wichtig: Wenn Sie nicht die richtige Version und das richtige Service Pack von Microsoft .NET Framework installieren, wird Mapping Architect for Visio nicht ordnungsgemäß installiert.

Überprüfen von Drittanbieteranforderungen für Mapping Analyst for Excel

Mapping Analyst for Excel enthält ein Excel-Add-In, das ein Metadatenmenü oder ein Menüband zu Microsoft Excel hinzufügt. Sie können das Add-In nur für Excel 2016 installieren. Wenn Sie Mapping Architect for Excel verwenden möchten, installieren Sie die folgende Software von Drittanbietern, bevor Sie den PowerCenter Client installieren:

- Microsoft Office Excel Version 2016
- Java-Version 1.8 oder höher

Installieren der Clients

Führen Sie die folgenden Schritte aus, um das Client-Tool zu installieren:

1. Schließen Sie alle anderen Anwendungen.
2. Wechseln Sie in das Stammverzeichnis für die Installationsdateien und führen Sie die Datei install.bat als Administrator aus.

Klicken Sie zum Ausführen der Datei als Administrator mit der rechten Maustaste auf die Datei install.bat und wählen Sie **Als Administrator ausführen** aus.

Hinweis: Wenn Sie das Installationsprogramm nicht als Administrator ausführen, meldet der Windows-Systemadministrator möglicherweise Probleme beim Zugriff auf die Dateien im Informatica-Installationsverzeichnis.

Wenn beim Ausführen der Datei install.bat im Stammverzeichnis Probleme auftreten, führen Sie die folgende Datei aus: <Verzeichnis der Installationsdateien>\client\install.exe

3. Wählen Sie **Informatica <Version>-Clients installieren** aus und klicken Sie auf **Weiter**.
4. Die Seite **Installationsvoraussetzungen** zeigt die Systemanforderungen an. Vergewissern Sie sich, dass alle Voraussetzungen für die Installation erfüllt sind, bevor Sie die Installation fortsetzen.
5. Geben Sie auf der Seite **Installationsverzeichnis** den absoluten Pfad für das Installationsverzeichnis ein.
Das Installationsverzeichnis muss sich auf dem aktuellen Rechner befinden. Der Pfad darf maximal 260 Zeichen umfassen. Die Verzeichnisnamen in dem Pfad dürfen weder Leerzeichen noch die folgenden Sonderzeichen enthalten: @ | * \$ # ! % () { } [] , ; ' "

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

6. Aktivieren Sie das Kontrollkästchen, wenn Sie Verteilungspakete über das Informatica-Installationsprogramm installieren möchten.
7. Wenn Sie Verteilungspakete installieren möchten, wählen Sie ein oder mehrere Pakete aus der Liste aus, die Sie installieren möchten.
8. Klicken Sie auf **Weiter**.
9. Überprüfen Sie auf der Seite mit der **Vorinstallationsübersicht** die Installationsdaten und klicken Sie auf **Installieren**.

Das Installationsprogramm kopiert die Dateien des Developer Tools in das Installationsverzeichnis.

Auf der Seite **Nach der Installation – Zusammenfassung** wird angezeigt, ob die Installation erfolgreich abgeschlossen wurde.

10. Klicken Sie zum Beenden des Installationsprogramms auf **Fertig**.

In den Installationsprotokolldateien finden Sie weitere Informationen zu den vom Installationsprogramm durchgeführten Aufgaben.

Nach der Installation

Nachdem Sie die Client-Tools installiert haben, können Sie andere Sprachen installieren, die sichere Kommunikation innerhalb der Domäne aktivieren und das Tool starten.

Installation von Sprachen

Zur Anzeige anderer Sprachen als derjenigen des Gebietsschemas und zum Arbeiten mit Repositories, die eine UTF-8-Codepage nutzen, müssen unter Windows weitere Sprachen für die Verwendung mit den Informatica-Clients installiert werden.

Hinweis: Falls Sie die PowerCenter-Clients installiert haben und diese Aufgabe zur Installation von Sprachen durchgeführt haben, müssen Sie diese Aufgabe nicht wiederholen.

Außerdem müssen Sie Sprachen für die Verwendung des Windows Input Method Editor (IME) installieren.

1. Klicken Sie auf **Starten > Einstellungen > Systemsteuerung**.
2. Klicken Sie auf **Regionale Einstellungen**.
3. Wählen Sie unter den Spracheinstellungen für das System die zu installierenden Sprachen aus.
4. Klicken Sie auf **Anwenden**.

Wenn Sie das Systemgebietsschema beim Installieren der Sprache ändern, starten Sie den Windows-Computer neu.

Konfigurieren des Client für eine sichere Domäne

Wenn Sie die sichere Kommunikation innerhalb der Domäne aktivieren, sichern Sie auch Verbindungen zwischen der Domäne und Informatica-Client-Anwendungen. Basierend auf den verwendeten TrustStore-Dateien müssen Sie möglicherweise den Speicherort und das Passwort für die TrustStore-Dateien in Umgebungsvariablen auf jedem Client-Host angeben.

Möglicherweise müssen Sie die folgenden Umgebungsvariablen auf jedem Client-Host festlegen:

INFA_TRUSTSTORE

Legen Sie diese Variable auf das Verzeichnis fest, das die Truststore-Dateien für die SSL-Zertifikate enthält. Das Verzeichnis muss Truststore-Dateien mit der Bezeichnung `infa_truststore.jks` und `infa_truststore.pem` enthalten.

INFA_TRUSTSTORE_PASSWORD

Legen Sie diese Variable auf das Passwort für die Datei `infa_truststore.jks` fest. Das Passwort muss verschlüsselt werden. Verwenden Sie das Befehlszeilenprogramm `pmpasswd` zum Verschlüsseln des Passworts.

Hinweis: `INFA_TRUSTSTORE_PASSWORD` ist optional, wenn Sie einen PowerCenter-Thick-Client oder Befehle wie `pmcmd` oder `pmrep` verwenden. Geben Sie nur für die `infacmd`-Befehle ein Passwort ein.

Informatica stellt ein SSL-Zertifikat zur Verfügung, das Sie zum Sichern der Domäne verwenden können. Wenn Sie die Informatica-Clients installieren, legt das Installationsprogramm die Umgebungsvariablen fest und installiert die TrustStore-Dateien standardmäßig im folgenden Verzeichnis: `<Informatica-Installationsverzeichnis>\clients\shared\security`.

Wenn Sie das SSL-Standardzertifikat von Informatica verwenden und `infa_truststore.jks` und `infa_truststore.pem` sich im Standardverzeichnis befinden, brauchen Sie die Umgebungsvariablen `INFA_TRUSTSTORE` oder `INFA_TRUSTSTORE_PASSWORD` nicht festzulegen.

In den folgenden Szenarios müssen Sie die Umgebungsvariablen `INFA_TRUSTSTORE` und `INFA_TRUSTSTORE_PASSWORD` auf jedem Client-Host festlegen:

Sie verwenden ein benutzerdefiniertes SSL-Zertifikat zum Sichern der Domäne.

Wenn Sie ein SSL-Zertifikat bereitstellen, um die Domäne zu sichern, kopieren Sie die TrustStore-Dateien `infa_truststore.jks` und `infa_truststore.pem` auf jeden Client-Host. Sie müssen den Speicherort der Dateien und das Truststore-Passwort angeben.

Sie verwenden das SSL-Standardzertifikat von Informatica, die Truststore-Dateien befinden sich aber nicht im Informatica-Standardverzeichnis.

Wenn Sie das SSL-Standardzertifikat von Informatica verwenden, aber sich die TrustStore-Dateien `infa_truststore.jks` und `infa_truststore.pem` nicht im Informatica-Standardverzeichnis befinden, müssen Sie den Speicherort der Dateien und das TrustStore-Passwort angeben.

Hinweis: Wenn Sie eine Verbindung zwischen der Informatica-Domäne und dem PowerCenter-Client herstellen, ist es nicht zwingend erforderlich, die Umgebungsvariable `INFA_TRUSTSTORE_PASSWORD`

festzulegen. Sie können eine Verbindung herstellen, indem Sie nur die Variable `INFA_TRUSTSTORE` konfigurieren. Bevor Sie diese Umgebungsvariablen festlegen, lesen Sie die folgenden Richtlinien:

- Mit der Datei `infa_truststore.jks` ist ein Passwort verknüpft, während mit der Datei `infa_truststore.pem` kein Passwort verknüpft ist.
- Wenn Sie nur den PowerCenter-Client installiert haben, ist es nicht erforderlich, die Umgebungsvariable `INFA_TRUSTSTORE_PASSWORD` zu konfigurieren.

Konfigurieren des Workspace-Verzeichnisses für das Developer-Tool

Konfigurieren Sie Informatica Developer so, dass die Workspace-Metadaten in den Computer geschrieben werden, auf dem der Benutzer angemeldet ist.

Hinweis: Falls Sie die PowerCenter-Clients installiert haben und diese Aufgabe durchgeführt haben, müssen Sie diese Aufgabe nicht wiederholen.

1. Wechseln Sie zum folgenden Verzeichnis: `<Informatica-Installationsverzeichnis>\clients\DeveloperClient\configuration\`
2. Suchen Sie die Datei `config.ini`.
3. Erstellen Sie eine Sicherungskopie der Datei `config.ini`.
4. Öffnen Sie die Datei `config.ini` in einem Texteditor.
5. Fügen Sie die Variable `osgi.instance.area.default` an das Ende der Datei `config.ini` an, und stellen Sie die Variable auf den Verzeichnisort ein, wo Sie die Workspace-Metadaten speichern möchten. Der Dateipfad darf keine Nicht-ANSI-Zeichen enthalten. Ordernamen im Workspace-Verzeichnis dürfen nicht das Nummernzeichen (#) enthalten. Wenn Ordernamen im Workspace-Verzeichnis Leerzeichen enthalten, umschließen Sie das gesamte Verzeichnis mit doppelten Anführungszeichen.

- Wenn Sie Informatica Developer vom lokalen Computer aus ausführen, stellen Sie die Variable auf den absoluten Pfad des Workspace-Verzeichnisses ein:

```
osgi.instance.area.default=<Drive>/<WorkspaceDirectory>
```

oder

```
osgi.instance.area.default=<Drive>\\<WorkspaceDirectory>
```

- Wenn Sie Informatica Developer von einem Remote-Computer aus ausführen, stellen Sie die Variable auf den Verzeichnisort des lokalen Computers ein:

```
osgi.instance.area.default=\\\\<LocalMachine>/<WorkspaceDirectory>
```

oder

```
osgi.instance.area.default=\\\\<LocalMachine>\\<WorkspaceDirectory>
```

Der Benutzer muss über eine Schreibberechtigung für das Workspace-Verzeichnis verfügen.

Informatica Developer schreibt die Workspace-Metadaten in das Workspace-Verzeichnis. Wenn Sie sich in Informatica Developer von einem lokalen Computer aus anmelden, schreibt Informatica Developer die Workspace-Metadaten in den lokalen Computer. Wenn das Workspace-Verzeichnis nicht auf dem Computer existiert, auf dem Sie angemeldet sind, erstellt Informatica Developer das Verzeichnis beim Schreiben der Dateien.

Sie können das Workspace-Verzeichnis überschreiben, wenn Sie Informatica Developer starten.

Starten von PowerCenter Client

Beim Starten von PowerCenter Client wird eine Verbindung zu einem PowerCenter-Repository hergestellt.

1. Klicken Sie im Windows-Startmenü auf **Programme > Informatica[Version] > Client > [Name des Client-Tools]**.

Beim ersten Ausführen eines PowerCenter Client-Tools müssen Sie ein Repository hinzufügen und eine Verbindung dazu herstellen

2. Klicken Sie auf **Repository > Repository hinzufügen**.

Das Dialogfeld **Repository hinzufügen** wird angezeigt.

3. Geben Sie den Repository- und den Benutzernamen ein.

4. Klicken Sie auf **OK**.

Das Repository wird im Navigator angezeigt.

5. Klicken Sie auf **Repository > Verbinden**.

Das Dialogfeld für das Verbinden mit dem Repository wird angezeigt.

6. Klicken Sie im Abschnitt mit den Verbindungseinstellungen auf **Hinzufügen**, um die Informationen zur Domänenverbindung einzugeben.

Das Dialogfeld **Domäne hinzufügen** wird angezeigt.

7. Geben Sie den Domännennamen, den Gateway-Host und die Gateway-Portnummer ein.

8. Klicken Sie auf **OK**.

9. Geben Sie in das Dialogfeld **Mit Repository verbinden** das Passwort für den Administrator-Benutzer ein.

10. Wählen Sie die Sicherheitsdomäne.

11. Klicken Sie auf **Verbinden**.

Nachdem die Verbindung zum Repository hergestellt wurde, können Sie Objekte erstellen.

Starten des Developer Tools

Beim Starten des Developer Tools wird eine Verbindung zu einem Model-Repository hergestellt. Im Model-Repository werden im Developer Tool erstellte Metadaten gespeichert. Der Model Repository Service verwaltet das Model Repository. Stellen Sie daher eine Verbindung zum Repository her, bevor Sie ein Projekt erstellen.

1. Klicken Sie im Windows-Startmenü auf **Programme > Informatica[Version] > Client > Developer Client > Informatica Developer starten**.

Beim ersten Ausführen des Developer Tools wird die Begrüßungsseite mit mehreren Symbolen angezeigt. Beim nachfolgenden Ausführen des Developer Tools wird die Begrüßungsseite nicht mehr angezeigt.

2. Klicken Sie auf **Workbench**.

Beim ersten Starten des Entwicklertools müssen Sie das Repository auswählen, in dem die Objekte, die Sie erstellen, gespeichert werden sollen

3. Klicken Sie auf **Datei > Mit Repository verbinden**.

Das Dialogfeld **Mit Repository verbinden** wird eingeblendet.

4. Wenn Sie im Developer Tool keine Domäne konfiguriert haben, klicken Sie auf **Domänen konfigurieren**, um eine Domäne zu konfigurieren.

Sie müssen eine Domäne konfigurieren, um auf einen Model Repository Service zugreifen zu können.

5. Klicken Sie auf **Hinzufügen**, um eine Domäne hinzuzufügen.

Das Dialogfeld **Neue Domäne** wird eingeblendet

6. Geben Sie den Domänennamen, den Hostnamen und die Portnummer ein.

7. Klicken Sie auf **Fertigstellen**.

8. Klicken Sie auf **OK**.

9. Klicken Sie im Dialogfeld **Mit Repository verbinden** auf **Durchsuchen** und wählen Sie den Model Repository Service aus.

10. Klicken Sie auf **OK**.

11. Klicken Sie auf **Weiter**.

12. Geben Sie einen Benutzernamen und ein Passwort ein.

13. Klicken Sie auf **Fertigstellen**.

Das Model Repository wird der Objekt-Explorer-Ansicht hinzugefügt. Beim nächsten Ausführen des Developer-Tools können Sie eine Verbindung zum selben Repository herstellen.

KAPITEL 16

Installation im automatischen Modus

Dieses Kapitel umfasst die folgenden Themen:

- [Übersicht über die Installation im automatischen Modus, 320](#)
- [Konfigurieren der Eigenschaftendatei, 320](#)
- [Ausführen des automatischen Installationsprogramms, 321](#)

Übersicht über die Installation im automatischen Modus

Beim automatischen Installieren der Informatica-Clients ist keinerlei Benutzereingriff erforderlich.

Geben Sie die Installationsoptionen mithilfe einer Eigenschaftendatei an. Das Installationsprogramm liest die Datei, um die Installationsoptionen festzustellen. Mit der automatischen Installation können Sie die Informatica-Clients auf mehreren Computern im Netzwerk installieren oder die Installation auf den verschiedenen Computern standardisieren.

Gehen Sie zum automatischen Installieren folgendermaßen vor:

1. Konfigurieren Sie die Installationseigenschaftendatei und geben Sie darin die Installationsoptionen an.
2. Führen Sie das Installationsprogramm mit der Installationseigenschaftendatei aus.

Konfigurieren der Eigenschaftendatei

Informatica stellt eine Beispielseigenschaftendatei bereit, die die vom Installationsprogramm benötigten Eigenschaften enthält. Erstellen Sie eine Eigenschaftendatei, indem Sie die Beispieldatei anpassen und die Optionen für Ihre Installation festlegen. Führen Sie anschließend die Installation im Hintergrund aus.

Die Beispieldatei „SilentInput.properties“ befindet sich im Downloadverzeichnis des Installationsprogramms.

1. Wechseln Sie zum Verzeichnis-Root, der den Installer enthält.
2. Suchen Sie die Beispieldatei `SilentInput.properties`.
3. Erstellen Sie eine Sicherungskopie der Datei `SilentInput.properties`.

4. Verwenden Sie einen Texteditor, um die Datei zu öffnen, und ändern Sie die Werte der Eigenschaften. In der folgenden Tabelle werden die Installationseigenschaften beschrieben, die Sie ändern können:

Eigenschaftsname	Beschreibung
INSTALL_TYPE	Zeigt an, ob Informatica-Clients installiert oder upgegradet werden müssen. Wenn der Wert 0 ist, werden die Informatica-Clients in dem von Ihnen festgelegten Verzeichnis installiert. Wenn der Wert 1 ist, werden die Informatica-Clients upgegradet. Der Standardwert ist 0.
USER_INSTALL_DIR	Installationsverzeichnis des Informatica-Clients.
DXT_COMP	Zeigt an, ob Informatica Developer installiert werden muss. Wenn der Wert 1 ist, wird das Developer-Tool installiert. Wenn der Wert 0 ist, wird das Developer-Tool nicht installiert. Standard ist 1.
INSTALL_HADOOP_LIBRARIES	Legt fest, ob Verteilungspakete über das Installationsprogramm installiert werden sollen. Legen Sie den Wert auf „true“ fest, wenn Sie Verteilungspakete über das Installationsprogramm installieren möchten. Legen Sie den Wert auf „false“ fest, wenn Sie keine Verteilungspakete benötigen oder diese später installieren möchten.
SELECTED_HADOOP_LIBRARIES	Gibt die zu installierenden Integrationspakete in der Liste der unterstützten Pakete an. Geben Sie die Verteilungspakete ein, die installiert werden sollen. Trennen Sie mehrere Verteilungspakete jeweils durch ein Komma.

5. Speichern Sie die Eigenschaftendatei.

Ausführen des automatischen Installationsprogramms

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

1. Öffnen Sie die Eingabeaufforderung.
2. Wechseln Sie zum Root-Verzeichnis, das die Installationsdateien enthält.
3. Stellen Sie sicher, dass das Verzeichnis die Datei SilentInput.properties enthält, die Sie bearbeitet und erneut gespeichert haben.

4. Zum Ausführen der automatischen Installation führen Sie silentInstall.bat aus.

Die automatische Installation wird im Hintergrund ausgeführt. Der Vorgang kann eine Weile dauern. Die automatische Installation ist abgeschlossen, wenn die Datei

„Informatica_<Version>_Client_InstallLog<Zeitstempel>.log“ im Installationsverzeichnis erstellt ist.

Die automatische Installation schlägt fehl, wenn die Eigenschaftendatei nicht ordnungsgemäß konfiguriert oder der Zugriff auf das Installationsverzeichnis nicht möglich ist. Zeigen Sie die Installationsprotokolldateien an und korrigieren Sie die Fehler. Führen Sie die automatische Installation anschließend noch einmal aus.

Teil VI: Deinstallation

- [Deinstallation, 324](#)

KAPITEL 17

Deinstallation

Dieses Kapitel umfasst die folgenden Themen:

- [Deinstallation von Informatica – Übersicht, 324](#)
- [Regeln und Richtlinien für die Deinstallation, 324](#)
- [Deinstallieren des Informatica-Servers im Konsolenmodus, 325](#)
- [Deinstallieren des Informatica-Servers im automatischen Modus, 326](#)
- [Deinstallieren des Informatica-Servers im Grafikmodus, 326](#)
- [Deinstallation von Informatica-Clients, 327](#)

Deinstallation von Informatica – Übersicht

Deinstallieren Sie Informatica, um den Informatica-Server und die Informatica-Clients von einem Computer zu entfernen.

Der Informatica-Deinstallationsvorgang löscht alle Informatica-Dateien und -Konfigurationen von einem Computer. Dateien, die nicht mit Informatica installiert wurden, werden bei der Deinstallation nicht gelöscht. Beispiel: Beim Installationsvorgang werden temporäre Verzeichnisse erstellt. Bei der Deinstallation werden keine Aufzeichnungen zu diesen Verzeichnissen aufbewahrt, daher können sie nicht gelöscht werden. Zur Vervollständigung der Deinstallation müssen Sie diese Verzeichnisse manuell löschen.

Wichtig: Bei Installation von PowerCenter Client und den Informatica-Diensten in demselben Installationsverzeichnis werden die Programmdateien deinstalliert, wenn Sie den PowerCenter Client deinstallieren

Regeln und Richtlinien für die Deinstallation

Halten Sie sich an die folgenden Regeln und Richtlinien, wenn Sie Informatica-Komponenten deinstallieren:

- Der Deinstallationsmodus von Informatica hängt vom Modus ab, den Sie zum Installieren des Informatica-Servers verwendet haben. Wenn Sie den Informatica-Server beispielsweise im Konsolenmodus installiert haben, wird das Deinstallationsprogramm ebenfalls im Konsolenmodus ausgeführt. Der Deinstallationsmodus der Informatica-Clients hängt nicht von dem Modus ab, den Sie zum Installieren der Informatica-Clients verwendet haben. Wenn Sie die Informatica-Clients beispielsweise im automatischen Modus installiert haben, kann das Deinstallationsprogramm im Grafikmodus oder im automatischen Modus ausgeführt werden.

- Die Deinstallation von Informatica hat keine Auswirkungen auf die Informatica-Repositorys. Das Deinstallationsprogramm entfernt die Informatica-Dateien. Es entfernt keine Repositorys aus der Datenbank. Wenn Sie die Repositorys verschieben müssen, können Sie ein Backup von ihnen erstellen und sie dann in einer anderen Datenbank wiederherstellen.
- Bei der Deinstallation von Informatica werden die Metadatentabellen nicht aus der Domänenkonfigurationsdatenbank entfernt. Wenn Sie Informatica 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.
- Bei der Deinstallation von Informatica werden alle Installationsdateien und Unterverzeichnisse aus dem Informatica-Installationsverzeichnis entfernt. Bevor Sie Informatica deinstallieren, halten Sie alle Informatica-Dienste und -Prozesse an und stellen Sie sicher, dass alle Dateien im Installationsverzeichnis geschlossen sind. Am Ende des Deinstallationsvorgangs zeigt das Deinstallationsprogramm die Namen der Dateien und Verzeichnisse an, die nicht entfernt werden konnten.
- Bei der Installation des Informatica-Servers wird für Dateien und Bibliotheken, die mithilfe der Informatica Developer Platform-APIs erstellten Drittanbieteradaptoren benötigt werden, der folgende Ordner erstellt:
`<Informatica-Installationsverzeichnis>/services/shared/extensions`
 Bei der Deinstallation des Informatica-Servers werden dieser Ordner und alle erstellten Unterordner gelöscht. Wenn Sie im Ordner `/extensions` Adapterdateien gespeichert haben, müssen Sie ein Backup des Ordners erstellen, bevor Sie mit der Deinstallation beginnen.
- Wenn Sie die Deinstallation auf einem Computer ausführen, müssen Sie vor der Deinstallation ein Backup des ODBC-Ordners erstellen. Stellen Sie den Ordner nach Abschluss der Deinstallation wieder her.

Deinstallieren des Informatica-Servers im Konsolenmodus

Wenn Sie den Informatica-Server im Konsolenmodus installiert haben, erfolgt die Deinstallation des Informatica-Servers ebenfalls im Konsolenmodus.

Bevor Sie das Deinstallationsprogramm auszuführen, halten Sie alle Informatica-Dienste und -Prozesse an und stellen Sie sicher, dass alle Dateien im Installationsverzeichnis geschlossen sind. Der Deinstallationsvorgang kann keine Dateien löschen, die geöffnet sind oder von einem gerade ausgeführten Dienst oder Prozess verwendet werden.

1. Gehen Sie zu folgendem Verzeichnis:

```
<Informatica-Installationsverzeichnis>/Uninstaller_Server
```

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

```
./uninstaller.sh
```

Wenn Sie den Informatica-Server im Konsolenmodus installiert haben, dann startet das Deinstallationsprogramm ebenfalls im Konsolenmodus.

Deinstallieren des Informatica-Servers im automatischen Modus

Wenn Sie den Informatica-Server im automatischen Modus installiert haben, erfolgt die Deinstallation des Informatica-Servers ebenfalls im automatischen Modus.

Bevor Sie das Deinstallationsprogramm auszuführen, halten Sie alle Informatica-Dienste und -Prozesse an und stellen Sie sicher, dass alle Dateien im Installationsverzeichnis geschlossen sind. Der Deinstallationsvorgang kann keine Dateien löschen, die geöffnet sind oder von einem gerade ausgeführten Dienst oder Prozess verwendet werden.

1. Gehen Sie zu folgendem Verzeichnis:

```
<Informatica-Installationsverzeichnis>/Uninstaller_Server
```

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

```
./uninstaller.sh
```

Wenn Sie den Informatica-Server im automatischen Modus installiert haben, dann startet das Deinstallationsprogramm ebenfalls im automatischen Modus. Die automatische Deinstallation wird im Hintergrund ausgeführt. Der Vorgang kann eine Weile dauern. Die automatische Deinstallation schlägt fehl, wenn kein Zugriff auf das Installationsverzeichnis besteht.

Nachdem Sie den Informatica-Server deinstalliert haben, löschen Sie alle übrigen Ordner und Dateien aus dem Informatica-Installationsverzeichnis. Beispiel:

- Datei Informatica_<Version>_Services_InstallLog.log
- Datei Informatica_<Version>_Services_<timestamp>.log

Deinstallieren des Informatica-Servers im Grafikmodus

Bevor Sie das Deinstallationsprogramm auszuführen, halten Sie alle Informatica-Dienste und -Prozesse an und stellen Sie sicher, dass alle Dateien im Installationsverzeichnis geschlossen sind. Der Deinstallationsvorgang kann keine Dateien löschen, die geöffnet sind oder von einem gerade ausgeführten Dienst oder Prozess verwendet werden.

1. Klicken Sie auf **Start > Programmdateien > Informatica [Version] > Server > Deinstallationsprogramm**. Die Seite **Deinstallation** wird angezeigt.
2. Klicken Sie auf **Deinstallieren**, um die Deinstallation zu beginnen.
Nachdem das Installationsprogramm alle Informatica-Dateien aus dem Verzeichnis gelöscht hat, wird die Seite **Deinstallations-Zusammenfassung** angezeigt.
3. Klicken Sie auf **Fertig**, um das Deinstallationsprogramm zu schließen.

Nachdem Sie den Informatica-Server deinstalliert haben, löschen Sie alle übrigen Ordner und Dateien aus dem Informatica-Installationsverzeichnis. Beispiel:

- Datei Informatica_<Version>_Client_InstallLog.log
- Datei Informatica_<Version>_Client.log

Melden Sie sich vom Computer ab und wieder an. Löschen Sie danach die Informatica-spezifischen CLASSPATH und PATH-Umgebungsvariablen.

Deinstallation von Informatica-Clients

Sie können die Informatica-Clients im Grafikmodus und automatischen Modus unter Windows deinstallieren.

Wenn Sie Informatica-Clients deinstallieren, entfernt das Installationsprogramm nicht die INFA_TRUSTSTORE-Umgebungsvariablen, die während der Installation erstellt werden. Wenn Sie eine neuere Version von Informatica-Clients installieren, müssen Sie die Umgebungsvariable bearbeiten, um auf den neuen Wert des SSL-Zertifikats zu zeigen.

Deinstallieren von Informatica-Clients im Grafikmodus

Wenn Sie die Informatica-Clients im Grafikmodus installiert haben, erfolgt die Deinstallation der Informatica-Clients ebenfalls im Grafikmodus.

1. Klicken Sie auf **Start > Programmdateien > Informatica [Version] > Client > Deinstallationsprogramm**.
Die Seite **Deinstallation** wird angezeigt.
2. Klicken Sie auf **Weiter**.
Die Seite **Auswahl zur Deinstallation des Anwendungs-Clients** wird angezeigt.
3. Wählen Sie die gewünschten Client-Anwendungen aus und klicken Sie auf **Deinstallieren**.
4. Klicken Sie auf **Fertig**, um das Deinstallationsprogramm zu schließen.
Nach abgeschlossener Deinstallation werden auf der Seite **Deinstallationsübersicht** die Ergebnisse der Deinstallation angezeigt.

Nachdem Sie die Informatica-Clients deinstalliert haben, löschen Sie alle verbleibenden Ordner und Dateien aus dem Informatica-Installationsverzeichnis. Beispiel:

- Datei Informatica_<Version>_Client_InstallLog.log
- Datei Informatica_<Version>_Client.log

Melden Sie sich vom Computer ab und wieder an. Löschen Sie danach die Informatica-spezifischen Umgebungsvariablen CLASSPATH und PATH.

Deinstallieren von Informatica-Clients im automatischen Modus

Wenn Sie die Informatica-Clients im automatischen Modus installiert haben, erfolgt die Deinstallation der Informatica-Clients ebenfalls im automatischen Modus.

Erstellen der Eigenschaftendatei

Informatica stellt eine Beispiелеigenschaftendatei bereit, die die vom Installationsprogramm benötigten Eigenschaften enthält.

Erstellen Sie eine Eigenschaftendatei, indem Sie die Beispieldatei anpassen und die Optionen für Ihre Deinstallation festlegen. Führen Sie anschließend die automatische Deinstallation aus.

1. Wechseln Sie zum Verzeichnis <Informatica-Installationsverzeichnis>/Uninstaller_Client.
2. Suchen Sie die Beispieldatei `SilentInput.properties`.
3. Erstellen Sie eine Sicherungskopie der Datei `SilentInput.properties`.
4. Verwenden Sie einen Texteditor, um die Eigenschaftendatei zu öffnen und die Werte darin zu ändern.

In der folgenden Tabelle werden die Eigenschaften beschrieben, die Sie ändern können:

Eigenschaftsname	Beschreibung
DXT_COMP	Zeigt an, ob Informatica Developer deinstalliert wird. Wenn der Wert 1 ist, wird das Developer Tool deinstalliert. Wenn der Wert 0 ist, wird das Developer Tool nicht deinstalliert. Der Standardwert ist 1.

5. Speichern Sie die Datei `SilentInput.properties`.

Automatisches Deinstallationsprogramm ausführen

Führen Sie nach dem Konfigurieren der Eigenschaftendatei die automatische Deinstallation aus.

1. Wechseln Sie zu dem Verzeichnis `<Informatica-Installationsverzeichnis>/Uninstaller_Client`.
2. Zum Ausführen der automatischen Installation doppelklicken Sie auf die Datei `uninstaller.bat` oder `uninstaller.exe`.

Die automatische Deinstallation wird im Hintergrund ausgeführt. Der Vorgang kann eine Weile dauern. Die automatische Deinstallation schlägt fehl, wenn die Eigenschaftendatei nicht ordnungsgemäß konfiguriert oder der Zugriff auf das Installationsverzeichnis nicht möglich ist.

Nachdem Sie die Informatica-Clients deinstalliert haben, löschen Sie alle übrigen Ordner und Dateien aus dem Informatica-Installationsverzeichnis. Beispiel:

- Datei `Informatica_<Version>_Client_InstallLog.log`
- Datei `Informatica_<Version>_Client.log`

Melden Sie sich vom Computer ab und wieder an. Löschen Sie danach die Informatica-spezifischen CLASSPATH und PATH-Umgebungsvariablen.

ANHANG A

Starten und Anhalten der Informatica-Dienste

Dieser Anhang umfasst die folgenden Themen:

- [Starten und Anhalten der Informatica-Dienste - Übersicht , 329](#)
- [Starten oder Beenden der Informatica-Dienste über die Konsole, 330](#)
- [Beenden von Informatica in Informatica Administrator, 330](#)
- [Starten oder Beenden von Informatica über die Systemsteuerung, 330](#)
- [Starten oder Anhalten von Informatica über das Startmenü, 331](#)
- [Starten bzw. Anhalten von Informatica über eine Eingabeaufforderung, 331](#)
- [Regeln und Richtlinien zum Starten oder Beenden von Informatica, 331](#)

Starten und Anhalten der Informatica-Dienste - Übersicht

Der Informatica-Dienst führt den Dienstmanager auf dem Knoten aus. Der Dienstmanager erweitert alle Domänenfunktionen und startet Anwendungsdienste, die zum Ausführen auf dem Knoten konfiguriert sind. Die Methode zum Starten oder Beenden von Informatica hängt vom Betriebssystem ab. Sie können mit Informatica Administrator einen Knoten ausschalten. Bei Ausschalten eines Knotens wird Informatica auf diesem Knoten beendet.

Der Informatica-Dienst führt auch Informatica Administrator aus. Mit Informatica Administrator können Sie die Informatica-Domänenobjekte und -Benutzerkonten verwalten. Melden Sie sich bei Informatica Administrator an, um die Benutzerkonten für Informatica-Benutzer zu erstellen und die Anwendungsdienste in der Domäne zu erstellen und zu konfigurieren.

Starten oder Beenden der Informatica-Dienste über die Konsole

Führen Sie `infaservice.sh` aus, um den Informatica-Daemon zu starten und zu stoppen. `infaservice.sh` ist standardmäßig im folgenden Verzeichnis installiert:

```
<Informatica installation directory>/tomcat/bin
```

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

```
infaservice.sh startup
```

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

```
infaservice.sh shutdown
```

Hinweis: Starten Sie Informatica-Knoten immer mit einem Nicht-Root-Benutzer. Wenn Sie den Speicherort von `infaservice.sh` mithilfe eines Softlinks festlegen, stellen Sie die Umgebungsvariable `INFA_HOME` auf den Speicherort des Informatica-Installationsverzeichnis ein.

Beenden von Informatica in Informatica Administrator

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

Sie können die laufenden Vorgänge abbrechen oder zum Abschluss bringen, bevor der Dienst geschlossen wird. Wenn Sie einen Knoten ausschalten und die Repository Service-Prozesse abbrechen, die auf dem Knoten ausgeführt werden, können Änderungen verloren gehen, die noch nicht in das Repository geschrieben wurden. Wenn Sie einen Knoten ausschalten, auf dem Integrations-Dienstvorgänge ausgeführt werden, werden die Arbeitsabläufe abgebrochen.

1. Melden Sie sich bei Informatica Administrator an.
2. Wählen Sie den zu schließenden Knoten im Navigator aus.
3. Klicken Sie auf der Registerkarte "Domäne" im Menü **Aktionen** auf **Knoten schließen**.

Starten oder Beenden von Informatica über die Systemsteuerung

Das Verfahren zum Starten oder Beenden des Informatica Windows-Dienstes ist das gleiche wie für alle anderen Windows-Dienste.

1. Öffnen Sie die Windows-Systemsteuerung.
2. Wählen Sie **Verwaltung**.
3. Klicken Sie mit der rechten Maustaste auf **Dienste** und wählen Sie **Als Administrator ausführen** aus.
4. Klicken Sie mit der rechten Maustaste auf den Informatica-Dienst.

5. Wenn der Dienst ausgeführt wird, klicken Sie auf **Beenden**.
Wenn der Dienst angehalten ist, klicken Sie auf **Starten**.

Starten oder Anhalten von Informatica über das Startmenü

Klicken Sie zum Starten von Informatica über das Windows-Startmenü auf **Programme > Informatica[Version] > Server**. Klicken Sie mit der rechten Maustaste auf **Informatica-Dienste starten** und wählen Sie **Als Administrator ausführen** aus.

Klicken Sie zum Anhalten von Informatica über das Windows-Startmenü auf **Programme > Informatica[Version] > Server**. Klicken Sie mit der rechten Maustaste auf **Informatica-Dienste anhalten**, und wählen Sie **Als Administrator ausführen** aus.

Starten bzw. Anhalten von Informatica über eine Eingabeaufforderung

Sie können „infaservice.bat“ aus der Befehlszeile zum Starten und Anhalten von Informatica-Diensten unter Windows ausführen.

infaservice.bat ist standardmäßig im folgenden Verzeichnis installiert:

```
<Informatica-Installationsverzeichnis>\tomcat\bin
```

1. Öffnen Sie eine Eingabeaufforderung als Administrator.
2. Gehen Sie zu dem Verzeichnis, in dem sich infaservice.bat befindet.
3. Geben Sie den folgenden Befehl zum Starten der Informatica-Dienste ein:

```
infaservice.bat startup
```

Geben Sie den folgenden Befehl zum Anhalten der Informatica-Dienste ein:

```
infaservice.bat shutdown
```

Regeln und Richtlinien zum Starten oder Beenden von Informatica

Beachten Sie beim Starten und Beenden von Informatica auf einem Knoten die folgenden Richtlinien:

- Wenn ein Knoten ausgeschaltet wird, ist dieser für die Domäne nicht verfügbar. Wenn ein Gateway-Knoten ausgeschaltet wird und es keinen anderen Gateway-Knoten in der Domäne gibt, ist die Domäne nicht verfügbar.
- Überprüfen Sie beim Starten von Informatica, ob der vom Dienst auf dem Knoten verwendete Port verfügbar ist. Beispiel: Wenn Sie Informatica auf einem Knoten beenden, vergewissern Sie sich vor dem

Neustart, dass der Port von keinem anderen Prozess auf dem Rechner verwendet wird. Wenn der Port nicht verfügbar ist, schlägt der Start von Informatica fehl.

- Wenn Sie einen Knoten nicht mithilfe von Informatica Administrator ausschalten, werden auf dem Knoten ausgeführte Prozesse abgebrochen. Wenn Sie vor dem Ausschalten eines Knotens warten möchten, bis alle Prozesse abgeschlossen sind, verwenden Sie Informatica Administrator.
- Wenn es zwei Knoten in einer Domäne gibt, von denen einer als Primärknoten für einen Anwendungsdienst und der andere als Sicherungsknoten konfiguriert ist, starten Sie Informatica auf dem Primärknoten, bevor Sie den Sicherungsknoten starten. Andernfalls wird der Anwendungsdienst auf dem Sicherungsknoten, nicht auf dem Primärknoten ausgeführt.

ANHANG B

Verwalten von Verteilungspaketen

Dieser Anhang umfasst die folgenden Themen:

- [Verwaltung von Verteilungspaketen – Übersicht, 333](#)
- [Vorbereitungen, 333](#)
- [Installieren oder Entfernen von Verteilungspaketen im Konsolenmodus, 334](#)
- [Installieren oder Entfernen von Verteilungspaketen im automatischen Modus, 335](#)
- [Nach der Installation, 336](#)

Verwaltung von Verteilungspaketen – Übersicht

Verteilungspakete können Sie mit Integration Package Manager (dem Paketmanager) auf den Informatica-Dienst- und -Clientcomputern installieren und von diesen entfernen.

Ein Verteilungspaket ist ein Satz von Verteilungsbinarydateien, die Sie innerhalb der Domäne für die folgenden Verarbeitungsanforderungen installieren:

- Die Verarbeitung soll in die Hadoop- oder Databricks-Umgebung verlagert werden.
- Es sollen komplexe Dateien innerhalb der Informatica-Domäne verarbeitet werden.
- Es soll eine Verbindung zur Hadoop- oder Databricks-Umgebung hergestellt werden, wenn die Verarbeitung innerhalb der Informatica-Domäne stattfindet.

Sie können Verteilungspakete installieren, wenn dies während des Upgrade- oder Installationsvorgangs nicht erfolgt ist oder wenn Sie ein Verteilungspaket hinzufügen möchten. Sie können ein Verteilungspaket entfernen, wenn Sie ein anderes Paket verwenden möchten oder wenn Sie ein Paket installiert haben, das Sie nicht verwenden.

Stellen Sie beim Installieren oder Entfernen von Verteilungspaketen sicher, dass Sie den Vorgang auf allen Dienst- und Clientcomputern durchführen.

Vorbereitungen

Vor der Ausführung des Integration Package Managers führen Sie einige Aufgaben durch. So legen Sie beispielsweise Umgebungsvariablen fest und laden Dateien herunter.

1. Schließen Sie die Informatica-Dienste.

2. Legen Sie eine der folgenden Umgebungsvariablen fest:

Variable	Beschreibung
INFA_JDK_HOME	Speicherort des Ordners mit dem unterstützten Java Development Kit (JDK). Legen Sie die Umgebungsvariable INFA_JDK_HOME in den folgenden Szenarien fest: <ul style="list-style-type: none">- Die Informatica-Domäne befindet sich auf einer Windows- oder Linux-Plattform- Informatica-Client
INFA_JRE_HOME	Speicherort des Ordners, der die unterstützte Java-Laufzeitumgebung (JRE) enthält. Wenn sich die Informatica-Domäne auf der AIX-Plattform befindet, legen Sie die Umgebungsvariable INFA_JRE_HOME fest.

3. Stellen Sie sicher, dass der Benutzer, der den Paketmanager ausführt, über Lese- und Schreibberechtigungen für das Informatica-Installationsverzeichnis sowie über Ausführungsberechtigungen für die ausführbare Datei verfügt.
4. Laden Sie die folgenden Dateien von der Informatica Electronic Software-Download-Site herunter:
 - [Integration Package Manager](#)
 - [Distribution packages](#)
5. Extrahieren Sie die ZIP-Datei des Integration Package Managers auf ein lokales Laufwerk.
6. Kopieren Sie die ZIP-Dateien der Verteilungspakete, die Sie benötigen, an den folgenden Speicherort:
<Integration Package Manager-Verzeichnis>/source
Hinweis: Der Paketmanager schlägt fehl, wenn die ZIP-Dateien für Verteilungspakete nicht im Quellverzeichnis verfügbar sind.

Installieren oder Entfernen von Verteilungspaketen im Konsolenmodus

Sie können den Integration Package Manager im Konsolenmodus ausführen, um Verteilungspakete zu installieren oder zu entfernen.

1. Führen Sie im Verzeichnis des Package Manager einen der folgenden Befehle aus:
 - `./Server.sh console` für Linux oder UNIX
 - `Server.bat console` für Windows
 - `Client.bat console` für Client**Hinweis:** Verwenden Sie die Administrator-Eingabeaufforderung, um den Befehl unter Windows auszuführen.
2. Geben Sie das Installationsverzeichnis der Dienste oder des Clients ein und drücken Sie die **Eingabetaste**.
3. Wählen Sie den Vorgangstyp aus und drücken Sie die **Eingabetaste**.
 - Wählen Sie 1 aus, um die vorhandenen Verteilungspakete zu entfernen.
 - Wählen Sie 2 aus, um ein oder mehrere Verteilungspakete zu installieren.In der Konsole werden die Verteilungspakete aufgelistet, die Sie installieren oder entfernen können.

4. Geben Sie die Verteilungspakete ein, die installiert oder entfernt werden sollen. Trennen Sie mehrere Verteilungspakete jeweils durch ein Komma und drücken Sie die **Eingabetaste**.
5. Überprüfen Sie den Installations- oder Entfernungsstatus in der Protokolldatei des Integration Package Managers.

Sie finden die Protokolldatei im folgenden Speicherort: <Verzeichnis des Integration Package Managers>/ IntegrationPackageManager_<Datum und Zeitstempel>.log

Installieren oder Entfernen von Verteilungspaketen im automatischen Modus

Sie können den Integration Package Manager im automatischen Modus ausführen, um Verteilungspakete zu installieren oder zu entfernen. Die Eigenschaftendatei für die automatische Eingabe enthält die Eigenschaften für den Paketmanager, der für Dienste und Clients im automatischen Modus ausgeführt werden soll. Legen Sie den entsprechenden Wert für jede Eigenschaft in der Datei fest.

1. Suchen Sie die Datei „IntegrationPackageManager.properties“ im folgenden Speicherort: <Integration Package Manager-Verzeichnis>/
2. Bearbeiten Sie die Eigenschaftendatei in einem Texteditor.

In der folgenden Tabelle werden die Eigenschaften beschrieben, die Sie ändern können:

Eigenschaftsname	Beschreibung
USER_INSTALL_DIR	Das Installationsverzeichnis des Diensts oder Clients.
OPERATION_TYPE	Der Vorgang, der durchgeführt werden soll: <ul style="list-style-type: none"> - Legen Sie dies auf DELETE fest, um die vorhandenen Verteilungspakete zu entfernen. - Legen Sie dies auf EXTRACT fest, um ein oder mehrere Verteilungspakete zu installieren.
SELECTED_HADOOP_LIBRARIES	Listet die Verteilungspakete und -versionen auf. Geben Sie die Verteilungspakete ein, die installiert oder entfernt werden sollen. Trennen Sie mehrere Pakete durch ein Komma.

3. Speichern Sie die Eigenschaftendatei.
4. Führen Sie im Verzeichnis des Package Manager einen der folgenden Befehle aus:
 - `./Server.sh still` für Linux oder UNIX
 - `Server.bat silent` für Windows
 - `Client.bat silent` für Client

Hinweis: Verwenden Sie die Administrator-Eingabeaufforderung, um den Befehl unter Windows auszuführen.

5. Überprüfen Sie den Installations- oder Entfernungsstatus in der Protokolldatei des Integration Package Managers.

Sie finden die Protokolldatei im folgenden Speicherort:<Integration Package Manager-Verzeichnis>/ IntegrationPackageManager_<Datum und Zeitstempel>.log

Nach der Installation

Um die Verteilungspakete zu verwenden, die mit dem Paketmanager installiert werden, konfigurieren Sie die Eigenschaft oder Umgebungsvariable auf Dienst- und Clientcomputern.

Konfigurieren Sie das Developer Tool.

Nachdem Sie die Verteilungspakete im Developer Tool installiert haben, aktualisieren Sie die Datei „developerCore.ini“ mit dem installierten Verteilungspaket.

1. Suchen Sie die Datei „developerCore.ini“ an folgendem Speicherort: <Informatica-Installationsverzeichnis>\clients\DeveloperClient
2. Bearbeiten Sie die Datei, um folgende Eigenschaft zu aktualisieren:
-DINFA_HADOOP_DIST_DIR=hadoop\<Hadoop distribution name>_<version>
Beispiel:
-DINFA_HADOOP_DIST_DIR=hadoop\CDH_7.1
3. Starten Sie das Developer Tool neu.

Konfigurieren der Umgebungsvariablen

Einige Adapter erfordern Umgebungsvariablen für den Datenintegrationsdienst und den Metadaten-Zugriffsdienst, um auf die Verteilungspakete zuzugreifen. Weitere Informationen hierzu finden Sie unter [Configure environment variables to process complex files](#).

ANHANG C

Verbinden mit Datenbanken unter UNIX oder Linux

Dieser Anhang umfasst die folgenden Themen:

- [Verbinden mit Datenbanken unter UNIX oder Linux – Übersicht, 337](#)
- [Herstellen einer Verbindung zu einer IBM DB2 Universal-Datenbank, 338](#)
- [Verbinden zu einer Informix-Datenbank, 340](#)
- [Herstellen einer Verbindung zu einer Microsoft SQL Server-Datenbank, 341](#)
- [Herstellen einer Verbindung zu einer Netezza-Datenbank, 342](#)
- [Herstellen einer Verbindung zu einer Oracle-Datenbank, 344](#)
- [Herstellen einer Verbindung zu einer PostgreSQL-Datenbank, 347](#)
- [Verbinden zu einer Sybase ASE-Datenbank, 351](#)
- [Herstellen einer Verbindung zu einer Teradata-Datenbank, 353](#)
- [Verbinden zu einer JDBC-Datenquelle, 356](#)
- [Herstellen einer Verbindung zu einer ODBC-Datenquelle, 357](#)
- [odbc.ini-Beispieldatei, 359](#)

Verbinden mit Datenbanken unter UNIX oder Linux – Übersicht

Zur Verwendung der nativen Konnektivität müssen Sie die Datenbank-Client-Software für die Datenbank, auf die Sie zugreifen möchten, installieren und konfigurieren. Um die Kompatibilität zwischen dem Anwendungsdienst und der Datenbank zu gewährleisten, installieren Sie eine Client-Software, die mit der Datenbankversion kompatibel ist, und verwenden Sie die entsprechenden Bibliotheken des Datenbank-Client. Um die Leistung zu erhöhen, verwenden Sie native Konnektivität.

Die Informatica-Installation enthält DataDirect-ODBC-Treiber. Wenn ODBC-Datenquellen bereits mit früheren Versionen der Treiber erstellt wurden, müssen Sie mit den neuen Treibern neue ODBC-Datenquellen erstellen. Konfigurieren Sie die ODBC-Verbindungen mithilfe der von Informatica mitgelieferten DataDirect-ODBC-Treiber oder mit ODBC-Treibern von Drittanbietern, die mit Level 2 oder höher kompatibel sind.

Sie müssen eine Datenbankverbindung für die folgenden Dienste in der Informatica-Domäne konfigurieren:

- PowerCenter-Repository-Dienst

- Modellrepository-Dienst
- Datenintegrationsdienst
- Analyst-Dienst

Wenn Sie über Linux oder UNIX eine Verbindung zu Datenbanken herstellen, verwenden Sie native Treiber zum Herstellen einer Verbindung zu IBM DB2-, Oracle- oder Sybase ASE-Datenbanken. Mit ODBC können Sie eine Verbindung zu anderen Quellen und Zielen herstellen.

Herstellen einer Verbindung zu einer IBM DB2 Universal-Datenbank

Installieren Sie für native Konnektivität die Version von IBM DB2 Client Application Enabler (CAE), die für die Version des IBM DB2-Datenbankservers geeignet ist. Um die Kompatibilität zwischen Informatica und Datenbanken sicherzustellen, verwenden Sie die entsprechenden Datenbank-Client-Bibliotheken.

Konfigurieren von nativer Konnektivität

Sie können native Konnektivität für eine IBM DB2-Datenbank konfigurieren, um die Leistung zu erhöhen.

Die folgenden Schritte stellen eine Richtlinie zum Konfigurieren der nativen Konnektivität dar. Spezifische Anweisungen finden Sie in der Dokumentation zur Datenbank.

1. Um die Konnektivität auf dem Computer zu konfigurieren, auf dem der Datenintegrationsdienst-, PowerCenter-Integrationsdienst- oder PowerCenter-Repository-Dienst-Prozess ausgeführt wird, melden Sie sich am Computer als ein Benutzer an, der einen Dienstprozess starten kann.
2. Setzen Sie die Umgebungsvariablen DB2INSTANCE, INSTHOME, DB2DIR und PATH.

Die IBM DB2-Software für UNIX hat immer eine zugeordnete Benutzeranmeldung, meistens db2admin, die für Datenbankkonfigurationen benutzt wird. Der Benutzer besitzt die DB2-Instanz.

DB2INSTANCE. Der Name des Instanzbesitzers.

Bei Verwendung einer Bourne-Shell:

```
$ DB2INSTANCE=db2admin; export DB2INSTANCE
```

Bei Verwendung einer C-Shell:

```
$ setenv DB2INSTANCE db2admin
```

INSTHOME. Das ist ein db2admin-Basisverzeichnispfad.

Bei Verwendung einer Bourne-Shell:

```
$ INSTHOME=~db2admin
```

Bei Verwendung einer C-Shell:

```
$ setenv INSTHOME ~db2admin>
```

DB2DIR. Legen Sie die Variable so fest, dass sie auf das Installationsverzeichnis von IBM DB2 CAE verweist. Wenn beispielsweise der Client im Verzeichnis /opt/IBM/db2/V9.7 installiert ist:

Bei Verwendung einer Bourne-Shell:

```
$ DB2DIR=/opt/IBM/db2/V9.7; export DB2DIR
```

Bei Verwendung einer C-Shell:

```
$ setenv DB2DIR /opt/IBM/db2/V9.7
```

PATH. Legen Sie zum Ausführen der IBM DB2-Befehlszeilenprogramme die Variable so fest, dass sie das DB2-bin-Verzeichnis enthält.

Bei Verwendung einer Bourne-Shell:

```
$ PATH=${PATH}:$DB2DIR/bin; export PATH
```

Bei Verwendung einer C-Shell:

```
$ setenv PATH ${PATH}:$DB2DIR/bin
```

3. Legen Sie die Variable der gemeinsam genutzten Bibliothek so fest, dass sie das DB2-lib-Verzeichnis enthält.

Die IBM DB2-Clientsoftware enthält eine Reihe von gemeinsam genutzten Bibliothekskomponenten, die die Datenintegrationsdienst-, PowerCenter-Integrationsdienst- und PowerCenter-Repository-Dienst-Prozesse dynamisch laden. Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek so fest, dass die Dienste die gemeinsam genutzten Bibliotheken zur Laufzeit suchen können.

Der Pfad der gemeinsam genutzten Bibliothek muss außerdem das Informatica-Installationsverzeichnis (*server_dir*) enthalten.

Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek basierend auf dem Betriebssystem fest.

In der folgenden Tabelle werden die Variablen der gemeinsam genutzten Bibliothek für jedes Betriebssystem beschrieben:

Betriebssystem	Variable
Linux	LD_LIBRARY_PATH
AIX	LIBPATH

Verwenden Sie zum Beispiel die folgende Syntax für Linux:

- Bei Verwendung einer Bourne-Shell:

```
$ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:$HOME/server_dir:$DB2DIR/lib; export LD_LIBRARY_PATH
```

- Bei Verwendung einer C-Shell:

```
$ setenv LD_LIBRARY_PATH ${LD_LIBRARY_PATH}:$HOME/server_dir:$DB2DIR/lib
```

Für AIX:

- Bei Verwendung einer Bourne-Shell:

```
$ LIBPATH=${LIBPATH}:$HOME/server_dir:$DB2DIR/lib; export LIBPATH
```

- Bei Verwendung einer C-Shell:

```
$ setenv LIBPATH ${LIBPATH}:$HOME/server_dir:$DB2DIR/lib
```

4. Bearbeiten Sie die .cshrc- oder die .profile-Datei, um den gesamten Satz der Shell-Befehle einzubeziehen. Speichern Sie die Datei und melden Sie sich entweder erneut an oder führen Sie den Quellbefehl aus.

Bei Verwendung einer Bourne-Shell:

```
$ source .profile
```

Bei Verwendung einer C-Shell:

```
$ source .cshrc
```

5. Wenn sich die DB2-Datenbank auf demselben Computer befindet, auf dem der Datenintegrationsdienst-, PowerCenter-Integrationsdienst- oder PowerCenter-Repository-Dienst-Prozess läuft, konfigurieren Sie die DB2-Instanz als Remoteinstanz.

Führen Sie den folgenden Befehl aus, um zu überprüfen, ob es einen Remote-Eintrag für die Datenbank gibt:

```
DB2 LIST DATABASE DIRECTORY
```

Der Befehl listet neben allen Datenbanken, auf die der DB2-Client zugreifen kann, auch ihre Konfigurationseigenschaften auf. Wenn dieser Befehl „Remote“ als Eintrag für „Verzeichniseintragstyp“ auflistet, fahren Sie mit [7](#) fort.

6. Wenn die Datenbank nicht als „Remote“ konfiguriert ist, dann führen Sie den folgenden Befehl aus, um zu überprüfen, ob ein TCP/IP-Knoten für den Host katalogisiert ist:

```
DB2 LIST NODE DIRECTORY
```

Wenn der Knotenname leer ist, können Sie beim Einrichten einer Remotedatenbank einen Knoten erstellen. Verwenden Sie den folgenden Befehl, um eine Remotedatenbank einzurichten und um ggfs. einen Knoten zu erstellen:

```
db2 CATALOG TCPIP NODE <nodename> REMOTE <hostname_or_address> SERVER <port number>
```

Führen Sie den folgenden Befehl aus, um die Datenbank zu katalogisieren:

```
db2 CATALOG DATABASE <dbname> as <dbalias> at NODE <nodename>
```

Weitere Informationen zu diesen Befehlen finden Sie in der Datenbankdokumentation.

7. Prüfen Sie, ob Sie eine Verbindung zu der DB2-Datenbank herstellen können. Öffnen Sie den DB2-Befehlszeilenprozessor und führen Sie folgenden Befehl aus:

```
CONNECT TO <dbalias> USER <username> USING <password>
```

Wenn die Verbindung erfolgreich hergestellt wurde, führen Sie mit den Befehlen `CONNECT RESET` oder `TERMINATE` eine Bereinigung durch.

Verbinden zu einer Informix-Datenbank

Verwenden Sie ODBC zum Herstellen einer Verbindung zu einer Informix-Datenbank unter UNIX oder Linux.

Konfigurieren der ODBC-Konnektivität

Sie können ODBC-Konnektivität für eine Informix-Datenbank konfigurieren.

Die folgenden Schritte enthalten eine Richtlinie zum Konfigurieren der ODBC-Konnektivität. Spezifische Anweisungen finden Sie in der Dokumentation zur Datenbank.

1. Legen Sie die Umgebungsvariablen ODBCHOME gemäß dem ODBC-Installationsverzeichnis fest.

Beispiel:

Bei Verwendung einer Bourne-Shell:

```
$ ODBCHOME=<Informatica server home>/ODBC7.1; export ODBCHOME
```

Bei Verwendung einer C-Shell:

```
$ setenv ODBCHOME <Informatica server home>/ODBC7.1
```

2. Richten Sie die Umgebungsvariable ODBCINI auf den Speicherort der Datei odbc.ini ein. Die Datei odbc.ini befindet sich zum Beispiel im Verzeichnis \$ODBCHOME:

Bei Verwendung einer Bourne-Shell:

```
ODBCINI=$ODBCHOME/odbc.ini; export ODBCINI
```

Bei Verwendung einer C-Shell:

```
$ setenv ODBCINI $ODBCHOME/odbc.ini
```

3. Bearbeiten Sie die bestehende Datei `odbc.ini` im Verzeichnis `$ODBCHOME` oder kopieren Sie die Datei `odbc.ini` in das UNIX-Basisverzeichnis und bearbeiten Sie sie dort.

```
$ cp $ODBCHOME/odbc.ini $HOME/.odbc.ini
```

4. Fügen Sie einen Eintrag zu der Informix-Datenquelle unter dem Abschnitt [ODBC Data Sources] hinzu und konfigurieren Sie die Datenquelle. Beispiel:

```
[Informix Wire Protocol]
Driver=/export/home/Informatica/10.0.0/ODBC7.1/lib/DWifcl27.so
Description=DataDirect 7.1 Informix Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
CancelDetectInterval=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
HostName=<Informix_host>
LoadBalancing=0
LogonID=
Password=
PortNumber=<Informix_server_port>
ReportCodePageConversionErrors=0
ServerName=<Informix_server>
TrimBlankFromIndexName=1
```

5. Legen Sie die Umgebungsvariablen für `PATH` und für die geteilte Bibliothek durch Ausführen des Skripts `odbc.sh` oder `odbc.csh` im Verzeichnis `$ODBCHOME` fest.

Bei Verwendung einer Bourne-Shell:

```
sh odbc.sh
```

Bei Verwendung einer C-Shell:

```
source odbc.csh
```

6. Stellen Sie sicher, dass Sie mithilfe der ODBC-Datenquelle eine Verbindung zur Informix-Datenbank herstellen können. Falls die Verbindung fehlschlägt, lesen Sie die Dokumentation zur Datenbank.

Herstellen einer Verbindung zu einer Microsoft SQL Server-Datenbank

Über die Microsoft SQL Server-Verbindung können Sie an einem UNIX- oder Linux-Computer eine Verbindung zu einer Microsoft SQL Server-Datenbank herstellen.

Konfigurieren der SSL-Authentifizierung über ODBC

Sie können die SSL-Authentifizierung für Microsoft SQL Server über ODBC mit dem neuen SQL Server-Übertragungsprotokolltreiber von DataDirect konfigurieren.

1. Öffnen Sie die `odbc.ini`-Datei und fügen Sie einen Eintrag für die ODBC-Datenquelle und den neuen SQL Server-Übertragungsprotokolltreiber von DataDirect unter dem Abschnitt [ODBC Data Sources] hinzu.
2. Fügen Sie die Attribute in der `odbc.ini`-Datei zum Konfigurieren von SSL hinzu:

In der folgenden Tabelle werden die Attribute aufgelistet, die Sie bei der Konfiguration der SSL-Authentifizierung zur `odbc.ini`-Datei hinzufügen müssen:

Attribut	Beschreibung
EncryptionMethod	Die vom Treiber verwendete Methode zum Verschlüsseln der zwischen dem Treiber und dem Datenbankserver gesendeten Daten. Legen Sie den Wert auf 1 fest, um Daten mit SSL zu verschlüsseln.
ValidateServerCertificate	Bestimmt, ob der Treiber das vom Datenbankserver gesendete Zertifikat validiert, wenn Sie die sichere Kommunikation aktivieren. Legen Sie den Wert für den Treiber auf 1 fest, um das Serverzertifikat zu validieren.
TrustStore	Der Speicherort und der Name der Truststore-Datei. Die Truststore-Datei enthält eine Liste mit Zertifizierungsstellen, die der Treiber für sichere Authentifizierung verwendet.
TrustStorePassword	Das Passwort für den Zugriff auf den Inhalt der Truststore-Datei.
HostNameInCertificate	Optional. Der Hostname, den der Treiber verwendet, um den im Zertifikat für sichere Kommunikation enthaltenen Hostnamen zu überprüfen.

Konfigurieren von benutzerdefinierten Eigenschaften für Microsoft SQL Server

Zur Verbesserung der Bulk Load-Leistung können Sie benutzerdefinierte Eigenschaften für Microsoft SQL Server konfigurieren.

1. Starten Sie den PowerCenter-Client und stellen Sie eine Verbindung zum Workflow Manager her.
2. Öffnen Sie einen Arbeitsablauf und wählen Sie eine Sitzung aus, die Sie konfigurieren möchten.
3. Klicken Sie auf die Registerkarte **Konfig-Objekt**.
4. Ändern Sie den Wert der **Standard-Pufferblockgröße** in 5 MB. Sie können auch den folgenden Befehl verwenden: `$INFA_HOME/server/bin/.pmrep massupdate -t session_config_property -n "Default buffer block size" -v "5MB" -f $<folderName>`

Wenn Sie für eine Zeilengröße von 1 KB einen optimalen Durchsatz erzielen möchten, müssen Sie die Pufferblockgröße auf 5 MB festlegen.
5. Klicken Sie auf die Registerkarte **Eigenschaften**.
6. Ändern Sie das **Commit-Intervall** in 100000, falls die Sitzung ein relationales Ziel enthält.
7. Legen Sie die **DTM-Puffergröße** fest. Die optimale DTM-Puffergröße ist $((10 \times \text{Pufferblockgröße}) \times \text{Anzahl der Partitionen})$.

Herstellen einer Verbindung zu einer Netezza-Datenbank

Installieren Sie den Netezza ODBC-Treiber auf dem Rechner, auf dem die PowerCenter-Integrationsdienstprozesse ausgeführt werden. Verwenden Sie den DataDirect-Treiber-Manager im DataDirect-Treiberpaket (im Lieferumfang von Informatica enthalten) zum Konfigurieren der Netezza-Datenquellendetails in der Datei `odbc.ini`.

Konfigurieren der ODBC-Konnektivität

Sie können ODBC-Konnektivität für eine Netezza-Datenbank konfigurieren.

Die folgenden Schritte enthalten eine Richtlinie zum Konfigurieren der ODBC-Konnektivität. Spezifische Anweisungen finden Sie in der Dokumentation zur Datenbank.

1. Um die Konnektivität für den Integration-Service-Prozess zu konfigurieren, melden Sie sich am Computer als Benutzer an, der einen Dienstprozess starten kann.
2. Setzen Sie die Umgebungsvariablen ODBCHOME, NZ_ODBC_INI_PATH und PATH.

ODBCHOME. Legen Sie die Variable auf das ODBC-Installationsverzeichnis fest. Beispiel:

Bei Verwendung einer Bourne-Shell:

```
$ ODBCHOME=<Informatica server home>/ODBC7.1; export ODBCHOME
```

Bei Verwendung einer C-Shell:

```
$ setenv ODBCHOME =<Informatica server home>/ODBC7.1
```

PATH. Legen Sie die Variable auf das Verzeichnis ODBCHOME/bin fest. Beispiel:

Bei Verwendung einer Bourne-Shell:

```
PATH="${PATH}:${ODBCHOME}/bin"
```

Bei Verwendung einer C-Shell:

```
$ setenv PATH ${PATH}:${ODBCHOME}/bin
```

NZ_ODBC_INI_PATH. Legen Sie die Variable so fest, dass sie auf das Verzeichnis verweist, das die Datei odbc.ini enthält. Die Datei odbc.ini befindet sich zum Beispiel im Verzeichnis \$ODBCHOME:

Bei Verwendung einer Bourne-Shell:

```
NZ_ODBC_INI_PATH=$ODBCHOME; export NZ_ODBC_INI_PATH
```

Bei Verwendung einer C-Shell:

```
$ setenv NZ_ODBC_INI_PATH $ODBCHOME
```

3. Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek fest.

Der Pfad der gemeinsam genutzten Bibliothek muss die ODBC-Bibliotheken enthalten. Er muss außerdem das Installationsverzeichnis der Informatica-Dienste (`server_dir`) enthalten.

Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek basierend auf dem Betriebssystem fest. Setzen Sie den Ordner der Netezza-Bibliothek auf `<NetezzaInstallationDir>/lib64`.

In der folgenden Tabelle werden die Variablen der gemeinsam genutzten Bibliothek für jedes Betriebssystem beschrieben:

Betriebssystem	Variable
Linux	LD_LIBRARY_PATH
AIX	LIBPATH

Verwenden Sie zum Beispiel die folgende Syntax für Linux:

- Bei Verwendung einer Bourne-Shell:

```
$ LD_LIBRARY_PATH="${LD_LIBRARY_PATH}:${HOME}/server_dir:$ODBCHOME/  
lib:<NetezzaInstallationDir>/lib64"  
export LD_LIBRARY_PATH
```

- Bei Verwendung einer C-Shell:

```
$ setenv LD_LIBRARY_PATH "${LD_LIBRARY_PATH}:${HOME}/server_dir:$ODBCHOME/  
lib:<NetezzaInstallationDir>/lib64"
```

Für AIX

- Bei Verwendung einer Bourne-Shell:

```
$ LIBPATH=${LIBPATH}:${HOME}/server_dir:$ODBCHOME/lib:<NetezzaInstallationDir>/lib64; export LIBPATH
```

- Bei Verwendung einer C-Shell:

```
$ setenv LIBPATH ${LIBPATH}:${HOME}/server_dir:$ODBCHOME/lib:<NetezzaInstallationDir>/lib64
```

4. Bearbeiten Sie die vorhandene `odbc.ini`-Datei oder kopieren Sie die `odbc.ini`-Datei in das Basisverzeichnis und bearbeiten Sie sie.

Die Datei befindet sich im Verzeichnis `$ODBCHOME`.

```
$ cp $ODBCHOME/odbc.ini $HOME/.odbc.ini
```

Fügen Sie einen Eintrag zu der Netezza-Datenquelle unter dem Abschnitt [ODBC Data Sources] hinzu und konfigurieren Sie die Datenquelle.

Beispiel:

```
[NZSQL]
Driver = /export/home/appsga/thirdparty/netezza/lib64/libnzodbc.so
Description = NetezzaSQL ODBC
Servername = netezza1.informatica.com
Port = 5480
Database = infa
Username = admin
Password = password
Debuglogging = true
StripCRLF = false
PreFetch = 256
Protocol = 7.0
ReadOnly = false
ShowSystemTables = false
Socket = 16384
DateFormat = 1
TranslationDLL =
TranslationName =
TranslationOption =
NumericAsChar = false
```

Weitere Informationen zur Netezza-Konnektivität finden Sie in der Netezza-ODBC-Treiber-Dokumentation.

5. Prüfen Sie, ob der letzte Eintrag in der `odbc.ini`-Datei `InstallDir` ist und lassen Sie ihn auf das ODBC-Installationsverzeichnis verweisen.

Beispiel:

```
InstallDir=<Informatica install directory>/<ODBCHOME directory>
```

6. Bearbeiten Sie die `.cshrc`- oder die `.profile`-Datei, um den gesamten Satz der Shell-Befehle einzubeziehen.
7. Starten Sie die Informatica-Dienste neu.

Herstellen einer Verbindung zu einer Oracle-Datenbank

Installieren Sie für eine native Konnektivität die für die Oracle-Datenbankserverversion geeignete Version des Oracle-Client. Verwenden Sie zur Gewährleistung der Kompatibilität zwischen Informatica und den Datenbanken die entsprechenden Datenbank-Client-Bibliotheken.

Sie müssen kompatible Versionen des Oracle-Client und des Oracle-Datenbankservers installieren. Des Weiteren müssen Sie dieselbe Version des Oracle-Client auf allen Rechnern installieren, die ihn benötigen. Informationen zur Überprüfung der Kompatibilität erhalten Sie von Oracle.

Konfigurieren der nativen Konnektivität

Sie können native Konnektivität für eine Oracle-Datenbank konfigurieren, um die Leistung zu erhöhen.

Die folgenden Schritte enthalten eine Richtlinie zum Konfigurieren der nativen Konnektivität über Oracle Net Services oder Net8. Spezifische Anweisungen finden Sie in der Dokumentation zur Datenbank.

1. Um die Konnektivität für den Datenintegrationsdienst-, PowerCenter-Integrationsdienst- oder PowerCenter-Repository-Dienst-Prozess zu konfigurieren, melden Sie sich am Computer als Benutzer an, der den Serverprozess starten kann.
2. Legen Sie die Umgebungsvariablen ORACLE_HOME, NLS_LANG, TNS_ADMIN und PATH fest.

ORACLE_HOME. Legen Sie die Variable so fest, dass sie auf das Installationsverzeichnis des Oracle-Client verweist. Wenn der Client beispielsweise im Verzeichnis /HOME2/oracle installiert ist, legen Sie die Variable wie folgt fest:

Bei Verwendung einer Bourne-Shell:

```
$ ORACLE_HOME=/HOME2/oracle; export ORACLE_HOME
```

Bei Verwendung einer C-Shell:

```
$ setenv ORACLE_HOME /HOME2/oracle
```

NLS_LANG. Legen Sie die Variable auf das Gebietsschema fest (Sprache, Gebiet, Zeichensatz), das der Datenbank-Client und der Server beim Anmelden benutzen sollen. Der Wert dieser Variable hängt von der Konfiguration ab. Wenn es sich bei dem Wert beispielsweise um american_america.UTF8 handelt, legen Sie die Variable wie folgt fest:

Bei Verwendung einer Bourne-Shell:

```
$ NLS_LANG=american_america.UTF8; export NLS_LANG
```

Bei Verwendung einer C-Shell:

```
$ NLS_LANG american_america.UTF8
```

Kontaktieren Sie den Administrator, um den Wert dieser Variablen zu ermitteln.

ORA_SDTZ. Geben Sie zum Einrichten der Zeitzone einer Standardsitzung die Umgebungsvariable ORA_SDTZ an, wenn der Datenintegrationsdienst Daten vom Typ „Zeitstempel mit lokaler Zeitzone“ liest oder schreibt.

Sie können die Umgebungsvariable ORA_SDTZ auf einen der folgenden Werte festlegen:

- Lokale Zeitzone des Betriebssystems ('OS_TZ')
- Zeitzone der Datenbank ('DB_TZ')
- Absoluter Versatz von UTC (z. B. '-05:00')
- Name der Zeitzone (z. B. 'America/Los_Angeles')

Sie können die Umgebungsvariable auf dem Computer festlegen, auf dem der Informatica-Server ausgeführt wird.

TNS_ADMIN. Wenn sich die Datei tnsnames.ora nicht in demselben Speicherort wie das Oracle-Installationsverzeichnis befindet, legen Sie die TNS_ADMIN-Umgebungsvariable tnsnames.ora für das Verzeichnis fest, in dem sich die Datei tnsnames.ora befindet. Wenn sich die Datei beispielsweise im Verzeichnis /HOME2/oracle/files befindet, legen Sie die Variable wie folgt fest:

Bei Verwendung einer Bourne-Shell:

```
$ TNS_ADMIN=$HOME2/oracle/files; export TNS_ADMIN
```

Bei Verwendung einer C-Shell:

```
$ setenv TNS_ADMIN=$HOME2/oracle/files
```

Hinweis: Die Datei `tnsnames.ora` ist standardmäßig in folgendem Verzeichnis gespeichert:

`$ORACLE_HOME/network/admin`.

PATH. Zum Ausführen der Oracle-Befehlszeilenprogramme, legen Sie die Variable so fest, dass sie das Oracle-bin-Verzeichnis enthält.

Bei Verwendung einer Bourne-Shell:

```
$ PATH=${PATH}:$ORACLE_HOME/bin; export PATH
```

Bei Verwendung einer C-Shell:

```
$ setenv PATH ${PATH}:ORACLE_HOME/bin
```

3. Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek fest.

Die Oracle-Clientsoftware enthält eine Reihe von gemeinsam genutzten Bibliothekskomponenten, die die Datenintegrationsdienst-, PowerCenter-Integrationsdienst- und PowerCenter-Repository-Dienst-Prozesse dynamisch laden. Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek fest, um die gemeinsam genutzten Bibliotheken während der Laufzeit zu suchen.

Der Pfad der gemeinsam genutzten Bibliothek muss außerdem das Informatica-Installationsverzeichnis (`server_dir`) enthalten.

Legen Sie die Umgebungsvariable der gemeinsamen Bibliothek auf `LD_LIBRARY_PATH` fest.

Verwenden Sie zum Beispiel die folgende Syntax:

- Bei Verwendung einer Bourne-Shell:

```
$ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:$HOME/server_dir:$ORACLE_HOME/lib; export LD_LIBRARY_PATH
```

- Bei Verwendung einer C-Shell:

```
$ setenv LD_LIBRARY_PATH ${LD_LIBRARY_PATH}:$HOME/server_dir:$ORACLE_HOME/lib
```

4. Bearbeiten Sie die `.cshrc`- oder die `.profile`-Datei, um den gesamten Satz der Shell-Befehle einzubeziehen. Speichern Sie die Datei und melden Sie sich entweder erneut an oder führen Sie den Quellbefehl aus.

Bei Verwendung einer Bourne-Shell:

```
$ source .profile
```

Bei Verwendung einer C-Shell:

```
$ source .cshrc
```

5. Vergewissern Sie sich, dass der Oracle-Client so konfiguriert ist, dass er auf die Datenbank zugreifen kann.

Verwenden Sie das Dienstprogramm SQL*Net Easy Configuration oder kopieren Sie eine bestehende `tnsnames.ora`-Datei in das Basisverzeichnis und verändern Sie diese.

Die Datei `tnsnames.ora` ist in folgendem Verzeichnis gespeichert: `$ORACLE_HOME/network/admin`.

Geben Sie die richtige Syntax für die Oracle-Verbindungszeichenfolge ein. Diese lautet normalerweise `databasesname.world`.

Hier ist eine `tnsnames.ora`-Beispieldatei. Geben Sie die Informationen für die Datenbank ein.

```
mydatabase.world =
  (DESCRIPTION
    (ADDRESS_LIST =
      (ADDRESS =
        (COMMUNITY = mycompany.world
          (PROTOCOL = TCP)
          (Host = mymachine)
          (Port = 1521)
        )
      )
    )
  )
```

```

)
(CONNECT_DATA =
  (SID = MYORA7)
  (GLOBAL_NAMES = mydatabase.world)

```

Bei Folgendem handelt es sich um eine Beispieldatei namens `tnsnames.ora` zum Herstellen einer Verbindung zu Oracle mithilfe des Oracle-Verbindungsmanagers:

```

ORCL19C_CMAN =
(description=
(address_list=
(source_route=yes)
(address=(protocol=tcp) (host=lnrh74ocm.mycompany.com) (port=1521))
(address=(protocol=tcp) (host=lnrh74oradb.mycompany.com) (port=1521))
)
(connect_data=
(service_name=ORCL19C.mycompany.com)
)
)

```

6. Vergewissern Sie sich, dass Sie eine Verbindung zu der Oracle-Datenbank herstellen können.

Um eine Verbindung zu der Oracle-Datenbank herzustellen, starten Sie SQL*Plus und geben Sie dann die Konnektivitätsinformationen ein. Wenn Sie keine Verbindung zu der Datenbank herstellen können, vergewissern Sie sich, dass Sie alle Konnektivitätsinformationen korrekt eingegeben haben.

Geben Sie den in der `tnsnames.ora`-Datei definierten Benutzernamen und die Verbindungszeichenfolge ein.

Herstellen einer Verbindung zu einer PostgreSQL-Datenbank

Installieren Sie für native Konnektivität die für die PostgreSQL-Datenbankserverversion geeignete Version des PostgreSQL-Client.

Verwenden Sie zur Gewährleistung der Kompatibilität zwischen Informatica und den Datenbanken die entsprechenden Datenbank-Client-Bibliotheken.

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

Konfigurieren von nativer Konnektivität

Sie können native Konnektivität für eine PostgreSQL-Datenbank konfigurieren, um die Leistung zu erhöhen.

Die folgenden Schritte stellen eine Richtlinie zum Konfigurieren der nativen Konnektivität über PostgreSQL dar. Spezifische Anweisungen finden Sie in der Dokumentation zur Datenbank.

1. Um die Konnektivität für den PowerCenter-Integrationsdienst- oder den PowerCenter-Repository-Dienstprozess zu konfigurieren, melden Sie sich bei dem Computer als Benutzer an, der den Serverprozess starten kann.

2. Um eine PostgreSQL-Datenbank für das PowerCenter-Repository zu konfigurieren, legen Sie Werte für den PostgreSQL-Datenbankhost, -Port und -Dienstnamen für die Datei "pg_service.conf" im folgenden Format fest:

```
[PCRS_DB_SERVICE_NAME]
host=Database host IP
port=Database port
dbname=PowerCenter repository database service name
```

Stellen Sie sicher, dass die Einträge für [PCRS_DB_SERVICE_NAME] mit der Konfiguration für den PowerCenter-Repository-Dienst übereinstimmen. In der Datei "pg_service.conf" können Sie eine sichere Verbindung zu PostgreSQL für das PowerCenter-Repository herstellen. Um die sichere Verbindung einzurichten, legen Sie die Sicherheitseigenschaft und die erforderlichen Datenbankeigenschaften in der Datei "pg_service.conf" im folgenden Format fest: `sslmode=require`

3. Legen Sie die Umgebungsvariablen PGSERVICEFILE, PGHOME und PATH fest.

PGSERVICEFILE. Legen Sie die Variable auf die pg_service.conf-Datei fest, die die Verbindungsparameter für die PostgreSQL-Datenbankverbindung enthält. Legen Sie die Variable beispielsweise wie folgt fest:

Bei Verwendung einer Bourne-Shell:

```
$ export PGSERVICEFILE; PGSERVICEFILE=<pg_service.conf file
directory>/pg_service.conf
```

Bei Verwendung einer C-Shell:

```
$ setenv PGSERVICEFILE <pg_service.conf file
directory>/pg_service.conf
```

PGHOME. Legen Sie die Variable auf den PostgreSQL-Installationspfad fest, unter dem Sie den PostgreSQL-Client installiert haben. Legen Sie die Variable beispielsweise wie folgt fest:

Bei Verwendung einer Bourne-Shell:

```
$ export PGHOME; PGHOME=/usr/pgsql-10
```

Bei Verwendung einer C-Shell:

```
$ setenv PGHOME /usr/pgsql-10
```

PATH. Zum Ausführen der PostgreSQL-Befehlszeilenprogramme müssen Sie die Variable so festlegen, dass sie das PostgreSQL-Clientverzeichnis (psql) enthält. Legen Sie die Variable beispielsweise wie folgt fest:

Bei Verwendung einer Bourne-Shell:

```
$ export PATH; PATH=${PATH}:${PGHOME}
```

Bei Verwendung einer C-Shell:

```
$ setenv PATH ${PGHOME}:${PATH}
```

4. Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek fest.

Die PostgreSQL-Clientsoftware enthält eine Reihe von gemeinsam genutzten Bibliothekskomponenten, die die Prozesse vom PowerCenter-Integrationsdienst und vom PowerCenter-Repository-Dienst dynamisch laden. Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek fest, damit die gemeinsam genutzten Bibliotheken zur Laufzeit auffindbar sind.

Der Pfad der gemeinsam genutzten Bibliothek muss außerdem das Informatica-Installationsverzeichnis (`server_dir`) enthalten.

Legen Sie die Umgebungsvariable der gemeinsamen Bibliothek auf LD_LIBRARY_PATH fest.

Verwenden Sie zum Beispiel die folgende Syntax:

- Bei Verwendung einer Bourne-Shell:

```
$ export LD_LIBRARY_PATH; LD_LIBRARY_PATH $PGHOME/lib
$ LD_LIBRARY_PATH <InstallationDirectory>/server/bin:${LD_LIBRARY_PATH}
```

- Bei Verwendung einer C-Shell:

```
$ setenv LD_LIBRARY_PATH $PGHOME/lib
$ setenv LD_LIBRARY_PATH <InstallationDirectory>/server/bin:${LD_LIBRARY_PATH}
```

5. Prüfen Sie, ob Sie eine Verbindung zur PostgreSQL-Datenbank herstellen können.

Um eine Verbindung zur PostgreSQL-Datenbank herzustellen, starten Sie das Dienstprogramm psql und geben Sie die Konnektivitätsinformationen ein.

Konfigurieren der ODBC-Konnektivität

Sie können die ODBC-Verbindung zu einer PostgreSQL-Datenbank unter UNIX oder Linux konfigurieren.

Sie können die Verbindung zu PostgreSQL über ODBC mit dem DataDirect PostgreSQL Wire Protocol-Treiber konfigurieren.

Überprüfen Sie die folgenden Aufgaben, um einen Leitfaden für die Konfiguration der ODBC-Verbindung zu PostgreSQL zu erhalten:

1. Festlegen der Umgebungsvariable für PostgreSQL
2. Konfigurieren der ODBC-Verbindung in der Datei „ODBC.ini“
3. Aktualisieren des PowerCenter-Repositorys mit dem Namen der PostgreSQL-Datenquelle
4. Überprüfen der PostgreSQL-Verbindung mit der ODBC-Datenquelle

Spezifische Anweisungen finden Sie in der Dokumentation zur Datenbank.

Schritt 1. Festlegen der Umgebungsvariablen

1. Klicken Sie im Administrator Tool auf **Verwalten > Dienste und Knoten**.
2. Wählen Sie im Domänennavigator den PowerCenter-Repository-Dienst aus.
3. Klicken Sie in der Inhaltsübersicht auf die Ansicht Prozesse Legen Sie im Abschnitt "Umgebungsvariablen" den Variablennamen auf `POSTGRES_ODBC` und den Wert auf 1 fest.

Hinweis: Wenn Sie die erweiterte Eigenschaft `Hochverfügbarkeits-Persistenz` in der Datenbank speichern für den PowerCenter-Integrationsdienst festlegen, stellen Sie sicher, dass Sie die Umgebungsvariable `POSTGRES_ODBC` auf 1 setzen.

Schritt 2. Konfigurieren der ODBC-Konnektivität

1. Legen Sie die Umgebungsvariablen ODBCHOME gemäß dem ODBC-Installationsverzeichnis fest.
Beispiel:

Bei Verwendung einer Bourne-Shell:

```
$ ODBCHOME=<Informatica server home>/ODBC7.1; export ODBCHOME
```

Bei Verwendung einer C-Shell:

```
$ setenv ODBCHOME <Informatica server home>/ODBC7.1
```

2. Bearbeiten Sie die bestehende Datei vom Typ "odbc.ini" im Verzeichnis \$ODBCHOME oder kopieren Sie diese Datei in das UNIX-Basisverzeichnis und bearbeiten Sie sie dort.

```
$ cp $ODBCHOME/odbc.ini $HOME/.odbc.ini
```

3. Öffnen Sie die Datei "odbc.ini" und fügen Sie einen Eintrag für DataDirect PostgreSQL Wire Protocol-Datenquellen hinzu.

Konfigurieren Sie den Namen der Datenquelle, den Treiberpfad, den Hostnamen und die Portnummer, um eine Verbindung zur PostgreSQL-Datenbank herzustellen. Beispiel:

```
[PostgreSQL Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWpsql27.so
Description=DataDirect 7.1 PostgreSQL Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
DefaultLongDataBuffLen=2048
EnableDescribeParam=1
EncryptionMethod=1
ExtendedColumnMetadata=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
FetchTSWTZasTimestamp=0
FetchTWFSasTime=0
GSSClient=native
HostName=<PostgreSQL_host>
HostNameInCertificate=<Host name in SSL certificate>
InitializationString=
KeyPassword=
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
Password=
Pooling=0
PortNumber=<PostgreSQL_server_port>
QueryTimeout=0
ReportCodepageConversionErrors=0
TransactionErrorBehavior=1
TrustStore=<Path of the truststore certificates>
TrustStorePassword=<Password of the truststore certificates>
ValidateServerCertificate=1
XMLDescribeType=-10
```

4. Legen Sie die Umgebungsvariable PATH fest.

Bei Verwendung einer Bourne-Shell:

```
$ PATH=${PATH}:$ODBCHOME/bin; export PATH
```

Bei Verwendung einer C-Shell:

```
$ setenv PATH ${PATH}:$ODBCHOME/bin
```

5. Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek basierend auf dem Betriebssystem fest.

In der folgenden Tabelle werden die Variablen der gemeinsam genutzten Bibliothek für jedes Betriebssystem beschrieben:

Verwenden Sie beispielsweise die folgende Syntax, um den LD_LIBRARY_PATH für Linux festzulegen:

- Bei Verwendung einer Bourne-Shell:

```
$ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:$HOME/server_dir:$ODBCHOME/lib; export
LD_LIBRARY_PATH
```

- Bei Verwendung einer C-Shell:

```
$ setenv LD_LIBRARY_PATH $HOME/server_dir:$ODBCHOME/lib:${LD_LIBRARY_PATH}
```

Verwenden Sie beispielsweise die folgende Syntax, um den LIBPATH für AIX festzulegen:

- Bei Verwendung einer Bourne-Shell:

```
$ LIBPATH=${LIBPATH}:$HOME/server_dir :$ODBCHOME/lib; export LIBPATH
```
- Bei Verwendung einer C-Shell:

```
$ setenv LIBPATH ${LIBPATH}:$HOME/server_dir :$ODBCHOME/lib
```

Schritt 3. Aktualisieren der Eigenschaften der PowerCenter-Repository-Datenbank

1. Wählen Sie den PowerCenter-Repository-Dienst im Administrator Tool aus.
2. Geben Sie im Abschnitt „Datenbankeigenschaften“ denselben Datenquellennamen ein, den Sie für PostgreSQL in der Datei „ODBC.ini“ angegeben haben.
3. Speichern Sie Ihre Änderungen.

Schritt 4. Überprüfen der PostgreSQL-Verbindung

1. Stellen Sie sicher, dass Sie mithilfe der ODBC-Datenquelle eine Verbindung zur PostgreSQL-Datenbank herstellen können.
2. Falls die Verbindung fehlschlägt, lesen Sie die Dokumentation zur Datenbank.

Verbinden zu einer Sybase ASE-Datenbank

Installieren Sie für eine native Konnektivität die für Ihre Datenbankversion geeignete Version von Open Client. Verwenden Sie zur Gewährleistung der Kompatibilität zwischen Informatica und den Datenbanken die entsprechenden Datenbank-Client-Bibliotheken.

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

Wenn Sie ein Sybase ASE-Repository erstellen, wiederherstellen oder upgraden möchten, setzen Sie *Nullen standardmäßig zulassen* auf der Datenbankebene auf TRUE. Hiermit wird der Standard-Nulltyp der Spalte entsprechend dem SQL-Standard in Null geändert.

Konfigurieren von nativer Konnektivität

Sie können native Konnektivität für eine Sybase ASE-Datenbank konfigurieren, um die Leistung zu erhöhen.

Die folgenden Schritte stellen eine Richtlinie zum Konfigurieren der nativen Konnektivität dar. Spezifische Anweisungen finden Sie in der Dokumentation zur Datenbank.

1. Um die Konnektivität für den Datenintegrationsdienst-, PowerCenter-Integrationsdienst- oder PowerCenter-Repository-Dienst-Prozess zu konfigurieren, melden Sie sich am Computer als Benutzer an, der den Serverprozess starten kann.
2. Setzen Sie die Umgebungsvariablen SYBASE und PATH.

Sybase Legen Sie die Variable so fest, dass sie auf das Installationsverzeichnis von Sybase Open Client verweist. Wenn zum Beispiel der Client im Verzeichnis /usr/sybase installiert ist:

Bei Verwendung einer Bourne-Shell:

```
$ SYBASE=/usr/sybase; export SYBASE
```

Bei Verwendung einer C-Shell:

```
$ setenv SYBASE /usr/sybase
```

PATH. Zum Ausführen der Sybase-Befehlszeilenprogramme legen Sie die Variable so fest, dass sie das Sybase OCS-bin-Verzeichnis enthält.

Bei Verwendung einer Bourne-Shell:

```
$ PATH=${PATH}:/usr/sybase/OCS-15_0/bin; export PATH
```

Bei Verwendung einer C-Shell:

```
$ setenv PATH ${PATH}:/usr/sybase/OCS-15_0/bin
```

3. Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek fest.

Die Sybase Open Client-Software enthält eine Reihe von gemeinsam genutzten Bibliothekskomponenten, die die Datenintegrationsdienst-, PowerCenter-Integrationsdienst- und PowerCenter-Repository-Dienst-Prozesse dynamisch laden. Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek so fest, dass die Dienste die gemeinsam genutzten Bibliotheken zur Laufzeit finden.

Der Pfad der gemeinsam genutzten Bibliothek muss außerdem das Installationsverzeichnis der Informatica-Dienste (*server_dir*) enthalten.

Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek basierend auf dem Betriebssystem fest.

In der folgenden Tabelle werden die Variablen der gemeinsam genutzten Bibliothek für jedes Betriebssystem beschrieben.

Betriebssystem	Variable
Linux	LD_LIBRARY_PATH
AIX	LIBPATH

Verwenden Sie zum Beispiel die folgende Syntax für Linux:

- Bei Verwendung einer Bourne-Shell:

```
$ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:${HOME}/server_dir:$SYBASE/OCS-15_0/lib;$SYBASE/OCS-15_0/lib3p;$SYBASE/OCS-15_0/lib3p64; export LD_LIBRARY_PATH
```

- Bei Verwendung einer C-Shell:

```
$ setenv LD_LIBRARY_PATH ${LD_LIBRARY_PATH}:${HOME}/server_dir:$SYBASE/OCS-15_0/lib;$SYBASE/OCS-15_0/lib3p;$SYBASE/OCS-15_0/lib3p64;
```

Für AIX

- Bei Verwendung einer Bourne-Shell:

```
$ LIBPATH=${LIBPATH}:${HOME}/server_dir:$SYBASE/OCS-15_0/lib;$SYBASE/OCS-15_0/lib3p;$SYBASE/OCS-15_0/lib3p64; export LIBPATH
```

- Bei Verwendung einer C-Shell:

```
$ setenv LIBPATH ${LIBPATH}:${HOME}/server_dir:$SYBASE/OCS-15_0/lib;$SYBASE/OCS-15_0/lib3p;$SYBASE/OCS-15_0/lib3p64;
```

4. Bearbeiten Sie die *.cshrc*- oder die *.profile*-Datei, um den gesamten Satz der Shell-Befehle einzubeziehen. Speichern Sie die Datei und melden Sie sich entweder erneut an oder führen Sie den Quellbefehl aus.

Bei Verwendung einer Bourne-Shell:

```
$ source .profile
```


Bei Verwendung einer C-Shell:

```
$ source .cshrc
```

5. Überprüfen Sie den Sybase-ASE-Servernamen in der im Verzeichnis \$SYBASE gespeicherten Sybase-Schnittstellendatei.
6. Führen Sie optional die folgenden Aufgaben aus, um eine Verbindung zur SSL-fähigen Sybase ASE-Datenbank herzustellen:
 - Geben Sie die folgenden Sicherheitsattribute auf der Registerkarte **Sicherheit** an, wenn Sie den Datenquellennamen in der Sybase-Treibereigenschaft konfigurieren:

Attribut	Beschreibung
Verschlüsselungsmethode	Gibt an, ob Daten bei der Netzwerkübertragung verschlüsselt werden. Wählen Sie „SSL“ aus.
Serverzertifikat validieren	Gibt an, ob Informatica das vom Datenbankserver gesendete Zertifikat validiert, wenn die SSL-Verschlüsselung aktiviert wird.
Truststore	Der Speicherort und der Name der Truststore-Datei.
Truststore-Passwort	Das Passwort für den Zugriff auf den Inhalt der Truststore-Datei.
Hostname im Zertifikat	Der Hostname, der vom SSL-Administrator eingerichtet wird, um den im Zertifikat enthaltenen Hostnamen zu validieren.

- Fügen Sie der Datei „trusted.txt“ im Sybase ASE-Client das Sybase ASE-Serverzertifikat hinzu.
- Fügen Sie der Sybase-Schnittstellendatei die folgenden Sybase ASE-Serververbindungsdetails hinzu:

```
<server_instance_name>  
  master tcp ether <host name> <port number> ssl="CN='common_name'"  
  query tcp ether <host name> <port number> ssl="CN='common_name'"
```

7. Prüfen Sie, ob Sie eine Verbindung zu der Sybase-ASE-Datenbank herstellen können.

Um eine Verbindung zu der Sybase-ASE-Datenbank herzustellen, starten Sie ISQL und geben Sie dann die Konnektivitätsinformationen ein. Wenn Sie keine Verbindung zu der Datenbank herstellen können, vergewissern Sie sich, dass Sie alle Konnektivitäts-Informationen korrekt eingegeben haben.

Bei Benutzernamen und Datenbanknamen bitte die Groß-/Kleinschreibung beachten.

Herstellen einer Verbindung zu einer Teradata-Datenbank

Installieren und konfigurieren Sie native Clientsoftware auf den Computern, auf denen der Datenintegrationsdienst- oder PowerCenter-Integrationsdienst-Prozess ausgeführt wird. Um die Kompatibilität zwischen Informatica und Datenbanken sicherzustellen, verwenden Sie die entsprechenden Datenbank-Client-Bibliotheken.

Installieren Sie den Teradata-Client, den Teradata-ODBC-Treiber sowie weitere eventuell benötigte Teradata-Client-Software auf dem Computer, auf dem der Datenintegrationsdienst oder der PowerCenter-Integrationsdienst ausgeführt wird. Außerdem müssen Sie die ODBC-Konnektivität konfigurieren.

Hinweis: Entsprechend einer Empfehlung von Teradata verwendet Informatica ODBC für die Verbindung mit Teradata. ODBC ist eine native Schnittstelle für Teradata.

Konfigurieren der ODBC-Konnektivität

Sie können ODBC-Konnektivität für eine Teradata-Datenbank konfigurieren.

Die folgenden Schritte bieten eine Orientierungshilfe zur Konfiguration der ODBC-Konnektivität. Spezifische Anweisungen finden Sie in der Dokumentation zur Datenbank.

1. Um die Konnektivität für den Integration-Service-Prozess zu konfigurieren, melden Sie sich am Computer als Benutzer an, der einen Dienstprozess starten kann.
2. Legen Sie die Umgebungsvariablen `TERADATA_HOME`, `ODBCHOME` und `PATH` fest.

TERADATA_HOME. Legen Sie die Variable so fest, dass sie auf das Installationsverzeichnis des Teradata-Treibers verweist. Die Standardeinstellungen lauten wie folgt:

Bei Verwendung einer Bourne-Shell:

```
$ TERADATA_HOME=/opt/teradata/client/<version>; export TERADATA_HOME
```

Bei Verwendung einer C-Shell:

```
$ setenv TERADATA_HOME /opt/teradata/client/<version>
```

ODBCHOME. Legen Sie die Variable so fest, dass sie auf das ODBC-Installationsverzeichnis verweist. Beispiel:

Bei Verwendung einer Bourne-Shell:

```
$ ODBCHOME=$INFA_HOME/ODBC<version>; export ODBCHOME
```

Bei Verwendung einer C-Shell:

```
$ setenv ODBCHOME $INFA_HOME/ODBC<version>
```

PATH. Um das Hilfsprogramm `ddtestlib` auszuführen, damit überprüft wird, ob der DataDirect ODBC-Treibermanager die Treiberdateien laden kann, legen Sie die Variable folgendermaßen fest:

Bei Verwendung einer Bourne-Shell:

```
PATH="{PATH}:%ODBCHOME/bin:%TERADATA_HOME/bin"
```

Bei Verwendung einer C-Shell:

```
$ setenv PATH {PATH}:%ODBCHOME/bin:%TERADATA_HOME/bin
```

3. Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek fest.

Die Teradata-Client-Software enthält mehrere gemeinsam genutzte Bibliothekskomponenten, die der Integration-Service-Prozess dynamisch lädt. Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek so fest, dass die Dienste die gemeinsam genutzten Bibliotheken zur Laufzeit finden.

Der Pfad der gemeinsam genutzten Bibliothek muss außerdem das Installationsverzeichnis des Informatica-Diensts (*server_dir*) enthalten.

Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek abhängig vom Betriebssystem fest.

In der folgenden Tabelle werden die Variablen der gemeinsam genutzten Bibliothek für jedes Betriebssystem beschrieben:

Betriebssystem	Variable
Linux	LD_LIBRARY_PATH
AIX	LIBPATH

Verwenden Sie zum Beispiel die folgende Syntax für Linux:

- Bei Verwendung einer Bourne-Shell:


```
$ LD_LIBRARY_PATH="${LD_LIBRARY_PATH}:${HOME}/server_dir:$ODBCHOME/lib:
$TERADATA_HOME/lib64:$TERADATA_HOME/odbc_64/lib";
export LD_LIBRARY_PATH
```
- Bei Verwendung einer C-Shell:


```
$ setenv LD_LIBRARY_PATH "${LD_LIBRARY_PATH}:${HOME}/server_dir:$ODBCHOME/
lib:$TERADATA_HOME/lib64:
$TERADATA_HOME/odbc_64/lib"
```

Für AIX

- Bei Verwendung einer Bourne-Shell:


```
$ LIBPATH=${LIBPATH}:${HOME}/server_dir:$ODBCHOME/lib:$TERADATA_HOME/
lib64:$TERADATA_HOME/odbc_64/lib; export LIBPATH
```
- Bei Verwendung einer C-Shell:


```
$ setenv LIBPATH ${LIBPATH}:${HOME}/server_dir:$ODBCHOME/lib:$TERADATA_HOME/lib64:
$TERADATA_HOME/odbc_64/lib
```

- Bearbeiten Sie die vorhandene Datei `odbc.ini` oder kopieren Sie die Datei `odbc.ini` in das Basisverzeichnis und bearbeiten Sie sie.

Die Datei befindet sich im Verzeichnis `$ODBCHOME`.

```
$ cp $ODBCHOME/odbc.ini $HOME/.odbc.ini
```

Fügen Sie unter dem Abschnitt `[ODBC Data Sources]` einen Eintrag für die Teradata-Datenquelle hinzu und konfigurieren Sie die Datenquelle.

Beispiel für Teradata Parallel Transporter-Dienstprogramme:

```
TERADATA_DSN=DataDirect 7.1 Teradata
[TERADATA_DSN]
Driver=/opt/teradata/client/<version>/lib64/tdataodbc_sb64.so
Description=NCR 3600 running Teradata V1R5.2
DBCName=<hostname>
LastUser=
Username=
Password=
Database=
DefaultDatabase=
UseNativeLOBSupport=Yes
CharacterSet=UTF8
SessionMode=ANSI
```

- Setzen Sie das `DateTimeFormat` in der Teradata-Daten-ODBC-Konfiguration auf `AAA`.
- Optional können Sie den `SessionMode` auf `ANSI` setzen. Wenn Sie den ANSI-Sitzungsmodus verwenden, führt Teradata bei einem Zeilenfehler kein Rollback der Transaktion aus.

Wenn Sie den Teradata-Sitzungsmodus verwenden, führt Teradata bei einem Zeilenfehler ein Rollback der Transaktion aus. Im Teradata-Modus kann der Integration-Service-Prozess das Rollback nicht erkennen und meldet dies nicht im Sitzungs-Log.

7. Um eine Verbindung zu einer einzelnen Teradata-Datenbank zu konfigurieren, geben Sie den Namen der Standarddatenbank ein. Um eine einzelne Verbindung zur Standarddatenbank herzustellen, geben Sie den Benutzernamen und das Passwort ein. Lassen Sie das Feld für die Standarddatenbank leer, um eine Verbindung zu mehreren Datenbanken mit dem gleichen ODBC-DSN herzustellen.

Weitere Informationen zur Teradata-Konnektivität finden Sie in der Dokumentation zum Teradata-ODBC-Treiber.

8. Prüfen Sie, ob der letzte Eintrag in der `odbc.ini` „InstallDir“ lautet und lassen Sie ihn auf das `odbc`-Installationsverzeichnis verweisen.

Beispiel:

```
InstallDir=<Informatica installation directory>/ODBC<version>
```

9. Bearbeiten Sie die `.cshrc`- oder die `.profile`-Datei, um den gesamten Satz der Shell-Befehle einzubeziehen.
10. Speichern Sie die Datei und melden Sie sich entweder ab und wieder an oder führen Sie den Quellbefehl aus.

Bei Verwendung einer Bourne-Shell:

```
$ source .profile
```

Bei Verwendung einer C-Shell:

```
$ source .cshrc
```

11. Zeichnen Sie für jede Datenquelle, die Sie verwenden, den Dateinamen unter „Driver=<parameter>“ im Datenquelleneintrag in `odbc.ini` auf. Verwenden Sie das Hilfsprogramm `ddtestlib`, um sicherzustellen, dass der DataDirect ODBC-Treibermanager die Treiberdatei laden kann.

Wenn Sie zum Beispiel folgenden Treibereintrag haben:

```
Driver=/u01/app/teradata/td-tuf611/odbc/drivers/tdata.so
```

führen Sie den folgenden Befehl aus:

```
ddtestlib /u01/app/teradata/td-tuf611/odbc/drivers/tdata.so
```

12. Testen Sie die Verbindung mit BTEQ oder einem anderen Teradata-Client-Tool.

Verbinden zu einer JDBC-Datenquelle

Um dem Datenintegrationsdienst zu ermöglichen, in relationale Ziele zu schreiben, laden Sie die `.jar`-Datei des JDBC-Treibers auf den Host des Datenintegrationsdiensts und auf alle Client-Computer herunter, die Mappings ausführen, die über relationale Ziele verfügen.

Sie erhalten die `.jar`-Datei des Treibers vom Datenbankanbieter. Um beispielsweise auf eine Oracle-Datenbank zuzugreifen, laden Sie die Datei `ojdbc.jar` von der Oracle-Website herunter.

1. Legen Sie die `.jar`-Datei des JDBC-Treibers in folgendem Verzeichnis auf dem Datenintegrationsdienst-Computer ab: `<Informatica-Installationsverzeichnis>/externaljdbcjars`. Starten Sie den Datenintegrationsdienst neu.
2. Legen Sie die `.jar`-Datei des JDBC-Treibers in folgendem Verzeichnis auf Computern fest, auf denen sich das Developer Tool befindet: `<Informatica installation directory>/clients/externaljdbcjars`. Starten Sie dann das Developer Tool neu.

Herstellen einer Verbindung zu einer ODBC-Datenquelle

Installieren und konfigurieren Sie native Clientsoftware auf dem Computer, auf dem der Datenintegrationsdienst, PowerCenter-Integrationsdienst und PowerCenter-Repository-Dienst ausgeführt werden. Installieren und konfigurieren Sie außerdem die zugrunde liegende Clientzugriff-Software, die der ODBC-Treiber benötigt. Um die Kompatibilität zwischen Informatica und den Datenbanken sicherzustellen, verwenden Sie die entsprechenden Datenbank-Client-Bibliotheken.

Die Informatica-Installation enthält DataDirect-ODBC-Treiber. Wenn die `odbc.ini`-Datei Verbindungen enthält, die frühere Versionen des ODBC-Treibers verwenden, aktualisieren Sie die Verbindungsinformationen, um die neuen Treiber zu verwenden. Verwenden Sie System-DSN, um eine ODBC-Datenquelle unter Windows anzugeben.

1. Melden Sie sich am Computer, auf dem der Anwendungsdienst ausgeführt wird, als Benutzer an, der einen Dienstprozess starten kann.
2. Legen Sie die Umgebungsvariablen `ODBCHOME` und `PATH` fest.

ODBCHOME. Legen Sie die Variablen für das DataDirect ODBC-Installationsverzeichnis fest. Wenn das Verzeichnis beispielsweise folgendermaßen lautet: `/export/home/Informatica/10.0.0/ODBC7.1`.

Bei Verwendung einer Bourne-Shell:

```
$ ODBCHOME=/export/home/Informatica/10.0.0/ODBC7.1; export ODBCHOME
```

Bei Verwendung einer C-Shell:

```
$ setenv ODBCHOME /export/home/Informatica/10.0.0/ODBC7.1
```

PATH. Zum Ausführen der ODBC-Befehlszeilenprogramme, z. B. *ddtestlib*, legen Sie die Variable so fest, dass sie das ODBC-bin-Verzeichnis enthält.

Bei Verwendung einer Bourne-Shell:

```
$ PATH=${PATH}:${ODBCHOME}/bin; export PATH
```

Bei Verwendung einer C-Shell:

```
$ setenv PATH ${PATH}:${ODBCHOME}/bin
```

Führen Sie das Hilfsprogramm *ddtestlib* aus, um sicherzustellen, dass der DataDirect ODBC-Treibermanager die Treiberdateien laden kann.

3. Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek fest.

Die ODBC-Clientsoftware enthält eine Reihe von gemeinsam genutzten Bibliothekskomponenten, die die Dienstprozesse dynamisch laden. Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek so fest, dass die Dienste die gemeinsam genutzten Bibliotheken zur Laufzeit suchen können.

Der Pfad der gemeinsam genutzten Bibliothek muss außerdem das Informatica-Installationsverzeichnis (*server_dir*) enthalten.

Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek basierend auf dem Betriebssystem fest.

In der folgenden Tabelle werden die Variablen der gemeinsam genutzten Bibliothek für jedes Betriebssystem beschrieben:

Betriebssystem	Variable
Linux	LD_LIBRARY_PATH
AIX	LIBPATH

Benutzen Sie zum Beispiel die folgende Syntax für Linux:

- Bei Verwendung einer Bourne-Shell:


```
$ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:$HOME/server_dir:$ODBCHOME/lib; export LD_LIBRARY_PATH
```
- Bei Verwendung einer C-Shell:


```
$ setenv LD_LIBRARY_PATH $HOME/server_dir:$ODBCHOME:${LD_LIBRARY_PATH}
```

Für AIX

- Bei Verwendung einer Bourne-Shell:


```
$ LIBPATH=${LIBPATH}:$HOME/server_dir:$ODBCHOME/lib; export LIBPATH
```
 - Bei Verwendung einer C-Shell:


```
$ setenv LIBPATH ${LIBPATH}:$HOME/server_dir:$ODBCHOME/lib
```
4. Bearbeiten Sie die vorhandene `odbc.ini`-Datei oder kopieren Sie die `odbc.ini`-Datei in das Basisverzeichnis und bearbeiten Sie sie.

Die Datei befindet sich im Verzeichnis `$ODBCHOME`.

```
$ cp $ODBCHOME/odbc.ini $HOME/.odbc.ini
```

Fügen Sie einen Eintrag zu der ODBC-Datenquelle unter dem Abschnitt [ODBC Data Sources] hinzu und konfigurieren Sie die Datenquelle.

Beispiel:

```
MY_MSSQLSERVER_ODBC_SOURCE=<Driver name or data source description>
[MY_MSSQLSERVER_ODBC_SOURCE]
Driver=<path to ODBC drivers>
Description=DataDirect 8.0 SQL Server Wire Protocol
Database=<SQLServer_database_name>
LogonID=<username>
Password=<password>
Address=<TCP/IP address>,<port number>
QuoteId=No
AnsiNPW=No
ApplicationsUsingThreads=1
```

Diese Datei existiert möglicherweise bereits, wenn Sie eine oder mehrere ODBC-Datenquellen konfiguriert haben.

5. Prüfen Sie, ob der letzte Eintrag in der `odbc.ini`-Datei `InstallDir` ist und lassen Sie ihn auf das ODBC-Installationsverzeichnis verweisen.

Beispiel:

```
InstallDir=/export/home/Informatica/10.0.0/ODBC7.1
```

6. Wenn Sie die `odbc.ini`-Datei im Basisverzeichnis verwenden, setzen Sie die Umgebungsvariable `ODBCINI`.

Bei Verwendung einer Bourne-Shell:

```
$ ODBCINI=/HOME/.odbc.ini; export ODBCINI
```

Bei Verwendung einer C-Shell:

```
$ setenv ODBCINI $HOME/.odbc.ini
```

7. Bearbeiten Sie die `.cshrc`- oder die `.profile`-Datei, um den gesamten Satz der Shell-Befehle einzubeziehen. Speichern Sie die Datei und melden Sie sich entweder erneut an oder führen Sie den Quellbefehl aus.

Bei Verwendung einer Bourne-Shell:

```
$ source .profile
```

Bei Verwendung einer C-Shell:

```
$ source .cshrc
```

8. Verwenden Sie das Hilfsprogramm `ddtestlib`, um zu überprüfen, ob der DataDirect ODBC-Treibermanager die Treiberdatei laden kann, die Sie für die Datenquelle in der Datei „`odbc.ini`“ festgelegt haben.

Sie haben zum Beispiel den Treibereintrag:

```
Driver = /export/home/Informatica/10.0.0/ODBC7.1/lib/DWxxxxnn.so
```

Führen Sie den folgenden Befehl aus:

```
ddtestlib /export/home/Informatica/10.0.0/ODBC7.1/lib/DWxxxxnn.so
```

9. Installieren und konfigurieren Sie jede zugrunde liegende Clientzugriffs-Software, die der ODBC-Treiber benötigt.

Hinweis: Einige ODBC-Treiber sind eigenständig und haben alle Informationen in der `odbc.ini`-Datei; bei den meisten ist dies jedoch nicht der Fall. Wenn Sie beispielsweise einen ODBC-Treiber verwenden möchten, um auf Sybase IQ zuzugreifen, müssen Sie Sybase IQ Netzwerk-Clientsoftware installieren und die entsprechenden Umgebungsvariablen setzen.

Legen Sie zur Verwendung der Informatica ODBC-Treiber (`DWxxxxnn.so`) die Umgebungsvariablen für `PATH` und gemeinsam genutzte Bibliothekspfade manuell fest. Führen Sie alternativ das Skript „`odbc.sh`“ oder das Skript „`odbc.csh`“ im Ordner `$ODBCHOME` aus. Dieses Skript richtet die erforderlichen Umgebungsvariablen für `PATH` und gemeinsam genutzte Bibliothekspfade für die ODBC-Treiber ein, die von Informatica bereitgestellt werden.

odbc.ini-Beispieldatei

Das folgende Beispiel zeigt die Einträge für die ODBC-Treiber in der Datei `ODBC.ini`:

```
[ODBC Data Sources]
SQL Server Legacy Wire Protocol=DataDirect 7.1 SQL Server Legacy Wire Protocol
DB2 Wire Protocol=DataDirect 7.1 DB2 Wire Protocol
Informix Wire Protocol=DataDirect 7.1 Informix Wire Protocol
Oracle Wire Protocol=DataDirect 8.0 Oracle Wire Protocol
Sybase Wire Protocol=DataDirect 7.1 Sybase Wire Protocol
SQL Server Wire Protocol=DataDirect 8.0 SQL Server Wire Protocol
MySQL Wire Protocol=DataDirect 7.1 MySQL Wire Protocol
PostgreSQL Wire Protocol=DataDirect 7.1 PostgreSQL Wire Protocol
Greenplum Wire Protocol=DataDirect 7.1 Greenplum Wire Protocol

[ODBC]
IANAAppCodePage=4
InstallDir=<Informatica installation directory>/ODBC7.1
Trace=0
TraceFile=odbttrace.out
TraceDll=<Informatica installation directory>/ODBC7.1/lib/DWtrc27.so

[DB2 Wire Protocol]
Driver=<Informatica installation directory>/ODBC7.1/lib/DWdb227.so
Description=DataDirect 7.1 DB2 Wire Protocol
AccountingInfo=
AddStringToCreateTable=
AlternateID=
AlternateServers=
ApplicationName=
```

```

ApplicationUsingThreads=1
AuthenticationMethod=0
BulkBinaryThreshold=32
BulkCharacterThreshold=-1
BulkLoadBatchSize=1024
BulkLoadFieldDelimiter=
BulkLoadRecordDelimiter=
CatalogSchema=
CharsetFor65535=0
ClientHostName=
ClientUser=
#Collection applies to z/OS and iSeries only
Collection=
ConcurrentAccessResolution=0
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
CurrentFuncPath=
#Database applies to DB2 UDB only
Database=<database_name>
DefaultIsolationLevel=1
DynamicSections=1000
EnableBulkLoad=0
EncryptionMethod=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
GrantAuthid=PUBLIC
GrantExecute=1
GSSClient=native
HostNameInCertificate=
IpAddress=<DB2_server_host>
KeyPassword=
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
#Location applies to z/OS and iSeries only
Location=<location_name>
LogonID=
MaxPoolSize=100
MinPoolSize=0
Password=
PackageCollection=NULLID
PackageNamePrefix=DD
PackageOwner=
Pooling=0
ProgramID=
QueryTimeout=0
ReportCodePageConversionErrors=0
TcpPort=50000
TrustStore=
TrustStorePassword=
UseCurrentSchema=0
ValidateServerCertificate=1
WithHold=1
XMLDescribeType=-10

[Informix Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWifcl27.so
Description=DataDirect 7.1 Informix Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
CancelDetectInterval=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
HostName=<Informix_host>
LoadBalancing=0
LogonID=
Password=

```



```

PortNumber=<Informix_server_port>
ServerName=<Informix_server>
TrimBlankFromIndexName=1
UseDelimitedIdentifiers=0

[Oracle Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWora28.so
Description=DataDirect 8.0 Oracle Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
AccountingInfo=
Action=
ApplicationName=
ArraySize=60000
AuthenticationMethod=1
BulkBinaryThreshold=32
BulkCharacterThreshold=-1
BulkLoadBatchSize=1024
BulkLoadFieldDelimiter=
BulkLoadRecordDelimiter=
CachedCursorLimit=32
CachedDescLimit=0
CatalogIncludesSynonyms=1
CatalogOptions=0
ClientHostName=
ClientID=
ClientUser=
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
DataIntegrityLevel=0
DataIntegrityTypes=MD5,SHA1
DefaultLongDataBuffLen=1024
DescribeAtPrepare=0
EditionName=
EnableBulkLoad=0
EnableDescribeParam=0
EnableNcharSupport=0
EnableScrollableCursors=1
EnableStaticCursorsForLongData=0
EnableTimestampWithTimeZone=0
EncryptionLevel=0
EncryptionMethod=0
EncryptionTypes=AES128,AES192,AES256,DES,3DES112,3DES168,RC4_40,RC4_56,RC4_128,
RC4_256
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
FetchTSWTZasTimestamp=0
GSSClient=native
HostName=<Oracle_server>
HostNameInCertificate=
InitializationString=
KeyPassword=
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
LocalTimeZoneOffset=
LockTimeOut=-1
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
Module=
Password=
Pooling=0
PortNumber=<Oracle_server_port>
ProcedureRetResults=0
ProgramID=
QueryTimeout=0

```

```

ReportCodePageConversionErrors=0
ReportRecycleBin=0
ServerName=<server_name in tnsnames.ora>
ServerType=0
ServiceName=
SID=<Oracle_System_Identifier>
TimestampEscapeMapping=0
TNSNamesFile=<tnsnames.ora_filename>
TrustStore=
TrustStorePassword=
UseCurrentSchema=1
ValidateServerCertificate=1
WireProtocolMode=2

[Sybase Wire Protocol]
Driver=<Informatica installation directory>/ODBC7.1/lib/DWase27.so
Description=DataDirect 7.1 Sybase Wire Protocol
AlternateServers=
ApplicationName=
ApplicationUsingThreads=1
ArraySize=50
AuthenticationMethod=0
BulkBinaryThreshold=32
BulkCharacterThreshold=-1
BulkLoadBatchSize=1024
BulkLoadFieldDelimiter=
BulkLoadRecordDelimiter=
Charset=
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
CursorCacheSize=1
Database=<database_name>
DefaultLongDataBuffLen=1024
EnableBulkLoad=0
EnableDescribeParam=0
EnableQuotedIdentifiers=0
EncryptionMethod=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
GSSClient=native
HostNameInCertificate=
InitializationString=
Language=
LoadBalancing=0
LoadBalanceTimeout=0
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
NetworkAddress=<Sybase_host,Sybase_server_port>
OptimizePrepare=1
PacketSize=0
Password=
Pooling=0
QueryTimeout=0
RaiseErrorPositionBehavior=0
ReportCodePageConversionErrors=0
SelectMethod=0
ServicePrincipalName=
TruncateTimeTypeFractions=0
TrustStore=
TrustStorePassword=
ValidateServerCertificate=1
WorkStationID=

[SQL Server Wire Protocol]
Driver=<Informatica installation directory>/ODBC7.1/lib/DWsqls28.so
Description=DataDirect 8.0 SQL Server Wire Protocol
AlternateServers=

```

```

AlwaysReportTriggerResults=0
AnsiNFW=1
ApplicationName=
ApplicationUsingThreads=1
AuthenticationMethod=1
BulkBinaryThreshold=32
BulkCharacterThreshold=-1
BulkLoadBatchSize=1024
BulkLoadOptions=2
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
EnableBulkLoad=0
EnableQuotedIdentifiers=0
EncryptionMethod=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
FetchTSWTZasTimestamp=0
FetchTWFSasTime=1
GSSClient=native
HostName=<SQL_Server_host>
HostNameInCertificate=
InitializationString=
Language=
LoadBalanceTimeout=0
LoadBalancing=0
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
PacketSize=-1
Password=
Pooling=0
PortNumber=<SQL_Server_server_port>
QueryTimeout=0
ReportCodePageConversionErrors=0
SnapshotSerializable=0
TrustStore=
TrustStorePassword=
ValidateServerCertificate=1
WorkStationID=
XML Describe Type=-10

[MySQL Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWMysql27.so
Description=DataDirect 7.1 MySQL Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
DefaultLongDataBuffLen=1024
EnableDescribeParam=0
EncryptionMethod=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
HostName=<MySQL_host>
HostNameInCertificate=
InteractiveClient=0
LicenseNotice=You must purchase commercially licensed MySQL database software or
a MySQL Enterprise subscription in order to use the DataDirect Connect for ODBC
for MySQL Enterprise driver with MySQL software.
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
LogonID=

```

```

LoginTimeout=15
MaxPoolSize=100
MinPoolSize=0
Password=
Pooling=0
PortNumber=<MySQL_server_port>
QueryTimeout=0
ReportCodepageConversionErrors=0
TreatBinaryAsChar=0
TrustStore=
TrustStorePassword=
ValidateServerCertificate=1

[PostgreSQL Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWpsql27.so
Description=DataDirect 7.1 PostgreSQL Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
DefaultLongDataBuffLen=2048
EnableDescribeParam=1
EncryptionMethod=1
ExtendedColumnMetadata=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
FetchTSWTZasTimestamp=0
FetchTWFSasTime=0
GSSClient=native
HostName=<PostgreSQL_host>
HostNameInCertificate=<Host name in SSL certificate>
InitializationString=
KeyPassword=
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
Password=
Pooling=0
PortNumber=<PostgreSQL_server_port>
QueryTimeout=0
ReportCodepageConversionErrors=0
TransactionErrorBehavior=1
TrustStore=<Path of the truststore certificates>
TrustStorePassword=<Password of the truststore certificates>
ValidateServerCertificate=1
XMLDescribeType=-10

[Greenplum Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWgplm27.so
Description=DataDirect 7.1 Greenplum Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
DefaultLongDataBuffLen=2048
EnableDescribeParam=0
EnableKeysetCursors=0
EncryptionMethod=0
ExtendedColumnMetadata=0
FailoverGranularity=0
FailoverMode=0

```

```
FailoverPreconnect=0
FetchTSTZasTimestamp=0
FetchTWFSasTime=0
HostName=<Greenplum_host>
InitializationString=
KeyPassword=
KeysetCursorOptions=0
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
Password=
Pooling=0
PortNumber=<Greenplum_server_port>
QueryTimeout=0
ReportCodepageConversionErrors=0
TransactionErrorBehavior=1
XMLDescribeType=-10
```

Hinweis: Unter Umständen müssen Sie die DSN-Einträge in der Datei `ODBC.ini` basierend auf dem verwendeten Drittanbietertreiber anpassen. Weitere Informationen zu den DSN-Einträgen finden Sie in der entsprechenden Treiberdokumentation des Drittanbieters.

Verbinden zu Datenbanken unter Windows

Dieser Anhang umfasst die folgenden Themen:

- [Verbinden zu Datenbanken unter Windows - Übersicht, 366](#)
- [Verbinden zu einer IBM DB2 Universal-Datenbank unter Windows, 367](#)
- [Herstellen einer Verbindung zu einer Informix-Datenbank unter Windows, 368](#)
- [Verbinden mit Microsoft Access und Microsoft Excel unter Windows, 368](#)
- [Verbinden zu einer Microsoft SQL Server-Datenbank Unter Windows, 369](#)
- [Verbinden zu einer Netezza-Datenbank unter Windows, 371](#)
- [Herstellen einer Verbindung zu einer Oracle-Datenbank unter Windows, 371](#)
- [Herstellen einer Verbindung zu einer PostgreSQL-Datenbank, 373](#)
- [Verbinden zu einer Sybase ASE-Datenbank unter Windows, 375](#)
- [Herstellen einer Verbindung zu einer Teradata-Datenbank über Windows, 376](#)

Verbinden zu Datenbanken unter Windows - Übersicht

Konfigurieren Sie die Konnektivität, um die Kommunikation zwischen Clients, Diensten und anderen Komponenten in der Domäne zu aktivieren.

Zur Verwendung der nativen Konnektivität müssen Sie die Datenbank-Client-Software für die Datenbank, auf die Sie zugreifen möchten, installieren und konfigurieren. Um die Kompatibilität zwischen dem Anwendungsdienst und der Datenbank zu gewährleisten, installieren Sie eine Client-Software, die mit der Datenbankversion kompatibel ist, und verwenden Sie die entsprechenden Bibliotheken des Datenbank-Client. Um die Leistung zu erhöhen, verwenden Sie native Konnektivität.

Die Informatica-Installation enthält DataDirect-ODBC-Treiber. Wenn ODBC-Datenquellen bereits mit früheren Versionen der Treiber erstellt wurden, müssen Sie mit den neuen Treibern neue ODBC-Datenquellen erstellen. Konfigurieren Sie die ODBC-Verbindungen mithilfe der von Informatica mitgelieferten DataDirect-ODBC-Treiber oder mit ODBC-Treibern von Drittanbietern, die mit Level 2 oder höher kompatibel sind.

Die Informatica-Installation umfasst DataDirect JDBC-Treiber. Sie können diese Treiber ohne zusätzliche Schritte verwenden. Sie können auch JDBC-Treiber des Typs 4 von Drittanbietern herunterladen, um eine

Verbindung zu Quellen und Zielen herzustellen. Sie können jeden beliebigen JDBC-Treiber mit JDBC 3.0 oder höher verwenden.

Sie müssen eine Datenbankverbindung für die folgenden Dienste in der Informatica-Domäne konfigurieren:

- PowerCenter-Repository-Dienst
- Modellrepository-Dienst
- Datenintegrationsdienst
- Analyst-Dienst

Verbinden zu einer IBM DB2 Universal-Datenbank unter Windows

Installieren Sie für eine native Konnektivität die Version von IBM DB2 Client Application Enabler (CAE), die für die IBM DB2-Datenbankserverversion geeignet ist. Verwenden Sie zur Gewährleistung der Kompatibilität zwischen Informatica und den Datenbanken die entsprechenden Datenbank-Client-Bibliotheken.

Konfigurieren der nativen Konnektivität

Sie können native Konnektivität für eine IBM DB2-Datenbank konfigurieren, um die Leistung zu erhöhen.

Die folgenden Schritte stellen eine Richtlinie zum Konfigurieren der nativen Konnektivität dar. Spezifische Anweisungen finden Sie in der Dokumentation zur Datenbank.

1. Überprüfen Sie, ob von IBM DB2 Client Application Enabler (CAE) die folgenden Einstellungen zu Umgebungsvariablen vorgenommen wurden:

```
DB2HOME=C:\IBM\SQLLIB
DB2INSTANCE=DB2
DB2CODEPAGE=1208 (Sometimes required. Use only if you encounter problems. Depends on
the locale, you may use other values.)
```

2. Überprüfen Sie, ob die Umgebungsvariable PATH das IBM DB2-bin-Verzeichnis enthält. Beispiel:

```
PATH=C:\WINNT\SYSTEM32;C:\SQLLIB\BIN;...
```

3. Konfigurieren Sie den IBM DB2-Client so, dass eine Verbindung zur gewünschten Datenbank hergestellt wird. Konfigurieren des IBM DB2-Clients:

- a. Starten Sie den IBM DB2-Konfigurationsassistenten.
- b. Fügen Sie die Datenbankverbindung hinzu.
- c. Erstellen Sie eine Bindung an die Verbindung.

4. Führen Sie den folgenden Befehl im IBM DB2-Befehlszeilenprozessor aus, um sicherzustellen, dass eine Verbindung zur IBM DB2-Datenbank hergestellt werden kann:

```
CONNECT TO <dbalias> USER <username> USING <password>
```

5. Wenn die Verbindung erfolgreich ist, führen Sie den Befehl TERMINATE aus, um die Verbindung zur Datenbank zu trennen. Falls die Verbindung fehlschlägt, ziehen Sie die Dokumentation zur Datenbank hinzu.

Herstellen einer Verbindung zu einer Informix-Datenbank unter Windows

Verwenden Sie ODBC zum Herstellen einer Verbindung zu einer Informix-Datenbank unter Windows. Erstellen Sie mithilfe des mit Informatica installierten DataDirect-ODBC-Treibers eine ODBC-Datenquelle. Verwenden Sie zur Gewährleistung der Kompatibilität zwischen Informatica und den Datenbanken die entsprechenden Datenbank-Client-Bibliotheken.

Hinweis: Bei Verwendung des von Informatica mitgelieferten DataDirect-ODBC-Treibers wird der Datenbank-Client nicht benötigt. Die ODBC-Drahtprotokolle benötigen die Datenbank-Client-Software nicht, um eine Verbindung zur Datenbank herzustellen.

Konfigurieren der ODBC-Konnektivität

Sie können ODBC-Konnektivität für eine Informix-Datenbank konfigurieren.

Die folgenden Schritte enthalten eine Richtlinie zum Konfigurieren der ODBC-Konnektivität. Spezifische Anweisungen finden Sie in der Dokumentation zur Datenbank.

1. Erstellen Sie eine ODBC-Datenquelle mithilfe des Treibers DataDirect ODBC Wire Protocol Treiber für Informix von Informatica.
2. Stellen Sie sicher, dass Sie mithilfe der ODBC-Datenquelle eine Verbindung zur Informix-Datenbank herstellen können.

Verbinden mit Microsoft Access und Microsoft Excel unter Windows

Konfigurieren Sie die Konnektivität zu den folgenden Informatica-Komponenten unter Windows.

Installieren Sie Microsoft Access oder Excel auf dem Computer, auf dem die Datenintegrationsdienst- und PowerCenter-Integrationsdienst-Prozesse ausgeführt werden. Erstellen Sie eine ODBC-Datenquelle für die Microsoft Access- oder Excel-Daten, auf die Sie zugreifen möchten.

Konfigurieren der ODBC-Konnektivität

Sie können ODBC-Konnektivität zu einer Microsoft Access- oder Excel-Datenbank konfigurieren.

Die folgenden Schritte enthalten eine Richtlinie zum Konfigurieren der ODBC-Konnektivität. Spezifische Anweisungen finden Sie in der Dokumentation zur Datenbank.

1. Erstellen Sie mithilfe des von Microsoft bereitgestellten Treibers eine ODBC-Datenquelle.
2. Damit keine leeren Zeichenfolgen oder Nullen verwendet werden, verwenden Sie bei der Herstellung einer Datenbankverbindung im Workflow Manager die reservierten Wörter PmNullUser für den Benutzernamen und PmNullPasswd für das Passwort.

Verbinden zu einer Microsoft SQL Server-Datenbank Unter Windows

Sie können mithilfe des Providertyps ODBC oder OLEDB eine Verbindung zu einer Microsoft SQL Server-Datenbank herstellen.

Konfigurieren der nativen Konnektivität

Sie können mithilfe des Providertyps ODBC (Standard) oder OLEDB native Konnektivität zur Microsoft SQL Server-Datenbank konfigurieren.

Wenn Sie den Providertyp ODBC auswählen, können Sie die Option „DSN verwenden“ aktivieren, um den im Microsoft ODBC-Administrator konfigurierten DSN als Verbindungszeichenfolge zu verwenden. Falls Sie die Option „DSN verwenden“ nicht aktivieren, müssen Sie den Servernamen und den Datenbanknamen in den Verbindungseigenschaften angeben.

Wenn Sie den Providertyp OLEDB auswählen, müssen Sie Microsoft SQL Server 2012 Native Client installieren, um native Konnektivität zur Microsoft SQL Server-Datenbank zu konfigurieren. Wenn Sie keine Verbindung zur Datenbank herstellen können, stellen Sie sicher, dass alle Konnektivitätsinformationen korrekt eingegeben wurden.

Sie können Microsoft SQL Server 2012 Native Client von folgender Microsoft-Website herunterladen:
<http://www.microsoft.com/en-in/download/details.aspx?id=29065>.

Nach dem Upgrade wird die Microsoft SQL Server-Verbindung standardmäßig auf den Providertyp OLEDB festgelegt. Es wird empfohlen, zur Verwendung des Providertyps ODBC alle Microsoft SQL Server-Verbindungen zu aktualisieren. Mithilfe der folgenden Befehle können Sie alle Ihre Microsoft SQL Server-Verbindungen auf den Providertyp ODBC aktualisieren:

- Wenn Sie PowerCenter verwenden, führen Sie den folgenden Befehl aus: `pmrep upgradeSqlServerConnection`
- Wenn Sie die Informatica-Plattform verwenden, führen Sie den folgenden Befehl aus: `infacmd.sh isp upgradeSQLSConnection`

Spezifische Anweisungen zur Konnektivität finden Sie in der Dokumentation zur Datenbank.

Regeln und Richtlinien für Microsoft SQL Server

Beachten Sie beim Konfigurieren von ODBC-Konnektivität zu einer Microsoft SQL Server-Datenbank unter Windows die folgenden Regeln und Richtlinien:

- Falls Sie eine Microsoft SQL Server-Verbindung ohne Verwendung eines Datenquellennamens (Verbindung ohne DSN) nutzen möchten, müssen Sie die Umgebungsvariable „odbcinst.ini“ konfigurieren.
- Bei Verwendung einer DSN-Verbindung müssen Sie dem ODBC-DSN den Eintrag „EnableQuotedIdentifiers=1“ hinzufügen. Wenn Sie den Eintrag nicht hinzufügen, schlägt die Ausführung der Datenvorschau und des Mappings fehl.
- Wenn Sie eine DSN-Verbindung verwenden, können Sie spezifische DataDirect-Eigenschaften konfigurieren. Weitere Informationen zum Konfigurieren und Verwenden der spezifischen DataDirect-Eigenschaften finden Sie in der DataDirect-Dokumentation.
- Sie können die NTLM-Authentifizierung von Microsoft SQL Server für eine Microsoft SQL Server-Verbindung ohne DSN auf der Microsoft Windows-Plattform verwenden.

- Wenn die Microsoft SQL Server-Tabelle einen UUID-Datentyp enthält und Sie Daten aus einer SQL-Tabelle lesen sowie Daten in eine Einfachdatei schreiben, ist das Datenformat zwischen den OLEDB- und ODBC-Verbindungstypen möglicherweise nicht konsistent.
- Wählen Sie aus, ob Sie sichere Kommunikation für eine Microsoft SQL Server-Verbindung ohne DSN in PowerCenter verwenden möchten, indem Sie die SSL-Optionen in den Verbindungseigenschaften konfigurieren.
Um sichere Kommunikation über eine DSN-fähige Microsoft SQL Server-Verbindung in PowerCenter zu aktivieren, konfigurieren Sie die SSL-Optionen in der `odbc.ini`-Datei.
- Falls Microsoft SQL Server die Kerberos-Authentifizierung verwendet, müssen Sie die Eigenschaft „GSSClient“ festlegen, um auf die Kerberos-Bibliotheken von Informatica zu verweisen. Verwenden Sie den folgenden Pfad und Dateinamen: `<Informatica-Installationsverzeichnis>/server/bin/libgssapi_krb5.so.2`. Erstellen Sie für eine DSN-Verbindung in `odbc.ini` im Abschnitt für DSN-Einträge einen Eintrag für die Eigenschaft „GSSClient“ bzw. für eine Verbindung, bei der kein DSN verwendet wird, einen Eintrag in `odbcinst.ini` im Abschnitt für SQL Server Wire Protocol.
- Wenn Sie den DataDirect-ODBC-Treiber zum Herstellen einer Verbindung mit Microsoft SQL Server verwenden, werden die Dezimalzahlen innerhalb der Zieldatenbank basierend auf Dezimalstellenwerten in den Datenbanktabellen aufgerundet. Bei einer Dezimalstellenanzahl von 5 beispielsweise erfolgt die Abrundung der Dezimalstellen nach der fünften Stelle nach dem Dezimaltrennzeichen. Bei einer Dezimalstellenanzahl von 5 wird der Eingabewert 12.3456789 auf den Zieldezimalwert 12.34568 aufgerundet.
- Wenn Sie Microsoft SQL Server Native Client zum Konfigurieren der nativen Konnektivität zu Microsoft SQL Server-Datenbanken verwenden, werden die Dezimaldaten basierend auf der angegebenen Skalierung in den Zieldatenbanktabellen abgeschnitten. Bei einer Dezimalstellenanzahl von 5 beispielsweise erfolgt die Kürzung der Dezimalstellen ab der sechsten Stelle nach dem Dezimaltrennzeichen. Bei einer Dezimalstellenanzahl von 5 wird der Eingabewert 12.3456789 auf den Zieldezimalwert 12.34567 gekürzt.

Konfigurieren von benutzerdefinierten Eigenschaften für Microsoft SQL Server

Zur Verbesserung der Bulk Load-Leistung können Sie benutzerdefinierte Eigenschaften für Microsoft SQL Server konfigurieren.

1. Starten Sie den PowerCenter-Client und stellen Sie eine Verbindung zum Workflow Manager her.
2. Öffnen Sie einen Arbeitsablauf und wählen Sie eine Sitzung aus, die Sie konfigurieren möchten.
3. Klicken Sie auf die Registerkarte **Konfig-Objekt**.
4. Ändern Sie den Wert der **Standard-Pufferblockgröße** in 5 MB. Sie können auch den folgenden Befehl verwenden: `$INFA_HOME/server/bin/.pmrep massupdate -t session_config_property -n "Default buffer block size" -v "5MB" -f <folderName>`

Wenn Sie für eine Zeilengröße von 1 KB einen optimalen Durchsatz erzielen möchten, müssen Sie die Pufferblockgröße auf 5 MB festlegen.
5. Klicken Sie auf die Registerkarte **Eigenschaften**.
6. Ändern Sie das **Commit-Intervall** in 100000, falls die Sitzung ein relationales Ziel enthält.
7. Legen Sie die **DTM-Puffergröße** fest. Die optimale DTM-Puffergröße ist $((10 \times \text{Pufferblockgröße}) \times \text{Anzahl der Partitionen})$.

Verbinden zu einer Netezza-Datenbank unter Windows

Installieren und konfigurieren Sie ODBC auf den Computern, auf denen der PowerCenter-Integrationsdienst-Prozess ausgeführt wird und auf denen PowerCenter Client installiert wird. Sie müssen die Konnektivität zu folgenden Informatica-Komponenten unter Windows konfigurieren:

- **PowerCenter Integration Service** Installieren Sie den Netezza ODBC-Treiber auf dem Rechner, auf dem die PowerCenter Integration Service-Vorgänge ausgeführt werden. Verwenden Sie den Microsoft ODBC-Datenquellen-Administrator zum Konfigurieren der ODBC-Konnektivität.
- **PowerCenter Client.** Installieren Sie den ODBC-Treiber von Netezza auf jedem PowerCenter Client-Computer, der auf die Netezza-Datenbank zugreift. Verwenden Sie den Microsoft ODBC-Datenquellen-Administrator zum Konfigurieren der ODBC-Konnektivität. Verwenden Sie den Workflow Manager zum Erstellen eines Datenbankverbindungsobjekts für die Netezza-Datenbank.

Konfigurieren der ODBC-Konnektivität

Sie können ODBC-Konnektivität für eine Netezza-Datenbank konfigurieren.

Die folgenden Schritte enthalten eine Richtlinie zum Konfigurieren der ODBC-Konnektivität. Spezifische Anweisungen finden Sie in der Dokumentation zur Datenbank.

1. Erstellen Sie eine ODBC-Datenquelle für jede Netezza-Datenbank, auf die Sie zugreifen möchten.
Erstellen Sie mithilfe des von Netezza bereitgestellten Treibers die ODBC-Datenquelle.
Erstellen Sie einen System-DSN, wenn Sie den Informatica-Dienst mit einer Lokalen Systemkonto-Anmeldung starten. Erstellen Sie einen Benutzer-DSN, wenn Sie zum Starten des Informatica-Dienstes die Anmeldeoption "Dieses Konto" wählen.
Konfigurieren Sie nach dem Erstellen der Datenquelle deren Eigenschaften.
2. Geben Sie einen Namen für die neue ODBC-Datenquelle ein.
3. Geben Sie die IP-Adresse/den Hostnamen und die Portnummer für den Netezza-Server ein.
4. Geben Sie den Namen des Netezza-Schemas ein, in dem Sie Datenbankobjekte erstellen möchten.
5. Konfigurieren Sie den Pfad und den Dateinamen für die ODBC-Protokolldatei.
6. Überprüfen Sie, ob Sie eine Verbindung zur Netezza-Datenbank herstellen können.
Sie können die Datenbankverbindung mit dem Microsoft ODBC-Datenquellen-Administrator testen. Zum Testen der Verbindung wählen Sie die Netezza-Datenquelle aus und klicken auf "Konfigurieren". Klicken Sie in der Registerkarte "Testen" auf "Verbindung testen" und geben Sie die Verbindungsdaten für das Netezza-Schema ein.

Herstellen einer Verbindung zu einer Oracle-Datenbank unter Windows

Installieren Sie für eine native Konnektivität die für die Oracle-Datenbankserverversion geeignete Version des Oracle-Client. Verwenden Sie zur Gewährleistung der Kompatibilität zwischen Informatica und den Datenbanken die entsprechenden Datenbank-Client-Bibliotheken.

Sie müssen kompatible Versionen des Oracle-Client und des Oracle-Datenbankservers installieren. Des Weiteren müssen Sie dieselbe Version des Oracle-Client auf allen Rechnern installieren, die ihn benötigen. Informationen zur Überprüfung der Kompatibilität erhalten Sie von Oracle.

Konfigurieren der nativen Konnektivität

Sie können native Konnektivität für eine Oracle-Datenbank konfigurieren, um die Leistung zu erhöhen.

Die folgenden Schritte stellen eine Richtlinie zum Konfigurieren der nativen Konnektivität mithilfe von Oracle Net Services oder Net8 dar. Spezifische Anweisungen zur Konnektivität finden Sie in der Dokumentation zur Datenbank.

1. Vergewissern Sie sich, dass das Basisverzeichnis von Oracle eingerichtet ist.

Beispiel:

```
ORACLE_HOME=C:\Oracle
```

2. Überprüfen Sie, ob die Umgebungsvariable PATH das Oracle-bin-Verzeichnis enthält.

Wenn Sie beispielsweise Net8 installieren, kann der Pfad den folgenden Eintrag enthalten:

```
PATH=C:\ORANT\BIN;
```

3. Konfigurieren Sie den Oracle-Client so, dass eine Verbindung zur gewünschten Datenbank hergestellt wird.

Starten Sie das Dienstprogramm SQL*Net Easy Configuration oder bearbeiten Sie eine vorhandene `tnsnames.ora`-Datei im Basisverzeichnis und ändern Sie sie.

Hinweis: Standardmäßig wird die Datei `tnsnames.ora` in folgendem Verzeichnis gespeichert:

`<OracleInstallationDir>\network\admin.`

Geben Sie die richtige Syntax für die Oracle-Verbindungszeichenfolge ein. Diese lautet normalerweise `database.world`. Vergewissern Sie sich, dass die eingegebene SID mit der auf dem Oracle-Server definierten ID der Datenbankserverinstanz übereinstimmt.

Hier ist eine `tnsnames.ora`-Beispieldatei. Geben Sie die Informationen für die Datenbank ein.

```
mydatabase.world =
  (DESCRIPTION
    (ADDRESS_LIST =
      (ADDRESS =
        (COMMUNITY = mycompany.world
        (PROTOCOL = TCP)
        (Host = mymachine)
        (Port = 1521)
      )
    )
    (CONNECT_DATA =
      (SID = MYORA7)
      (GLOBAL_NAMES = mydatabase.world)
```

Bei Folgendem handelt es sich um eine Beispieldatei namens `tnsnames.ora` zum Herstellen einer Verbindung zu Oracle mithilfe des Oracle-Verbindungsmanagers:

```
ORCL19C_CMAN =
  (description=
    (address_list=
      (source_route=yes)
      (address=(protocol=tcp) (host=inh74ocm.mycompany.com) (port=1521))
      (address=(protocol=tcp) (host=inh74oradb.mycompany.com) (port=1521))
    )
    (connect_data=
      (service_name=ORCL19C.mycompany.com)
    )
  )
```

4. Stellen Sie die Umgebungsvariable `NLS_LANG` auf das Gebietsschema (Sprache, Region und Zeichensatz) ein, das der Datenbank-Client und -Server bei der Anmeldung verwenden sollen.
Der Wert dieser Variable hängt von der Konfiguration ab. Lautet der Wert beispielsweise `american_america.UTF8`, müssen Sie die Variable folgendermaßen einstellen:

```
NLS_LANG=american_america.UTF8;
```


Setzen Sie sich mit dem Datenbankadministrator in Verbindung, um den Wert dieser Variable zu bestimmen.
5. Geben Sie zum Einrichten der Zeitzone einer Standardsitzung die Umgebungsvariable `ORA_SDTZ` an, wenn der Datenintegrationsdienst Daten vom Typ „Zeitstempel mit lokaler Zeitzone“ liest oder schreibt.
Sie können die Umgebungsvariable `ORA_SDTZ` auf einen der folgenden Werte festlegen:
 - Lokale Zeitzone des Betriebssystems ('`OS_TZ`')
 - Zeitzone der Datenbank ('`DB_TZ`')
 - Absoluter Versatz von UTC (z. B. '`-05:00`')
 - Name der Zeitonenregion (z. B. '`America/Los_Angeles`')
Sie können die Umgebungsvariable auf dem Computer festlegen, auf dem der Informatica-Server ausgeführt wird.
6. Wenn sich die Datei `tnsnames.ora` nicht in demselben Speicherort wie das Oracle-Installationsverzeichnis befindet, legen Sie die `TNS_ADMIN`-Umgebungsvariable `tnsnames.ora` für das Verzeichnis fest, in dem sich die Datei `tnsnames.ora` befindet.
Wenn sich die Datei `tnsnames.ora` beispielsweise im Verzeichnis `C:\oracle\files` befindet, legen Sie die Variable wie folgt fest:

```
TNS_ADMIN= C:\oracle\files
```
7. Vergewissern Sie sich, dass Sie eine Verbindung zu der Oracle-Datenbank herstellen können.
Zum Herstellen der Verbindung zur Datenbank starten Sie `SQL*Plus` und geben die Konnektivitätsinformationen ein. Wenn Sie keine Verbindung zu der Datenbank herstellen können, vergewissern Sie sich, dass Sie alle Konnektivitätsinformationen korrekt eingegeben haben.
Verwenden Sie die in der `tnsnames.ora`-Datei definierte Verbindungszeichenfolge.

Herstellen einer Verbindung zu einer PostgreSQL-Datenbank

Installieren Sie für native Konnektivität die für die PostgreSQL-Datenbankserverversion geeignete Version des PostgreSQL-Client.

Verwenden Sie zur Gewährleistung der Kompatibilität zwischen Informatica und den Datenbanken die entsprechenden Datenbank-Client-Bibliotheken.

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

Konfigurieren der nativen Konnektivität

Sie können native Konnektivität für eine PostgreSQL-Datenbank konfigurieren, um die Leistung zu erhöhen.

Die folgenden Schritte stellen eine Richtlinie zum Konfigurieren der nativen Konnektivität über PostgreSQL dar. Spezifische Anweisungen finden Sie in der Dokumentation zur Datenbank.

1. Um die Konnektivität für den PowerCenter-Integrationsdienst- oder den PowerCenter-Repository-Dienstprozess zu konfigurieren, melden Sie sich bei dem Computer als Benutzer an, der den Serverprozess starten kann.
2. Um die PostgreSQL-Datenbank für das PowerCenter-Repository zu installieren, legen Sie Werte für den PostgreSQL-Datenbankhost, -Port und -Dienstnamen für die `pg_service.conf`-Datei im folgenden Format fest:

```
[PCRS_DB_SERVICE_NAME]
host=Database host IP
port=Database port
dbname=PowerCenter Repository Service database service name
```

Um eine sichere Verbindung zu PostgreSQL für das PowerCenter-Repository herzustellen, legen Sie den `sslmode` zusammen mit den übrigen erforderlichen Datenbankeigenschaften in der `pg_service.conf`-Datei im folgenden Format auf `require` fest: `sslmode=require`

3. Legen Sie die Umgebungsvariablen `PGSERVICEFILE`, `PGHOME` und `PATH` fest.

PGSERVICEFILE. Legen Sie die Variable auf die `pg_service.conf`-Datei fest, die die Verbindungsparameter für die PostgreSQL-Datenbankverbindung enthält. Legen Sie die Variable beispielsweise wie folgt fest:

Bei Verwendung einer Bourne-Shell:

```
$ export PGSERVICEFILE; PGSERVICEFILE=<InstallationDirectory>/pg_service.conf
```

Bei Verwendung einer C-Shell:

```
$ setenv PGSERVICEFILE <InstallationDirectory>/pg_service.conf
```

PGHOME. Legen Sie die Variable auf den PostgreSQL-Installationspfad fest, unter dem Sie den PostgreSQL-Client installiert haben. Legen Sie die Variable beispielsweise wie folgt fest:

Bei Verwendung einer Bourne-Shell:

```
$ export PGHOME; PGHOME=/usr/pgsql-10
```

Bei Verwendung einer C-Shell:

```
$ setenv PGHOME /usr/pgsql-10
```

PATH. Zum Ausführen der PostgreSQL-Befehlszeilenprogramme müssen Sie die Variable so festlegen, dass sie das PostgreSQL-Clientverzeichnis (`pgsql`) enthält. Legen Sie die Variable beispielsweise wie folgt fest:

Bei Verwendung einer Bourne-Shell:

```
$ export PATH; PATH=${PATH}:${PGHOME}
```

Bei Verwendung einer C-Shell:

```
$ setenv PATH ${PGHOME}:${PATH}
```

4. Prüfen Sie, ob Sie eine Verbindung zur PostgreSQL-Datenbank herstellen können.

Um eine Verbindung zur PostgreSQL-Datenbank herzustellen, starten Sie das Dienstprogramm `psql` und geben Sie die Konnektivitätsinformationen ein.

Konfigurieren der ODBC-Konnektivität

Sie können die ODBC-Verbindung zu einer PostgreSQL-Datenbank unter Windows konfigurieren.

Die folgenden Schritte bieten eine Orientierungshilfe zur Konfiguration der ODBC-Konnektivität.

1. Erstellen Sie eine ODBC-Datenquelle mithilfe des DataDirect ODBC 7.1 Wire Protocol-Treibers für PostgreSQL von Informatica.
2. Stellen Sie sicher, dass Sie mithilfe der ODBC-Datenquelle eine Verbindung zur PostgreSQL-Datenbank herstellen können.

Spezifische Anweisungen finden Sie in der Dokumentation zur Datenbank.

Verbinden zu einer Sybase ASE-Datenbank unter Windows

Installieren Sie für eine native Konnektivität die für Ihre Datenbankversion geeignete Version von Open Client. Verwenden Sie zur Gewährleistung der Kompatibilität zwischen Informatica und den Datenbanken die entsprechenden Datenbank-Client-Bibliotheken.

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

Wenn Sie ein Sybase ASE-Repository erstellen, wiederherstellen oder upgraden möchten, setzen Sie *Nullen standardmäßig zulassen* auf der Datenbankebene auf TRUE. Hiermit wird der Standard-Nulltyp der Spalte entsprechend dem SQL-Standard in Null geändert.

Konfigurieren von nativer Konnektivität

Sie können native Konnektivität für eine Sybase ASE-Datenbank konfigurieren, um die Leistung zu erhöhen.

Die folgenden Schritte stellen eine Richtlinie zum Konfigurieren der nativen Konnektivität dar. Spezifische Anweisungen finden Sie in der Dokumentation zur Datenbank.

1. Überprüfen Sie, ob die Umgebungsvariable SYBASE auf das Sybase ASE-Verzeichnis verweist.

Beispiel:

```
SYBASE=C:\SYBASE
```

2. Überprüfen Sie, ob die Umgebungsvariable PATH das Sybase ASE-Verzeichnis enthält.

Beispiel:

```
PATH=C:\SYBASE\OCS-15_0\BIN;C:\SYBASE\OCS-15_0\DLL
```

3. Konfigurieren Sie Sybase Open Client so, dass eine Verbindung zur gewünschten Datenbank hergestellt wird.

Verwenden Sie SQLEDT zum Konfigurieren des Sybase-Client oder kopieren Sie eine vorhandene SQL.INI-Datei (im Verzeichnis %SYBASE%\INI) und nehmen Sie etwaige erforderliche Änderungen vor.

Wählen Sie NLWNSCK als Net-Library-Treiber und schließen Sie den Sybase ASE-Servernamen ein.

Geben Sie Hostnamen und Portnummer für den Sybase ASE-Server ein. Wenn Ihnen Hostname und Portnummer nicht bekannt sind, wenden Sie sich an den Systemadministrator.

4. Führen Sie optional die folgenden Aufgaben aus, um eine Verbindung zur SSL-fähigen Sybase ASE-Datenbank herzustellen:

- Geben Sie die folgenden Sicherheitsattribute auf der Registerkarte **Sicherheit** an, wenn Sie den Datenquellennamen in der Sybase-Treibereigenschaft konfigurieren:

Attribut	Beschreibung
Verschlüsselungsmethode	Gibt an, ob Daten bei der Netzwerkübertragung verschlüsselt werden. Wählen Sie „SSL“ aus.
Serverzertifikat validieren	Gibt an, ob Informatica das vom Datenbankserver gesendete Zertifikat validiert, wenn die SSL-Verschlüsselung aktiviert wird.
Truststore	Der Speicherort und der Name der Truststore-Datei.
Truststore-Passwort	Das Passwort für den Zugriff auf den Inhalt der Truststore-Datei.
Hostname im Zertifikat	Der Hostname, der vom SSL-Administrator eingerichtet wird, um den im Zertifikat enthaltenen Hostnamen zu validieren.

- Fügen Sie der Datei „trusted.txt“ im Sybase ASE-Client das Sybase ASE-Serverzertifikat hinzu.
- Fügen Sie der Datei SQL.INI die folgenden Sybase ASE-Serververbindungsdetails hinzu:

```
<server_instance_name>  
    master tcp ether <host name> <port number> ssl="CN='common_name'"  
    query tcp ether <host name> <port number> ssl="CN='common_name'"
```

5. Stellen Sie sicher, dass Sie eine Verbindung zur Sybase ASE-Datenbank herstellen können.

Zum Herstellen der Verbindung zur Datenbank starten Sie ISQL und geben die Konnektivitätsinformationen ein. Wenn Sie keine Verbindung zu der Datenbank herstellen können, vergewissern Sie sich, dass Sie alle Konnektivitäts-Informationen korrekt eingegeben haben.

Bei Benutzernamen und Datenbanknamen bitte die Groß-/Kleinschreibung beachten.

Herstellen einer Verbindung zu einer Teradata-Datenbank über Windows

Installieren und konfigurieren Sie native Client-Software auf den Computern, auf denen der Datenintegrationsdienst- und PowerCenter-Integrationsdienst-Prozess ausgeführt und auf denen Informatica Developer und PowerCenter Client installiert wird. Verwenden Sie zur Gewährleistung der Kompatibilität zwischen Informatica und den Datenbanken die entsprechenden Datenbank-Client-Bibliotheken. Sie müssen die Konnektivität zu folgenden Informatica-Komponenten unter Windows konfigurieren:

- **Integrationsdienst** Installieren Sie den Teradata-Client, den Teradata-ODBC-Treiber sowie weitere eventuell benötigte Teradata-Client-Software auf dem Computer, auf dem der Datenintegrationsdienst und der PowerCenter-Integrationsdienst ausgeführt wird. Außerdem müssen Sie die ODBC-Konnektivität konfigurieren.
- **Informatica Developer** Installieren Sie den Teradata-Client, den Teradata-ODBC-Treiber sowie weitere eventuell benötigte Teradata-Client-Software auf jedem Rechner, auf dem sich ein Developer Tool befindet, das auf Teradata zugreift. Außerdem müssen Sie die ODBC-Konnektivität konfigurieren.

- **PowerCenter Client** Installieren Sie den Teradata-Client, den Teradata-ODBC-Treiber sowie weitere eventuell benötigte Teradata-Client-Software auf jedem PowerClient-Rechner, der auf Teradata zugreift. Verwenden Sie den Workflow Manager zum Erstellen eines Datenbankverbindungsobjekts für die Teradata-Datenbank.

Hinweis: Entsprechend einer Empfehlung von Teradata verwendet Informatica ODBC für die Verbindung mit Teradata. ODBC ist eine native Schnittstelle für Teradata.

Konfigurieren der ODBC-Konnektivität

Sie können ODBC-Konnektivität für eine Teradata-Datenbank konfigurieren.

Die folgenden Schritte enthalten eine Richtlinie zum Konfigurieren der ODBC-Konnektivität. Spezifische Anweisungen finden Sie in der Dokumentation zur Datenbank.

1. Erstellen Sie eine ODBC-Datenquelle für jede Teradata-Datenbank, auf die Sie zugreifen möchten.
Erstellen Sie mithilfe des von Teradata bereitgestellten Treibers die ODBC-Datenquelle.
Erstellen Sie einen System-DSN, wenn Sie den Informatica-Dienst mit einer *Lokalen Systemkonto*-Anmeldung starten. Erstellen Sie einen Benutzer-DSN, wenn Sie zum Starten des Informatica-Dienstes die Anmeldeoption *Dieses Konto* wählen.
2. Geben Sie den Namen für die neue ODBC-Datenquelle und den Namen des Teradata-Servers oder dessen IP-Adresse ein.
Geben Sie zum Konfigurieren einer Verbindung zu einer einzelnen Teradata-Datenbank den DefaultDatabase-Namen ein. Geben Sie zum Erstellen einer Einzelverbindung zur Standard-Datenbank den Benutzernamen und das Passwort ein. Zum Herstellen einer Verbindung zu mehreren Datenbanken mithilfe derselben ODBC-Datenquelle lassen Sie die Felder DefaultDatabase, Benutzername und Passwort leer.
3. Konfigurieren Sie die Datumsoptionen im Dialogfeld "Optionen".
Geben Sie im Dialogfeld "Teradata-Optionen" AAA für das DateTime-Format an.
4. Konfigurieren Sie den Sitzungsmodus im Dialogfeld "Optionen".
Wählen Sie bei Erstellung einer Zieldatenquelle den Sitzungsmodus ANSI. Beim ANSI-Sitzungsmodus führt Teradata bei Auftreten eines Zeilenfehlers kein Rollback der Transaktion durch. Beim Teradata-Sitzungsmodus führt Teradata bei Auftreten eines Zeilenfehlers ein Rollback der Transaktion durch. Im Teradata-Modus kann der Integration Service das Rollback nicht erkennen und zeichnet ihn nicht im Sitzungsprotokoll auf.
5. Überprüfen Sie, ob Sie eine Verbindung zur Teradata-Datenbank herstellen können.
Verwenden Sie zum Testen der Verbindung ein Teradata-Client-Programm wie WinDDI, BTEQ, Teradata Administrator oder Teradata SQL Assistant.

Aktualisieren des DynamicSections-Parameters einer DB2-Datenbank

Dieser Anhang umfasst die folgenden Themen:

- [DynamicSections-Parameter - Übersicht, 378](#)
- [Einrichten des DynamicSections-Parameters, 378](#)

DynamicSections-Parameter - Übersicht

IBM DB2-Pakete enthalten die SQL-Anweisungen, die auf dem Datenbankserver ausgeführt werden sollen. Mit dem Parameter DynamicSections einer DB2-Datenbank wird die Höchstzahl der ausführbaren Anweisungen festgelegt, die es für einen Datenbanktreiber in einem Paket geben darf. Sie können den Wert des Parameters DynamicSections erhöhen, um eine größere Anzahl ausführbarer Anweisungen in einem DB2-Paket zu ermöglichen. Zum Ändern des Parameters DynamicSections stellen Sie mit einem Systemadministrator-Benutzerkonto mit BINDADD-Berechtigung eine Verbindung zur Datenbank her.

Einrichten des DynamicSections-Parameters

Verwenden Sie das Dienstprogramm DataDirect Connect für JDBC, um den Wert des DynamicSections-Parameters in der DB2-Datenbank zu erhöhen.

Gehen Sie zum Aktualisieren des DynamicSections-Parameters mithilfe des Dienstprogramms DataDirect Connect für JDBC folgendermaßen vor:

- Laden Sie das Dienstprogramm DataDirect Connect für JDBC herunter und installieren Sie es.
- Führen Sie den Test für das JDBC-Tool aus.

Herunterladen und Installieren des Dienstprogramms DDconnect JDBC

Laden Sie das Dienstprogramm DataDirect Connect für JDBC von der DataDirect-Download-Website auf einen Computer herunter, der auf den DB2-Datenbankserver zugreifen kann. Extrahieren Sie den Inhalt der Dienstprogrammdatei und führen Sie das Installationsprogramm aus.

1. Wechseln Sie zur DataDirect-Download-Site:
<http://www.datadirect.com/support/product-documentation/downloads>
2. Wählen Sie den Treiber Connect für JDBC für eine IBM DB2-Datenquelle aus.
3. Registrieren Sie sich, um das Dienstprogramm DataDirect Connect für JDBC herunterzuladen.
4. Laden Sie das Dienstprogramm auf einen Computer herunter, der auf den DB2-Datenbankserver zugreifen kann.
5. Extrahieren Sie den Inhalt des Dienstprogramms in ein temporäres Verzeichnis.
6. Führen Sie in dem Verzeichnis, in dem Sie die Datei extrahiert haben, das Installationsprogramm aus.

Das Installationsprogramm erstellt einen Ordner mit dem Namen „testforjdbc“ im Installationsverzeichnis.

Ausführen des Tests für das JDBC-Tool

Führen Sie nach der Installation des Dienstprogramms DataDirect Connect für JDBC den Test für das JDBC-Tool aus, um eine Verbindung zur DB2-Datenbank herzustellen. Zum Herstellen einer Verbindung zur Datenbank müssen Sie das Systemadministrator-Benutzerkonto mit der BINDADD-Berechtigung verwenden.

1. Richten Sie in der DB2-Datenbank ein Systemadministrator-Benutzerkonto mit der BINDADD-Berechtigung ein.
2. Führen Sie im Verzeichnis, in dem Sie das Dienstprogramm DataDirect Connect für JDBC installiert haben, den Test für das JDBC-Tool (testforjdbc) aus.
3. Klicken Sie im Fenster mit dem Test für das JDBC-Tool auf „Zum Fortsetzen hier klicken“.
4. Klicken Sie auf „Verbindung“ > „Zu DB verbinden“.
5. Geben Sie in das Feld Datenbank die folgenden Text ein:

```
jdbc:datadirect:db2://  
HostName:PortNumber;databaseName=DatabaseName;CreateDefaultPackage=TRUE;ReplacePackage=TRUE;DynamicSections=3000
```

HostName stellt den Namen des Rechners dar, auf dem sich der DB2-Datenbankserver befindet.

PortNumber stellt die Portnummer der Datenbank dar.

DatabaseName stellt den Namen der DB2-Datenbank dar.

6. Geben Sie in die Felder für den Benutzernamen und das Passwort den Systemadministrator-Benutzernamen und das Passwort ein, das Sie zum Verbinden mit der DB2-Datenbank verwenden.
7. Klicken Sie auf „Verbinden“ und schließen Sie anschließend das Fenster.

INDEX

A

- AddLicense (infacmd)
 - Fehlerbehebung [265](#)
- Analyst-Dienst
 - erstellen [306](#)
 - konfigurieren [306](#)
 - nach dem Erstellen [308](#)
 - Temporäre Verzeichnisse [274](#)
 - Voraussetzungen [274](#)
- Anforderungen an Software von Drittanbietern
 - Developer Tool [314](#)
 - PowerCenter-Client [314](#)
- Anmeldung
 - Fehlerbehebung [276](#)
- Anwendungsdienste
 - Content-Management-Dienst [58](#)
 - Analyst-Dienst [58](#)
 - Datenintegrationsdienst [61](#), [78](#)
 - Installationsanforderungen [31](#), [44](#)
 - Metadata Manager Service [68](#)
 - Modellrepository-Dienst [73](#), [79](#)
 - Ports [28](#), [42](#)
 - Produkte [52](#)
 - Suchdienst [82](#)
 - Überwachungsmodellrepository-Dienst [77](#)
- Arbeitsablauf
 - IBM DB2-Datenbankanforderungen [65](#)
 - Microsoft SQL Server-Datenbankanforderungen [66](#)
 - Oracle-Datenbankanforderungen [66](#)
- Arbeitsablauf-Datenbank
 - Microsoft Azure SQL-Datenbankanforderungen [66](#)
 - PostgreSQL-Datenbankanforderungen [67](#)
- Arbeitsabläufe
 - Datenbankanforderungen [65](#)
- automatischer Modus
 - Installieren der Informatica-Clients [320](#)
 - Installieren von Informatica-Diensten [257](#)

B

- Beispiele
 - odbc.ini, Datei [359](#)
- Benutzerkonten
 - Modellrepository [288](#)
 - PowerCenter-Repository [295](#)
 - UNIX [35](#)
 - Windows [46](#)
- Benutzerprinzipalnamen
 - Formatierung [96](#)
- Betriebsmodus
 - PowerCenter-Repository-Dienst [295](#)
- Bibliotheksanforderungen
 - Windows [42](#)

- Bibliothekspfade
 - Umgebungsvariablen [34](#)

C

- catalina.out
 - Fehler bei der Installation beheben [263](#)
- Clients
 - Konfigurieren für sichere Domänen [316](#)
- Content-Management-Dienst
 - konfigurieren [304](#)
- Content-Managementdienst
 - erstellen [304](#)

D

- database clients
 - IBM DB2 client application enabler [84](#)
 - Microsoft SQL Server native clients [84](#)
 - Oracle clients [84](#)
 - PostgreSQL client [84](#)
 - Sybase open clients [84](#)
- Datenbank
 - mit PostgreSQL verbinden [347](#), [373](#)
 - Verbinden zu Sybase ASE [351](#)
 - zu Netezza verbinden (Windows) [371](#)
 - zu Oracle verbinden [344](#)
 - zu Sybase ASE verbinden [375](#)
 - zu Teradata verbinden (Windows) [376](#)
- Datenbank-Clients
 - Konfigurieren [85](#)
 - Umgebungsvariablen [85](#)
- Datenbankanforderungen
 - Arbeitsablauf-Datenbank [65](#)
 - Datenobjekt-Cache [61](#)
 - Modellrepository [74](#)
 - PowerCenter-Repository [79](#)
 - Profiling Warehouse [63](#)
 - Referenzdaten-Warehouse [59](#)
- Datenbankbenutzerkonten
 - Richtlinien für das Einrichten [52](#)
- Datenbanken
 - mit IBM DB2 verbinden [338](#), [367](#)
 - mit Informix verbinden [340](#), [368](#)
 - mit Microsoft Access verbinden [368](#)
 - mit Microsoft SQL Server verbinden [369](#)
 - Repository [52](#)
 - verbinden zu (Windows) [366](#)
 - Verbindung herstellen (UNIX) [337](#)
 - Verbindungen testen [85](#)
 - zu Netezza verbinden (UNIX) [342](#)
 - zu Oracle verbinden [371](#)
 - zu Teradata verbinden (UNIX) [353](#)

- Datenbankenvorbereitungen
 - Repositorys [52](#)
- Datenbankverbindungen
 - erstellen [276](#)
- Datenintegrationsdienst
 - erstellen [289](#)
 - Konfiguration der Hostdatei [292](#)
 - konfigurieren [289](#)
 - nach dem Erstellen [292](#)
- Datenobjekt-Cache
 - Datenbankanforderungen [61](#)
 - IBM DB2-Datenbankanforderungen [62](#)
 - Microsoft Azure SQL-Datenbankanforderungen [62](#)
 - Microsoft SQL Server-Datenbankanforderungen [62](#)
 - Oracle-Datenbankanforderungen [62](#)
- dbs2 connect
 - Datenbankverbindungen testen [85](#)
- Debug-Protokolle
 - Beheben von Fehlern bei der Installation [262](#)
- Deinstallation
 - Regeln und Richtlinien [324](#)
- Developer Tool
 - Anforderungen an Software von Drittanbietern [314](#)
- Dienste
 - Aufgaben vor der Installation unter Windows [40](#)
- Dienstmanager
 - Protokolldateien [263](#)
- Dienstprinzipalnamen
 - erstellen [96](#)
 - Kerberos-Authentifizierung [91](#)
- DISPLAY
 - Umgebungsvariablen [46](#)
- Domänen
 - konfigurieren [268](#)
 - Ports [28, 42](#)
 - Übersicht [19](#)
- Domänen-Konfigurations-Repository
 - Fehlerbehebung [264](#)
 - Microsoft SQL Server-Datenbankanforderungen [76](#)
 - Vorbereiten der Datenbanken [53](#)
- Domänenkonfiguration
 - Microsoft Azure SQL-Datenbankanforderungen [55](#)
- Domänenkonfigurations-Repository
 - IBM DB2 – Datenbankanforderungen [54](#)
 - IBM DB2-Datenbankanforderungen [74](#)
 - Microsoft Azure SQL-Datenbankanforderungen [75](#)
 - Microsoft SQL Server – Datenbankanforderungen [55](#)
 - Oracle – Datenbankanforderungen [55](#)
 - PostgreSQL-Datenbankanforderungen [56](#)
 - Sybase ASE – Datenbankanforderungen [56](#)

E

- Erstellung von Repository-Inhalten
 - Metadata Manager-Dienst [304](#)

F

- Fehlerbehebung
 - Anfügen von Domänen [264](#)
 - anmelden [276](#)
 - Domänen-Konfigurations-Repository [264](#)
 - Erstellen von Domänen [264](#)
 - Informatica-Dienste [264](#)
 - Kerberos-Authentifizierung [276](#)
 - Lizenzen [265](#)

- Fehlerbehebung (*Fortsetzung*)
 - Pingen von Domänen [265](#)

G

- Gebietsschema-Umgebungsvariablen
 - konfigurieren [268](#)
- Geteilte Domäne für Metadata Manager
 - Definition [72](#)
 - Überlegungen [72](#)
- Globaler Kundensupport von Informatica
 - Kontaktinformationen [14](#)
- Grafikmodus
 - Installieren der Informatica-Clients [314](#)
 - Installieren von Informatica-Diensten [175](#)

H

- Hostdatei
 - Datenintegrationsdienst [292](#)
- HTTPS
 - Installationsanforderungen [35, 47](#)

I

- i10Pi
 - UNIX [112](#)
 - Windows [115](#)
- IATEMPDIR
 - Umgebungsvariablen [34, 46](#)
- IBM DB2
 - DB2CODEPAGE einrichten [367](#)
 - DB2INSTANCE einrichten [367](#)
 - Einzelknoten-Tabellenbereich [80](#)
 - mit Integration Service verbinden (Windows) [338, 367](#)
- IBM DB2 – Datenbankanforderungen
 - Modellrepository-Datenbank [54](#)
- IBM DB2-Datenbankanforderungen
 - Arbeitsablauf-Repository [65](#)
 - Datenobjekt-Cache [62](#)
 - Domänen-Repository [54, 74](#)
 - Metadata Manager-Repository [69](#)
 - Modellrepository-Datenbank [74](#)
 - PowerCenter-Repository [80](#)
 - Profiling-Warehouse [63](#)
 - Referenzdaten-Warehouse [59](#)
- infacmd
 - Hinzufügen von Knoten zu Domänen [264](#)
 - Pingen von Objekten [265](#)
- infasetup
 - Definieren von Domänen [264](#)
 - Definieren von Worker-Knoten [264](#)
- Informatica Administrator
 - anmelden [275](#)
- Informatica Developer
 - Konfigurieren von lokalem Workspace-Verzeichnis [317](#)
 - lokale Computer [317](#)
 - Remote-Computer [317](#)
 - Sprachen installieren [315](#)
- Informatica-Clients
 - automatische Installation [320](#)
 - deinstallieren [324, 327](#)
 - Installation im Grafikmodus [314](#)
- Informatica-Dienste
 - automatische Installation [257](#)

Informatica-Dienste (Fortsetzung)

- Fehlerbehebung [264](#)
- Installation im Grafikmodus [175](#)
- Starten und Stoppen unter UNIX [330](#)

Informatica-Server

- deinstallieren [324](#)

Informix

- mit Integration Service verbinden (UNIX) [340](#)
- mit Integration Service verbinden (Windows) [368](#)
- verbinden mit Integrationsdienst (UNIX) [340](#)

Installation

- Sichern der Dateien vor [33](#), [45](#)

Installationsanforderungen

- Anwendungsdienst-Anforderungen [31](#), [44](#)
- Port-Anforderungen [28](#), [42](#)
- Schlüsselspeicherdateien [35](#), [47](#)
- Truststore-Dateien [35](#), [47](#)
- Umgebungsvariablen [34](#), [46](#)

Installationsprotokolle

- Beschreibungen [262](#)

isql

- Datenbankverbindungen testen [85](#)

J

JDBC

- verbinden zu (Windows) [366](#)

JDBC-Datenquellen

- Verbindung herstellen (UNIX) [356](#)

JRE_HOME

- Umgebungsvariablen [34](#), [46](#)

K

Kerberos SPN-Formatgenerator [92](#)

Kerberos-Authentifizierung

- Erstellen von Dienstprinzipalnamen [96](#)
- Erstellen von Keytab-Dateien [96](#)
- Fehlerbehebung [276](#)
- Generieren der SPN-Formate [91](#)
- Generieren von Namensformaten für Keytab-Dateien [91](#)
- Konfigurationsdateien [89](#)

Keytab-Dateien

- Kerberos-Authentifizierung [91](#), [96](#)

Knoten

- Fehlerbehebung [264](#)

Kompatibilität der Codeseite

- Anwendungsdienste [268](#)
- Gebietsschema [268](#)

Konfiguration

- Domänen [268](#)
- Kerberos-Dateien [89](#)
- Umgebungsvariablen [269](#)
- Umgebungsvariablen unter UNIX [271](#)

L

LANG

- Gebietsschema-Umgebungsvariablen [34](#), [46](#)
- Umgebungsvariablen [268](#)

LC_ALL

- Gebietsschema-Umgebungsvariablen [34](#), [46](#)
- Umgebungsvariablen [268](#)

LC_CTYPE

- Umgebungsvariablen [268](#)

Linux

- Umgebungsvariablen für Datenbank-Clients [85](#)

Lizenzen

- hinzufügen [265](#)

Lizenzschlüssel

- überprüfen [39](#), [50](#)

localhost

- Datenintegrationsdienst [292](#)

M

Metadata Manager-Dienst

- erstellen [299](#)
- Geteilte Domäne [72](#)
- konfigurieren [299](#)
- nach dem Erstellen [304](#)
- Repository-Inhalte erstellen [304](#)
- Überlegungen zu geteilten Domänen [72](#)

Metadata Manager-Repository

- Heapgrößen [69](#)
- IBM DB2-Datenbankanforderungen [69](#)
- Microsoft SQL Server-Datenbankanforderungen [70](#)
- Optimieren der IBM DB2-Datenbanken [69](#)
- Oracle-Datenbankanforderungen [71](#)
- temporäre System-Tabellenbereiche [69](#)

Microsoft Access

- mit Integration Service verbinden [368](#)

Microsoft Azure SQL-Datenbankanforderungen

- Arbeitsablauf-Datenbank [66](#)
- Datenobjekt-Cache [62](#)
- Domänenkonfiguration [55](#)
- Domänenkonfigurations-Repository [75](#)
- Referenzdaten-Warehouse [60](#)

Microsoft Excel

- mit Integration Service verbinden [368](#)
- Verwenden von PmNullPasswd [368](#)
- Verwenden von PmNullUser [368](#)

Microsoft SQL Server

- mit Integration Service verbinden [369](#)
- Verbinden von UNIX [341](#)

Microsoft SQL Server-Datenbankanforderungen

- Arbeitsablauf-Repository [66](#)
- Datenobjekt-Cache [62](#)
- Domänen-Konfigurations-Repository [76](#)
- Domänenkonfigurations-Repository [55](#)
- Metadata Manager-Repository [70](#)
- PowerCenter-Repository [80](#)
- Profiling-Warehouse [63](#)
- Referenzdaten-Warehouse [60](#)

Mindestsystemanforderungen

- Knoten [31](#), [44](#)

Modellrepository

- Benutzer [288](#)
- Datenbankanforderungen [74](#)
- IBM DB2 – Datenbankanforderungen [54](#)
- IBM DB2-Datenbankanforderungen [74](#)
- Oracle-Datenbankanforderungen [76](#)
- PostgreSQL-Datenbankanforderungen [77](#)

Modellrepository-Dienst

- Erstellen [284](#)
- konfigurieren [284](#)
- nach dem Erstellen [287](#)

N

- Netezza
 - verbinden mit Informatica-Clients (UNIX) [342](#)
 - verbinden mit Integrationsdienst (UNIX) [342](#)
 - verbinden über Integrationsdienst (Windows) [371](#)
 - von Informatica-Clients aus verbinden (Windows) [371](#)
- node.log
 - Fehler bei der Installation beheben [263](#)
- Normalmodus
 - PowerCenter-Repository-Dienst [295](#)

O

- ODBC-Datenquellen
 - verbinden zu (Windows) [366](#)
 - Verbindung herstellen zu (UNIX) [357](#)
- odbc.ini, Datei
 - Beispiel [359](#)
- Optimierung
 - PowerCenter-Repository [80](#)
- Oracle
 - zu Integration Service verbinden (UNIX) [344](#)
 - zu Integration Service verbinden (Windows) [371](#)
- Oracle Net Services
 - zum Verbinden von Integration Service mit Oracle verwenden (UNIX) [344](#)
 - zum Verbinden von Integration Service mit Oracle verwenden (Windows) [371](#)
- Oracle-Datenbankanforderungen
 - Arbeitsablauf-Repository [66](#)
 - Datenobjekt-Cache [62](#)
 - Domänenkonfigurations-Repository [55](#)
 - Metadata Manager-Repository [71](#)
 - Modellrepository [76](#)
 - PowerCenter-Repository [80](#)
 - Profiling Warehouse [64](#)
 - Referenzdaten-Warehouse [60](#)

P

- Patch-Anforderungen
 - Installation [27](#)
- Patchanforderungen
 - Windows [42](#)
- PATH
 - Umgebungsvariablen [34](#)
- pg_service.conf
 - PostgreSQL-Datenbankanforderungen [81](#)
- PGSERVICEFILE-Umgebungsvariable
 - PostgreSQL-Datenbankanforderungen [81](#)
- Ping (infacmd)
 - Fehlerbehebung [265](#)
- Portanforderungen
 - Installationsanforderungen [28, 42](#)
- Ports
 - Anforderungen [28, 42](#)
 - Anwendungsdienste [28, 42](#)
 - Domänen [28, 42](#)
- PostgreSQL
 - mit Integration Service verbinden (Windows) [373](#)
 - mit Integrationsdienst verbinden (UNIX) [347](#)
- PostgreSQL-Datenbankanforderungen
 - Arbeitsablauf-Datenbank [67](#)
 - Domänenkonfigurations-Repository [56](#)
 - Modellrepository [77](#)

- PostgreSQL-Datenbankanforderungen (*Fortsetzung*)
 - pg_service.conf [81](#)
 - PGSERVICEFILE-Umgebungsvariable [81](#)
 - PowerCenter-Repository [81](#)
- PowerCenter Client
 - Anforderungen an Software von Drittanbietern [314](#)
- PowerCenter-Integrationsdienst
 - erstellen [297](#)
 - konfigurieren [297](#)
 - nach dem Erstellen [299](#)
- PowerCenter-Repository
 - Benutzer [295](#)
 - Datenbankanforderungen [79](#)
 - IBM DB2-Datenbankanforderungen [80](#)
 - Microsoft SQL Server-Datenbankanforderungen [80](#)
 - Optimieren der IBM DB2-Datenbanken [80](#)
 - Oracle RAC [80](#)
 - Oracle-Datenbankanforderungen [80](#)
 - PostgreSQL-Datenbankanforderungen [81](#)
 - Sybase ASE-Datenbankanforderungen [82](#)
- PowerCenter-Repository-Dienst
 - erstellen [293](#)
 - konfigurieren [293](#)
 - nach dem Erstellen [295](#)
 - Normalmodus [295](#)
- Profiling Warehouse
 - Datenbankanforderungen [63](#)
 - Microsoft SQL Server-Datenbankanforderungen [63](#)
 - Oracle-Datenbankanforderungen [64](#)
- Profiling-Warehouse
 - IBM DB2-Datenbankanforderungen [63](#)
- Protokolldateien
 - catalina.out [263](#)
 - Debug-Protokolle [262](#)
 - Installation [262](#)
 - Installation Protokolle [262](#)
 - node.log [263](#)
 - Typen [262](#)

Q

- Quelldatenbanken
 - durch ODBC (UNIX) Verbindung herstellen [357](#)
 - Verbinden über JDBC (UNIX) [356](#)

R

- Referenzdaten-Warehouse
 - Datenbankanforderungen [59](#)
 - IBM DB2-Datenbankanforderungen [59](#)
 - Microsoft Azure SQL-Datenbankanforderungen [60](#)
 - Microsoft SQL Server-Datenbankanforderungen [60](#)
 - Oracle-Datenbankanforderungen [60](#)
- repositories
 - installing database clients [84](#)
- Repositorys
 - Konfigurieren der nativen Konnektivität [83](#)
 - Vorbereiten der Datenbanken [52](#)

S

- Schlüsselspeicherdateien
 - Installationsanforderungen [35, 47](#)
- sichere Domänen
 - Konfigurieren von Clients [316](#)

- Sichern der Dateien
 - vor dem Installieren [33, 45](#)
 - vor dem Upgrade [33, 45](#)
- SPN [91](#)
- Sprachen
 - Client-Tools [315](#)
- sqlplus
 - Datenbankverbindungen testen [85](#)
- Suchdienst
 - Erstellen [308, 309](#)
 - konfigurieren [308](#)
- Sybase ASE
 - Verbinden zu Integration Service (UNIX) [351](#)
 - zu Integration Service verbinden (Windows) [375](#)
- Sybase ASE – Datenbankanforderungen
 - Domänenkonfigurations-Repository [56](#)
- Sybase ASE-Datenbankanforderungen
 - PowerCenter-Repository [82](#)
- Systemanforderungen
 - Minimal [26, 41](#)
- Systemvoraussetzungen
 - Anwendungsdienste [31, 44](#)
 - Minimal [26, 41](#)

T

- Tabellenbereichs
 - Einzelknoten [80](#)
- Target-Datenbanken
 - Verbinden über JDBC (UNIX) [356](#)
- Teradata
 - verbinden mit Informatica-Clients (UNIX) [353](#)
 - verbinden mit Informatica-Clients (Windows) [376](#)
 - verbinden mit Integrationsdienst (UNIX) [353](#)
 - verbinden mit Integrationsdienst (Windows) [376](#)
- Truststore-Dateien
 - Installationsanforderungen [35, 47](#)

U

- Übersicht
 - vor dem Installieren der Clients [313](#)
- Umgebungsvariablen
 - Bibliothekspfade unter UNIX [271](#)
 - Datenbank-Clients [85](#)
 - Gebietsschema [268](#)
 - INFA_TRUSTSTORE [316](#)
 - INFA_TRUSTSTORE_PASSWORD [316](#)
 - Installation [34, 46](#)
 - konfigurieren [269](#)
 - Konfigurieren unter UNIX [271](#)
 - Konfigurieren von Clients [316](#)
 - LANG [268](#)
 - LANG_C [268](#)
 - LC_ALL [268](#)
 - LC_CTYPE [268](#)
 - UNIX [269](#)
 - UNIX-Datenbank-Clients [85](#)
- UNIX
 - Benutzerkonten [35](#)
 - Bibliothekspfade [271](#)
 - i10Pi [112](#)
 - Kerberos SPN-Formatgenerator [92](#)
 - Starten und Stoppen der Informatica-Dienste [330](#)
 - Umgebungsvariablen [269](#)
 - Umgebungsvariablen für Datenbank-Clients [85](#)

- UNIX (Fortsetzung)
 - Variablen des Datenbank-Clients [85](#)
 - Verbinden zu JDBC-Datenquellen [356](#)
 - Verbindung zu ODBC-Datenquellen herstellen [357](#)
 - vor der Installation [112](#)
- upgrades
 - Sichern der Dateien vor [33, 45](#)

V

- verbinden
 - Integration Service mit IBM DB2 (Windows) [367](#)
 - Integration Service mit Informix (UNIX) [340](#)
 - Integration Service mit Informix ASE (Windows) [368](#)
 - Integration Service mit Microsoft Access [368](#)
 - Integration Service mit Oracle (UNIX) [344](#)
 - Integration Service mit Oracle (Windows) [371](#)
 - Integration Service mit Sybase ASE (UNIX) [351](#)
 - Integration Service mit Sybase ASE (Windows) [375](#)
 - Integrationsdienst mit PostgreSQL (UNIX) [347](#)
 - Integrationsdienst mit PostgreSQL (Windows) [373](#)
 - Microsoft Excel mit Integration Service [368](#)
 - UNIX-Datenbanken [337](#)
 - Windows über JDBC [366](#)
 - Windows-Datenbanken [366](#)
- Verbinden
 - Integration Service mit IBM DB2 (Windows) [338](#)
 - Integration Service mit Informix (UNIX) [340](#)
 - Integration Service mit Microsoft SQL Server [369](#)
 - Integrationsdienste zu ODBC-Datenquellen (UNIX) [357](#)
- Verbindung herstellen
 - Integrationsdienst zu JDBC-Datenquellen (UNIX) [356](#)
- Verbindungen
 - Eigenschaften für Oracle [280](#)
 - Erstellen von Datenbankverbindungen [276, 282](#)
 - IBM DB2-Eigenschaften [277](#)
 - Microsoft Azure SQL-Datenbankeigenschaften [278](#)
 - Microsoft SQL Server-Eigenschaften [279](#)
 - PostgreSQL-Eigenschaften [281](#)
- vor dem Installieren der Clients
 - Übersicht [313](#)
- Vor dem Installieren der Clients
 - Überprüfen der Installationsanforderungen [313](#)
 - Überprüfen der Mindestsystemanforderungen [313](#)
- vor der Installation
 - i10Pi unter UNIX [112](#)
 - i10Pi unter Windows [115](#)
 - Services unter Windows [40](#)

W

- Windows
 - Benutzerkonten [46](#)
 - Bibliotheksanforderungen [42](#)
 - i10Pi [115](#)
 - Installieren von Informatica-Clients im Grafikmodus [314](#)
 - Installieren von Informatica-Diensten im Grafikmodus [175](#)
 - Patchanforderungen [42](#)
 - vor der Installation [115](#)

Z

- Zieldatenbanken
 - durch ODBC (UNIX) Verbindung herstellen [357](#)