Informatica®
10.5.3

Installation für Data Engineering

Informatica Installation für Data Engineering
10.5.3
November 2022

Publikationsdatum: 2022-12-21

Inhalt

Einleitung

Folgen Sie den Anweisungen in *Installation für Data Engineering*, um die Data Engineering-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 sich telefonisch oder über das Informatica-Netzwerk an ein Global Support-Center wenden.

Die Telefonnummer des globalen Kundensupports von Informatica vor Ort finden Sie auf der Informatica-Website unter folgender Verknüpfung:
https://www.informatica.com/services-and-training/customer-success-services/contact-us.html.

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

Teil I: Erste Schritte der Installation

KAPITEL 1

Erste Schritte der Installation

Dieses Kapitel umfasst die folgenden Themen:

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 Repositorys, 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.

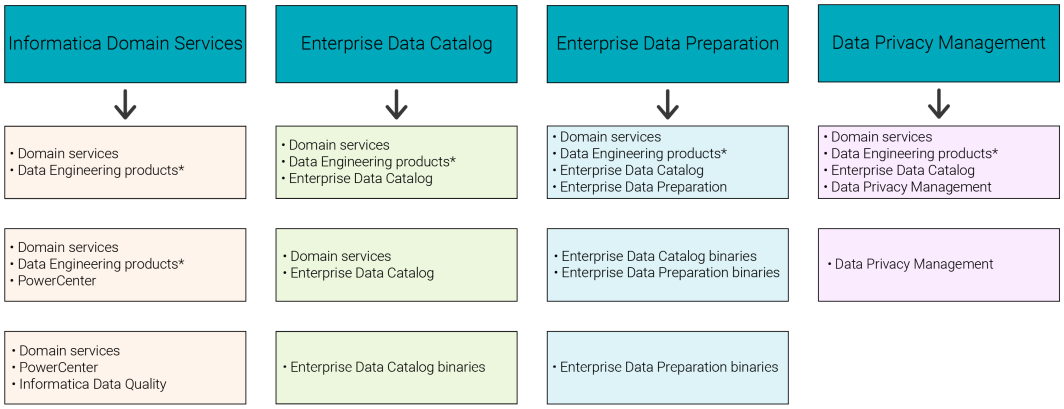
1. Überprüfen Sie die Anforderungen für Installation und Drittanbietersoftware für die Clients.
2. Verwenden Sie das Client-Installationsprogramm zum Installieren auf Windows-Computern.
3. Konfigurieren Sie erforderlichen Umgebungsvariablen und installieren Sie optional weitere Sprachen.

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.

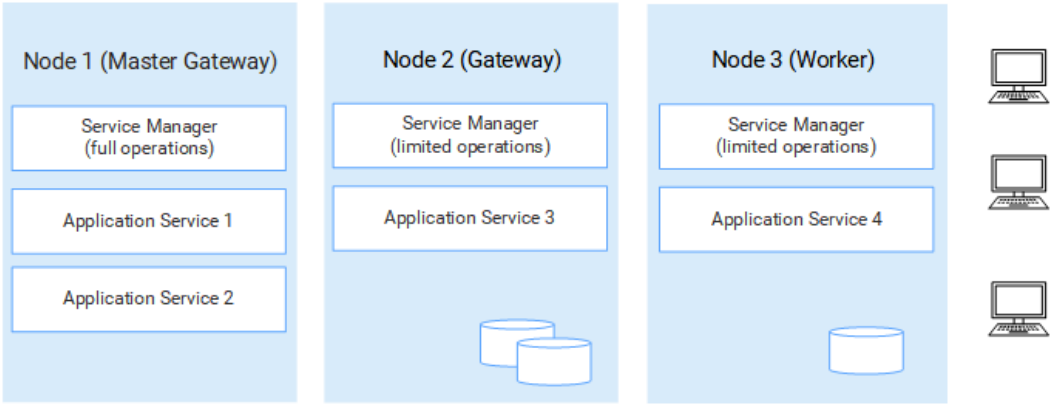
Wählen Sie bei der Installation von Data Privacy Management eine der folgenden Optionen aus:

- 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 Referenztabellenobjekte, 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.

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-Schlüsselverteilungscenter (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 Repositorys in der Domäne verwenden.

Die folgende Tabelle beschreibt die Client-Tools für Data Engineering-Produkte:

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.
Informatica Mass Ingestion (das Mass Ingestion Tool)	Eine Webanwendung zum Erstellen, Bereitstellen, Ausführen und Überwachen von Massenerfassungsspezifikationen.

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

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:

KAPITEL 2

Vor der Installation von Diensten unter UNIX oder Linux

Dieses Kapitel umfasst die folgenden Themen:

Before You Begin Checklist

This chapter contains preliminary tasks that you must complete. Use this checklist to track preliminary tasks before you prepare for services.

❑ Read the Informatica Release Notes for updates to the installation and upgrade process.

❑ Verify system requirements:

- Verify the distribution in the non-native environment.
- Verify sizing requirements based upon your processing and concurrency requirements.
- Review the patch requirements to verify that the machine has the required operating system patches and libraries.
- Verify that the port numbers to use for application service processes are available on the machines where you install the Informatica services.
- Review the distribution requirements to integrate the Informatica domain with the Hadoop or Databricks environment.
- Verify that the operating system meets the file descriptor limit.

- ❑ Back up the Data Transformation files that were created in a previous installation.
- ❑ Review system environment variables.
- ❑ Create a system user account to run the installer.
- ❑ Set up keystore and truststore files if you want to configure secure communication for the domain and set up a secure connection to web client applications.
- ❑ Extract the installer files:
  - Verify installer code signing.
  - Verify installer package integrity with checksum.
- ❑ Verify the license key.

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 Größenanforderungen

Weisen Sie Ressourcen zur Installation und Bereitstellung von Diensten auf Grundlage des erwarteten Bereitstellungstyps Ihrer Umgebung zu.

Bevor Sie Ressourcen zuweisen, müssen Sie den Bereitstellungstyp je nach Anforderungen an das Verarbeitungsvolumen und den Parallelverarbeitungsgrad identifizieren. Je nach Bereitstellungstyp können Sie Ressourcen für Speicherplatz, Kerne und Arbeitsspeicher zuweisen. Sie können auch festlegen, dass Dienste beim Ausführen des Installationsprogramms optimiert werden sollen.

Ermitteln des Installations- und Dienstbereitstellungstyps

In der folgenden Tabelle wird die Umgebung für die verschiedenen Bereitstellungstypen beschrieben:

Bereitstellungstyp	Umgebungsbeschreibung
Sandbox	Wird für Proof of Concept oder als Sandbox mit minimaler Benutzerzahl verwendet.
Basis	Wird zur Verarbeitung geringer Datenmengen bei geringer Parallelverarbeitung verwendet.
Standard	Wird zur Verarbeitung hoher Datenmengen bei geringer Parallelverarbeitung verwendet.
Erweitert	Wird zur Verarbeitung hoher Datenmengen bei starker Parallelverarbeitung verwendet.

Ermitteln der Größenanforderungen

In der folgenden Tabelle finden Sie die Mindestgrößenanforderungen für PowerCenter- oder Data Engineering-Produkte:

Bereitstellungstyp	Speicherplatz pro Knoten	Virtuelle Kerne insgesamt	RAM pro Knoten
Sandbox	50 GB	16	32 GB
Basis	100 GB	24	64 GB
Standard	100 GB	48	64 GB
Erweitert	100 GB	96	128 GB

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

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

Die folgende Tabelle listet die Mindestsystemanforderungen für einen Knoten basierend auf einigen allgemeinen Konfigurationsszenarien auf:

Dienste	Prozessor	Speicherkapazität	Festplattenspeicher
Ein Knoten führt die folgenden Dienste aus: - 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: - 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: - Analyst-Dienst	1 CPU mit mehreren Cores	4 GB	n/v
Ein Knoten führt den folgenden Dienst aus: - Suchdienst	1 CPU mit mehreren Cores	4 GB	10 GB

Dienste	Prozessor	Speicherkapazität	Festplattenspeicher
Ein Knoten führt die folgenden Dienste aus: - Analyst-Dienst - Suchdienst	1 CPU mit mehreren Cores	4 GB	10 GB
Ein Knoten führt die folgenden Dienste aus: - Metadata Manager-Dienst - PowerCenter-Integrationsdienst - PowerCenter-Repository-Dienst	2 CPUs mit mehreren Cores	8 GB	10 GB
Ein Knoten führt die folgenden Dienste aus: - Metadata Manager-Dienst - PowerCenter-Integrationsdienst - PowerCenter-Repository-Dienst	2 CPUs mit mehreren Cores	8 GB	10 GB
Ein Knoten führt die folgenden Dienste aus: - PowerCenter-Integrationsdienst - PowerCenter-Repository-Dienst	1 CPU mit mehreren Cores	4 GB	10 GB
Ein Knoten führt die folgenden Dienste aus: - Datenintegrationsdienst - Modellrepository-Dienst	1 CPU mit mehreren Cores	4 GB	10 GB
Ein Knoten führt die folgenden Dienste aus: - Datenintegrationsdienst - Content-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 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

Die Größenanforderungen berücksichtigen folgende Faktoren:

- Erforderlicher Speicherplatz zum Extrahieren des Installationsprogramms
- Temporärer Speicherplatz zur Ausführung des Installationsprogramms
- Erforderlicher Speicherplatz für die Installation der Dienste und Komponenten
- Erforderlicher Speicherplatz für Protokollverzeichnisse
- Anforderungen zum Ausführen der Anwendungsdienst

Die Größenangaben berücksichtigen nicht die Anforderungen an die operative Datenverarbeitung und die Zwischenspeicherung von Objekten für den nativen Ausführungsmodus.

Hinweis: Wählen Sie für Cloud-Bereitstellungen Computer mit einer Konfiguration aus, die den Größenanforderungen am ehesten entspricht.

Optimierung während der Installation

Wenn Sie das Installationsprogramm ausführen, können Sie festlegen, dass die Dienste je nach Bereitstellungsgröße optimiert werden sollen. Wenn Sie während der Installation einen Modellrepository-Dienst, einen Datenintegrationsdienst oder einen Content-Management-Dienst erstellen, kann das Installationsprogramm die Dienste abhängig vom von Ihnen eingegebenen Bereitstellungstyp optimieren. Das Installationsprogramm konfiguriert Eigenschaften wie die maximale Heap-Größe und die Größe des Ausführungspools.

Mit dem Befehl infacmd autotune können Sie die Optimierung der Dienste jederzeit nach der Installation der Dienste durchführen. Wenn Sie den Befehl ausführen, können Sie die Eigenschaften für andere Dienste und die Eigenschaften der Hadoop-Laufzeit-Engine optimieren.

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.

Data Engineering unter Linux

The following table lists the patches and libraries that the Informatica services require on Linux:

Platform	Operating System	Operating System Patch
AWS Linux	Linux 2 - 2.0.20220805.0	All of the following packages: - e2fsprogs-libs-1.42.9-12.amzn2.0.2.x86_64 - keyutils-libs-1.5.8-3.amzn2.0.2.x86_64 - libselinux-2.5-12.amzn2.0.2.x86_64 - libsepol-2.5-8.1.amzn2.0.2.x86_64
Ubuntu	20.04.1	All of the following packages: - e2fsprogs/focal,now 1.45.5-2ubuntu1 amd64 [installed] - libkeyutils1/focal,now 1.6-6ubuntu1 amd64 [installed,automatic] - libselinux1/focal,now 3.0-1build2 amd64 [installed,automatic] - libsepol1/focal,now 3.0-1 amd64 [installed,automatic]
Ubuntu	18.04	All of the following packages: - e2fsprogs/focal,now 1.45.5-2ubuntu1 amd64 [installed] - libkeyutils1/focal,now 1.5.9-9.2ubuntu2 amd64 [installed,automatic] - libselinux1/focal,now 2.7-2build2 amd64 [installed,automatic] - libsepol1/focal,now 2.7-1ubuntu0.1 amd64 [installed,automatic]
Linux-x64	Red Hat Enterprise Linux 6.7	All of the following packages, where <version> is any version of the package: - e2fsprogs-libs-<version>.el6 - keyutils-libs-<version>.el6 - libselinux-<version>.el6 - libsepol-<version>.el6
Linux-x64	Red Hat Enterprise Linux 7.3	All of the following packages, where <version> is any version of the package: - e2fsprogs-libs-<version>.el7 - keyutils-libs-<version>.el7 - libselinux-<version>.el7 - libsepol-<version>.el7

Platform	Operating System	Operating System Patch
Linux-x64	Red Hat Enterprise Linux 8	All of the following packages, where <version> is any version of the package: - e2fsprogs-libs-<version>.el8 - keyutils-libs-<version>.el8 - libselinux-<version>.el8 - libsepol-<version>.el8
Linux-x64	SUSE Linux Enterprise Server 12	Service Pack 2
Linux-x64	SUSE Linux Enterprise Server 15	Service Pack 0 and Service Pack 1.

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-Datendiensts. Standardwert ist 6006.
Schließungsport des Dienstmanagers	Portnummer, die das Herunterfahren des Servers für den Dienstmanager der Domäne steuert. An diesem Port wartet der Dienstmanager auf Ausschaltbefehle. Standardwert ist 6007.
Informatica Administrator-Port	Portnummer von Informatica Administrator. Standardwert ist 6008.
Informatica Administrator-Schließungsport	Portnummer, die das Herunterfahren des Servers für Informatica Administrator steuert. Informatica Administrator überwacht Befehle zum Herunterfahren auf diesem Port. Standardwert ist 6009.
Niedrigste Portnummer	Niedrigste Portnummer des dynamischen Portnummernbereichs, die den Anwendungsdienstprozessen, die auf diesem Knoten laufen, zugewiesen werden kann. Standardwert ist 6014.

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: - 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.

Verify Distribution Package Requirements (Linux and UNIX)

You can use third-party distribution packages to integrate the Informatica domain with the Hadoop or Databricks environment.

The Informatica domain and client require the distribution packages to process complex files within the Informatica domain, or to connect to Hadoop or Databricks environment when you process within the Informatica domain, or to push processing to Hadoop or Databricks environment.

If you need a distribution package, you can install it through the installer or through Integration Package Manager (the package manager) at any time.

Process within the Informatica domain

You can use the Cloudera CDP Private Cloud distribution package to process complex files within the Informatica domain or to connect to the Hadoop or Databricks environment when you process within the Informatica domain. However, you can use a different distribution package according to your requirements.

The following adapters require distribution packages for processing within the Informatica domain:

- 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

Process with Hadoop or Databricks environment

When you push processing to the Hadoop or Databricks environment, the Informatica domain and client require distribution packages. For more information about the supported distribution packages, see the Product Availability Matrix.

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.

Data Transformation-Dateien sichern

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

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

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

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

Überprüfen der Umgebungsvariablen

Konfigurieren Sie Umgebungsvariablen für die Informatica-Installation.

In der folgenden Tabelle werden die zu überprüfenden Umgebungsvariablen beschrieben:

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

Hinweis: Stellen Sie sicher, dass das Flag NOEXEC nicht für das Dateisystem festgelegt ist, das auf dem Verzeichnis /tmp gemountet ist.

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.

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

Sie haben ein signiertes SSL-Zertifikat.

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

Sie haben das Zertifikat in Schlüsselspeicher importiert.

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

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.

Wichtig: Importieren Sie die Zertifikatsdateien einmalig und kopieren Sie sie dann auf alle Computer, auf denen sich der Datenintegrationsdienst und der Metadaten-Zugriffsdienst befinden. Wenn der Datenintegrationsdienst in einem Gitter ausgeführt wird, schlagen Mappings, die Sie in die Hadoop-Umgebung übertragen, möglicherweise aufgrund inkonsistenter binärer Hex-Werte mit Initialisierungsfehlern fehl.

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.

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

Sie haben ein signiertes SSL-Zertifikat.

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

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

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

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

Der Schlüsselspeicher befindet sich im richtigen Verzeichnis.

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

Download and Extract the Installer Files

The installer files are distributed as compressed files. You can get the Informatica installation file and distribution packages from the FTP link contained in your fulfillment email.

Download the Informatica installation tar file and the required distribution package ZIP files from the Informatica Electronic Software Download site. You can download them to a local directory or a shared network drive that is mapped on your machine.

Extract the Informatica installer files to a directory on your machine. The user that runs the installer must have read and write permissions on the installer files directory and execute permissions on the executable file.

Hinweis: Ensure that you extract the installer files to a local directory as you can't run the installer from a mapped file.

Copy the ZIP files of the distribution packages to the following location: `<Informatica installer files>/source`

Hinweis: The installer fails if the ZIP files for distribution packages aren't available in the source directory.

Verify Installer Code Signing

You can verify the signature of the Informatica software code.

Informatica uses a certificate based digital signature to sign the Informatica software code. The code signing helps to validate the authenticity of the code and ensures that there has been no changes or corruptions to the code after Informatica signs the code. You can determine whether to trust the software based on whether the code sign is present or not.

You can request a code signing certificate that contains information that fully identifies Informatica LLC and a Certificate Authority (CA) that issues the certificate. The digital certificate binds the identity of Informatica to a public key and to a private key.

Digital signing of software begins with the creation of a cryptographic hash, or a digest. The digest has a one to one correspondence with the original data. Use the digest as there are no hints on how to recreate the original data, and even a small change in the original data results in a change in the hash value. Informatica uses its private key to sign the digest, or generates a signature in the form of a string of bits. Good digital signature algorithms allow a user with the public key to verify the creator of the signature.

To Verify the Signed Code is Authentic

After Informatica signs the software bundle, you can contact Informatica Global Customer Support to access the code signing certificate. Informatica ships the installer along with the signature file that contains the hash of the installer binary encrypted with Informatica's private key. You can validate the integrity of digitally signed binaries using any available tools, such as OpenSSL.

For instance, if you have to verify the package authentication and confirm the code security, enter the following OpenSSL commands:

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

Where `<signature>` is the file containing the signature in Base64, `<cert>` is the code signing certificate, and `<file>` is the file to verify.

Based on verification process, OpenSSL displays a success or error message to validate if the installer code is genuine or not. Note that the verification for the installer might take around two minutes.

Verify Installer Package Checksum on UNIX and Linux

Before you run the services installer, verify the install package integrity through the cksum command. The cksum command calculates the checksum value for the installers.

Verify the checksum for the specific installer files against the checksum of the installation files downloaded from the Informatica Electronic Software Download site.

The following table lists the checksum and file size for the Informatica services installer for UNIX and Linux:

Datei	Prüfsummenwert	Dateigröße
informatica_1053_server_linux-x64.tar	2154528627	11639828480

A checksum mismatch can occur when there are data errors during download due to network issues or when data corruption occurs in the file on disk. For more information about the checksum errors, see 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.

Vorbereiten auf den Clusterimport

Bei Ausführung des Installationsprogramms können Sie den Cluster konfigurieren. Mithilfe der Clusterkonfiguration kann der Datenintegrationsdienst Zuordnungslogik an den Cluster übertragen. Um die Informatica-Domäne mit dem nicht nativen Cluster zu integrieren, müssen Sie eine Clusterkonfiguration importieren. Sie können die Cluster-Informationen direkt aus dem Cluster oder aus einer Archivdatei importieren.

Sie können Cluster-Informationen aus einer Archivdatei jedes unterstützten Clusters in die Domäne importieren. Ihr Administrator stellt Ihnen möglicherweise vorzugsweise eine Archivdatei bereit, um vertrauliche Verbindungsinformationen zum Cluster zu schützen. Die Archivdatei kann das ZIP- oder TAR-Format aufweisen. Vergewissern Sie sich, dass Sie die Archivdatei lokal speichern.

Vorbereiten der Archivdatei für die Hadoop-Umgebung

Um die Clusterkonfiguration aus dem Amazon EMR-, MapR- oder Google Dataproc-Cluster zu importieren, müssen Sie sie aus einer Archivdatei importieren. Die Archivdatei mit der Hadoop-Clusterkonfiguration kann je nach Distribution folgenden Inhalt haben:

- core-site.xml
- hbase-site.xml. „hbase-site.xml“ ist nur erforderlich, wenn Sie auf HBase-Quellen und -Ziele zugreifen.
- hdfs-site.xml
- hive-site.xml
- mapred-site.xml oder tez-site.xml. Schließen Sie die Datei „mapred-site.xml“ oder die Datei „tez-site.xml“ in Abhängigkeit von dem im Hadoop-Cluster verwendeten Hive-Ausführungstyp ein.
- yarn-site.xml

Hinweis: Wenn Sie einen CDP Public Cloud-Cluster konfigurieren, befindet sich die Datei „hbase-site.xml“ im Data Lake-Cluster. Die anderen Dateien befinden sich im Data Hub-Cluster.

Vorbereiten der Archivdatei für die Databricks-Umgebung

Um die XML-Datei für den Import zu erstellen, müssen Sie die erforderlichen Informationen beim Databricks-Administrator anfordern. Sie können einen beliebigen Namen für die Datei angeben und sie lokal speichern.

In der folgenden Tabelle werden die Clustereigenschaften beschrieben, die in der Importdatei für die Databricks-Umgebung konfiguriert werden müssen:

Eigenschaftsname	Beschreibung
cluster_name	Name des Databricks-Clusters.
cluster_ID	Die Cluster-ID des Databricks-Clusters.
Basis-URL	Die URL für den Zugriff auf den Databricks-Cluster.
accesstoken	Innerhalb von Databricks erstellte Token-ID, die für die Authentifizierung erforderlich ist.

Optional können Sie andere Eigenschaften einschließen, die für die Databricks-Umgebung spezifisch sind. Wenn Sie die XML-Datei fertig gestellt haben, komprimieren Sie sie als ZIP- oder TAR-Datei für den Import.

KAPITEL 3

Vorbereiten von Anwendungsdiensten und Datenbanken

Dieses Kapitel umfasst die folgenden Themen:

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 Repositorys 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 Repositorys 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.

In der folgenden Tabelle sind die Anwendungsdienste aufgeführt, die von den einzelnen Produkten verwendet werden:

Produkt	**Anwendungsdienste**
Data Engineering Integration	- Analyst-Dienst - Datenintegrationsdienst * - Massenerfassungsdienst - Metadaten-Zugriffsdienst * - Modellrepository-Dienst *
Data Engineering Quality	- Analyst-Dienst - Content-Management-Dienst * - Datenintegrationsdienst * - Massenerfassungsdienst - Metadaten-Zugriffsdienst * - Modellrepository-Dienst * - Suchdienst
Data Engineering Streaming	- Analyst-Dienst - Datenintegrationsdienst * - Massenerfassungsdienst - Metadaten-Zugriffsdienst * - Modellrepository-Dienst *
** Diese Dienste können Sie bei der Installation des Produkts erstellen.*	

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

Produkt	Anwendungsdienste
PowerCenter	- 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	- Analyst-Dienst - Content-Management-Dienst * - Datenintegrationsdienst * - Metadata Manager-Dienst - Modellrepository-Dienst * - Überwachungsmodellrepository-Dienst * - PowerCenter-Integrationsdienst * - PowerCenter-Repository-Dienst * - Suchdienst
** Diese Dienste können Sie bei der Installation des Produkts erstellen.* *Beachten Sie, dass Dienste je nach Ihrer Produktedition variieren können.*	

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

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

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:

- 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 des Repository 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 die empfohlenen Werte für die Konfigurationsparameter aufgeführt, die Sie einstellen müssen:

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 Datenbanksperrfunktion als Sperrung auf Zeilenebene.
  In der folgenden Tabelle wird beschrieben, wie Sie die Datenbanksperrfunktion 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: - 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: - Datenintegrationsdienst - Modellrepository-Dienst

Abhängigkeit	Zusammenfassung
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 Referenztabellen verwenden. Er nutzt den Datenintegrationsdienst zum Ausführen von Mappings, die Daten zwischen Referenztabellen 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: - 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: - Modellrepository-Dienst - Datenintegrationsdienst
Datenbanken	Der Content-Management-Dienst verwendet die folgende Datenbank: - Referenzdaten-Warehouse. Speichert die Datenwerte für die Referenztabellenobjekte, die Sie im Modellrepository definieren. Beim Hinzufügen von Daten zu einer Referenztabelle schreibt der Content-Management-Dienst die Datenwerte in eine Tabelle im Referenzdaten-Warehouse.
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 Referenztabellenobjekte, die Sie in einem Modellrepository definieren. Konfigurieren Sie einen Content Management Service, um das Referenzdaten-Warehouse und das Modellrepository zu identifizieren.

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

Das Referenzdaten-Warehouse unterstützt die folgenden Datenbanktypen:

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL-Datenbank
- Oracle
- 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.DBTABAUTH verfügt.
- Informatica bietet keine Unterstützung für IBM DB2-Tabellenaliase für Repository-Tabellen. Stellen Sie sicher, dass für keine Tabellen in der Datenbank Tabellenaliase erstellt wurden.
- Setzen Sie den Tablespace-Parameter pageSize auf 32768 Byte.
- Legen Sie den NPAGES-Parameter auf mindestens 5000 fest. Der NPAGES-Parameter bestimmt die Anzahl der Seiten im Tabellenbereich.

Microsoft 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 des Repository 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: - 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: - Modellrepository-Dienst
Datenbanken	Der Datenintegrationsdienst verwendet die folgenden Datenbanken: - 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-Tabellenaliase für Repository-Tabellen. Stellen Sie sicher, dass für keine Tabellen in der Datenbank Tabellenaliase erstellt wurden.
- Setzen Sie den Tablespace-Parameter pageSize auf 32768 Byte.
- Legen Sie den NPAGES-Parameter auf mindestens 5000 fest. Der NPAGES-Parameter bestimmt die Anzahl der Seiten im Tabellenbereich.

Microsoft SQL Server-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository 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.

Anforderungen an das Profiling-Warehouse

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

Das Profiling-Warehouse unterstützt die folgenden Datenbanktypen:

- IBM DB2 UDB
- Microsoft SQL Server
- Oracle

Zulassen von 10 GB Speicherplatz für die Datenbank.

Hinweis: Stellen Sie sicher, dass Sie den Datenbank-Client auf dem Computer installieren, auf dem Sie den Datenintegrationsdienst ausführen möchten. Sie können eine JDBC-Verbindung 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-Tabellenaliase für Repository-Tabellen. Stellen Sie sicher, dass für keine Tabellen in der Datenbank Tabellenaliase erstellt wurden.
- Setzen Sie den Tablespace-Parameter pageSize auf 32768 Byte.
- Legen Sie den NPAGES-Parameter auf mindestens 5000 fest. Der NPAGES-Parameter bestimmt die Anzahl der Seiten im Tabellenbereich.

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

Microsoft SQL Server-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository 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
Prozesse	1000

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-Tabellenaliase für Repository-Tabellen. Stellen Sie sicher, dass für keine Tabellen in der Datenbank Tabellenaliase erstellt wurden.
- Setzen Sie den Tablespace-Parameter pageSize auf 32768 Byte.
- Legen Sie den NPAGES-Parameter auf mindestens 5000 fest. Der NPAGES-Parameter bestimmt die Anzahl der Seiten im Tabellenbereich.
- Legen Sie die Verbindungspooling-Parameter fest.

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

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

Microsoft 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 des Repository 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 die empfohlenen Werte für die Konfigurationsparameter aufgeführt, die Sie einstellen müssen:

Parameter	Mindestwert	Empfohlener Wert
max_connections	200	4000
shared_buffers	2 GB	16 GB

Parameter	Mindestwert	Empfohlener Wert
max_locks_per_transaction	1024	1024
max_wal_size	1 GB	8 GB
checkpoint_timeout	5 Minuten	30 Minuten

Massenerfassungsdienst

Der Massenerfassungsdienst verwaltet und validiert Massenerfassungsspezifikationen, die Daten in Zielen in einer nicht nativen Umgebung aufnehmen. 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 Massenerfassungsdienst zugeordnet sind:

Abhängigkeit	Zusammenfassung
Produkte	Die folgenden Produkte verwenden den Massenerfassungsdienst: - Data Engineering Integration - Data Engineering Quality - Data Engineering Streaming
Dienste	Der Massenerfassungsdienst muss den folgenden Diensten direkt zugeordnet werden: - Modellrepository-Dienst
Datenbanken	Der Massenerfassungsdienst ist keinen Datenbanken zugeordnet.
Installationsprogramm	Sie können den Massenerfassungsdienst nicht bei Ausführung des Installationsprogramms erstellen.

Metadaten-Zugriffsdienst

Der Metadaten-Zugriffsdienst ist ein Anwendungsdienst, mit dem das Developer Tool auf die Hadoop-Umgebung zugreifen kann, um Metadaten zu importieren und in der Vorschau anzuzeigen. Wenn die Domäne eine Nicht-Kerberos-Authentifizierung verwendet, können Sie den Metadaten-Zugriffsdienst erstellen und

konfigurieren. Wenn die Domäne die Kerberos-Authentifizierung verwendet, erstellen Sie den Metadaten-Zugriffsdienst nicht.

In der folgenden Tabelle werden die Abhängigkeiten für Produkte, Dienste und Datenbanken, die mit dem Metadaten-Zugriffsdienst verknüpft sind, sowie die Einschränkungen des Installationsprogramms zusammengefasst:

Abhängigkeit	Zusammenfassung
Produkte	Die folgenden Produkte verwenden den Metadaten-Zugriffsdienst: - Data Engineering Integration - Data Engineering Quality - Data Engineering Streaming - Enterprise Data Catalog - Enterprise Data Preparation
Dienste	Der Metadaten-Zugriffsdienst erfordert keine Zuordnung zu einem anderen Anwendungsdienst.
Datenbanken	Dem Metadaten-Zugriffsdienst ist keine Datenbank zugeordnet.
Installationsprogramm	Sie können den Metadaten-Zugriffsdienst bei Ausführung des Installationsprogramms erstellen.

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: - 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.
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

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

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

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 des Repository 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 die empfohlenen Werte für die Konfigurationsparameter aufgeführt, die Sie einstellen müssen:

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: - 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.

Abhängigkeit	Zusammenfassung
Datenbanken	Der Überwachungsmodellrepository-Dienst verwendet die folgende Datenbank: - 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: - PowerCenter - Informatica Data Quality - Test Data Management
Dienste	Der PowerCenter-Integrationsdienst muss dem folgenden Dienst direkt zugeordnet werden: - 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: - 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: - 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 10.5.3-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 PowerCenter Client und PowerCenter-Integrationsdienst schneller auf das Repository zu, als wenn sich die Repository-Tabellen auf unterschiedlichen Datenbankknoten befinden.

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

Microsoft SQL Server-Datenbankanforderungen

Beachten Sie beim Einrichten des Repository 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.

Microsoft Azure SQL-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 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.
  Die folgenden Vorgänge im PowerCenter-Repository-Dienst sind stabil gegenüber dem Datenbank-Failover beim Oracle RAC-Setup:
  - ExecuteQuery
  - ObjectExport
  - ObjectImport
  - PurgeVersion
  - RollbackDeployment

PostgreSQL Database Requirements

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

- Stellen Sie sicher, dass das Datenbankbenutzerkonto über die Berechtigungen CREATE TABLE und CREATE VIEW verfügt.
- 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 die empfohlenen Werte für die Konfigurationsparameter aufgeführt, die Sie einstellen müssen:

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

- To configure PostgreSQL database for the PowerCenter repository, set values for the PostgreSQL database host, port, and service name for the pg_service.conf file in the following format:

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

Ensure that the entries for the [PCRS_DB_SERVICE_NAME] entry matches the information for the PowerCenter Repository Service. To securely connect to PostgreSQL for the PowerCenter repository, set the security property along with the remaining required database properties in the pg_service.conf file in the following format: `sslmode=require`

- Set the PGSERVICEFILE environment variable to the location of the pg_service.conf file. The pg_service.conf file contains the connection parameters for PostgreSQL database connection in the Informatica installation directory. For example, set the variable as follows:
  Using a Bourne shell:

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

  Using a 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: - 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: - Modellrepository-Dienst
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.

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

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

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

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

Installieren der Datenbank-Clientsoftware

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

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

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

IBM DB2 Client Application Enabler (CAE)

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

Microsoft SQL Server 2014 Native Client

Laden Sie den Client von der folgenden Microsoft-Website herunter: http://www.microsoft.com/en-in/download/details.aspx?id=42295.

Oracle-Client

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

Sybase Open Client (OCS)

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

Konfigurieren von 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`

Umgebungsvariable	Wert
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}*

Umgebungsvariable	Wert
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 Repositorys 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*
LD_LIBRARY_PATH	*$ODBCHOME/lib*
INFA_TRUSTSTORE	*USER_INSTALL_DIR/server/bin:$LD_LIBRARY_PATH* 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 4

Vorbereiten der Kerberos-Authentifizierung

Dieses Kapitel umfasst die folgenden Themen:

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.

4. 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
   ```

5. Speichern Sie die Datei krb5.conf.
6. Speichern Sie die Datei krb5.conf in einem Verzeichnis, das auf dem Rechner zugänglich ist, wenn Sie 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 *localhost*. Der Hostname muss den Computer eindeutig kennzeichnen.
Dienstbereichsname	Name des Kerberos-Bereichs für die Informatica-Domänendienste. Der Bereichsname muss aus Großbuchstaben bestehen.

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

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

   Zum Generieren der SPN-Formate für mehrere Knoten geben Sie „1“ in jeder Eingabeaufforderung **Knoten hinzufügen?** ein, und geben Sie einen Knotennamen und Hostnamen des Knotens ein.

7. Geben Sie in der Eingabeaufforderung **Dienst hinzufügen?** „1“ zum Generieren des SPN-Formats für einen Dienst ein, der auf dem vorigen Knoten ausgeführt wird. Geben Sie dann den Dienstnamen ein.

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

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

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

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

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

Überprüfen der SPN- und Keytab-Format-Textdatei

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

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

Die Textdatei enthält die folgenden Informationen:

Entitätsname

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

SPN

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

Ein SPN kann eines der folgenden Formate aufweisen:

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

Keytab-Dateiname

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

Die Keytab-Dateinamen verwenden die folgenden Formate:

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

Schlüsseltabellentyp

Der Typ der Schlüsseltabelle. Folgende Schlüsseltabellentypen sind möglich:

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

Dienstprinzipale auf der Knotenebene

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

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

Dienstprinzipale auf der Prozessebene

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

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

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

Erstellen der Dienstprinzipalnamen und Keytab-Dateien

Senden Sie nach dem Generieren der Liste der 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 Prinicipal Name) muss identisch sein mit dem SPN.

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

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

Aktivieren Sie die Delegierung in Microsoft Active Directory.

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

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

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-Schlüsselverteilungscenters (KDC) ermitteln.

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

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

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

klist

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

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

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

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

kinit

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

```
kinit <user_account>
```

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

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

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

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

setspn

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

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

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

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

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

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

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

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

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

Existing SPN found!
```

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

```
setspn -X
```

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

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

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

kdestroy

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

KAPITEL 5

Aufzeichnen von Informationen für Abfragen des Installationsprogramms

Dieses Kapitel umfasst die folgenden Themen:

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.

Record Information for Installer Prompts Overview

When you install the Informatica services, you need to know information about the domain, nodes, application services, databases, and distribution packages for the environment.

This section lists information that you need to provide when you run the installer. Informatica recommends recording installer prompts before you start the installation process. For example, you might want to create a text file of information so you can copy into the installer.

Domain Object Naming Conventions

You cannot change domain, node, and application service names. Use names that continue to work if you migrate a node to another machine or if you add additional nodes and services to the domain. In addition, use names that convey how the domain object is used. Naming conventions are provided in applicable topics.

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
Domänenname	Der Name der Domäne, die Sie erstellen möchten. Der Name darf maximal 128 Zeichen umfassen und muss im 7-Bit-ASCII-Format vorliegen. Er darf weder Leerzeichen noch die folgenden Zeichen enthalten: ` % * + ; " ? , < > \ / 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	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. 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. **Hinweis:** Verwenden Sie nicht localhost. Der Hostname muss den Computer eindeutig kennzeichnen.
Knotenname	Name der Knoten, die Sie auf diesem Computer erstellen möchten. Der Knotenname ist nicht mit dem Hostnamen des Computers identisch. Ziehen Sie die folgende Benennungskonvention in Betracht: Knoten<Knoten-Nr.>_<ORG>_<optionale Unterscheidung>_<ENV>

Distribution Packages

If you are going to install a distribution package through the installer, record the distribution package that you downloaded.

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 Knotennemen 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 Domänen-Konfigurations-Repository. Das Domänenkonfigurations-Repository unterstützt IBM DB2 UDB, Microsoft SQL Server, Oracle, PostgreSQL oder Sybase ASE.
Hostname der Domänen-Konfigurationsdatenbank	Der Name des Computers, der die Datenbank hostet.

Content-Management-Dienst

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.
Datenbank-Hostname des Referenzdaten-Warehouse	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 oder Oracle.
Hostname der Profiling-Warehouse-Datenbank	Der Name des Computers, der die Datenbank hostet.
Arbeitsablauf-Datenbanktyp	Datenbanktyp für die Arbeitsablauf-Datenbank. Die Arbeitsablauf-Datenbank unterstützt IBM DB2 UDB, Microsoft 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.

The following table describes the security parameters that you must include in the JDBC connection string:

Parameter	Description
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 is sent by the database server. If this parameter is set to True, Informatica validates the certificate that is sent by the database server. If you specify the HostNameInCertificate parameter, Informatica also validates the host name in the certificate. If this parameter is set to false, Informatica doesn't validate the certificate that is sent by the database server. Informatica ignores any truststore information that you specify.
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. If SSL encryption and validation is enabled and this property is not specified, the driver uses the server name specified in the connection URL or data source of the connection to validate the 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 can use the following syntax in the JDBC connection string to connect to a secure database:

IBM DB2

```
jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=<database
name>;EncryptionMethod=SSL;HostNameInCertificate=<database host
name>;ValidateServerCertificate=<true or false>
```

Oracle

```
jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=<service
name>;EncryptionMethod=SSL;HostNameInCertificate=<database host
name>;ValidateServerCertificate=<true or false>
```

Use the following connection string to connect to the Oracle database through the Oracle Connection Manager:

```
jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora
file>;TNSServerName=<TNS server name>;
```

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 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.win
dows.net;ValidateServerCertificate=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 doesn't validate the connection string. Verify that the connection string contains all the connection parameters and security parameters required by your database.

Clusterkonfiguration

Sie importieren Konfigurationseigenschaften aus dem nicht nativen Cluster, um eine Clusterkonfiguration zu erstellen. Die Cluster-Konfiguration ermöglicht es dem Datenintegrationsdienst, Jobs an die nicht native Umgebung zu übertragen.

Sie können die Eigenschaften aus einer vom Hadoop-Administrator erstellten Archivdatei oder direkt aus dem Cluster importieren. Wenn Sie die Clusterkonfiguration erstellen, können Sie auch Hadoop-, Hive-, HBase-, HDFS- oder Databricks-Verbindungen erstellen, die dem Cluster zugeordnet werden. Das Installationsprogramm fügt den Verbindungstyp an den Namen der Clusterkonfiguration an, um die jeweiligen Verbindungsnamen zu erstellen.

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

Cluster-Informationen	Beschreibung
Name der Clusterkonfiguration	Name der zu erstellenden Clusterkonfiguration.
Distributionstyp	Typ der nicht nativen Clusterverteilung.
Importmethode der Clusterkonfiguration	Methode zum Importieren der Clusterkonfiguration. Sie können wählen, ob Sie die Clusterkonfiguration aus einer Archivdatei oder aus dem Cluster importieren wollen.

Importieren der Clusterkonfiguration aus einer Archivdatei

Um die Eigenschaften der Clusterkonfiguration aus einer Archivdatei zu importieren, geben Sie den Pfad der Konfigurationsarchivdatei an.

Importieren der Clusterkonfiguration vom Cluster

In der folgenden Tabelle werden die Clustereigenschaften für Cloudera, Hortonworks oder Azure HDInsight beschrieben, die Sie eingeben müssen, wenn Sie während des Installationsvorgangs vom Cluster importieren:

Eigenschaft	Beschreibung
Host	Der Hostname oder die IP-Adresse des Cluster-Managers.
Port	Der Port des Cluster-Managers.
Benutzer-ID	Benutzername des Clusters.
Passwort	Passwort für den Clusterbenutzer.
Clustername	Name des Clusters. Verwenden Sie den Anzeigenamen, wenn der Cluster-Manager mehrere Cluster verwaltet. Wenn Sie keinen Cluster-Namen angeben, importiert der Assistent Informationen basierend auf dem Standard-Cluster.
Engine-Typ	Für einen Cloudera-Cluster fordert das Installationsprogramm zur Eingabe des Engine-Typs auf. Wenn Sie einen CDP-Cluster verwenden, legen Sie Tez als Engine-Typ fest. Wenn Sie einen CDH-Cluster verwenden, legen Sie MRv2 als Engine-Typ fest.

In der folgenden Tabelle werden die Clustereigenschaften für Databricks beschrieben, die Sie während des Installationsvorgangs eingeben müssen:

Eigenschaft	Beschreibung
Databricks-Domäne	URL des Databricks-Clusters.
Databricks-Token-ID	Token-ID des Databricks-Clusters.
Databricks-Cluster ID	Cluster-ID des Databricks-Clusters.

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:

Property	Description
Encryption key directory	Directory in which to store the encryption key for the domain. By default, the encryption key is created in the following directory: `<Informatica installation directory>/isp/config/keys`.
Specify if you want to back up the site key that the installer generates or not:	Specify if you want to back up the site key that the installer generates or not: - Select **1** for No. If you choose No, the installer exits. - Select **2** for Yes. If you choose Yes, you agree to back up the file manually. 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.

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.
Speicherort der Kerberos-Konfigurationsdatei	Verzeichnis, in dem die Kerberos-Konfigurationsdatei namens *krb5.conf* gespeichert ist. Für Informatica müssen in der Konfigurationsdatei bestimmte Eigenschaften eingerichtet werden. Wenn Sie nicht über die Berechtigung zum Kopieren oder Aktualisieren der Kerberos-Konfigurationsdatei verfügen, müssen Sie unter Umständen den Kerberos-Administrator bitten, die Datei zu aktualisieren.

Sicherheitsinformationen	Beschreibung
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 6

Einführung in das Dienste-Installationsprogramm

Dieses Kapitel umfasst die folgenden Themen:

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.
      Use the following syntax in the JDBC connection string:

IBM DB2

```
jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=
```

Oracle

```
jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=
```

Use the following connection string to connect to the Oracle database through the Oracle Connection Manager:

```
jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS name>;
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=
```

Microsoft SQL Server with Windows NT credentials

If you 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.windows.net;ValidateServerCertificate=false
```

Azure SQL Database with Active Directory authentication

```
jdbc:informatica: sqlserver://<host_name>:<port_number>;database=<database_name>;encrypt=true;AuthenticationMethod=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=<seconds>
```

PostgreSQL

```
jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=
```

Azure PostgreSQL

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

Sybase

```
jdbc:Informatica:sybase://<host name>:<port number>;DatabaseName=
```

Verify that the connection string contains all the connection parameters required by your database system.

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

Eingabeaufforderung	Beschreibung
Datenbanktyp	Der Datenbanktyp für das Domänen-Konfigurations-Repository. Treffen Sie eine Auswahl aus den folgenden Datenbanktypen: - 1 – Oracle - 2 – Microsoft SQL Server - 3 – IBM DB2 - 4 – Sybase ASE - 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 88.

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.

    Each requirement is listed, along with one of the following check statuses:

    - [Pass] - The requirement meets the criteria for the Informatica installation or upgrade.
    - [Fail] - The requirement doesn't meet the criteria for the Informatica installation or upgrade. Resolve the issue before you proceed with the installation or upgrade.
    - [Information] - Verify the information and perform any additional tasks as outlined in the details.

    The results of the system check are saved to the following file: `...<Informatica installation directory>/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**.

If the Pre-Installation (i10Pi) System Check Tool finishes with failed requirements, resolve the failed requirements and run the Pre-Installation (i10Pi) System Check Tool again.

Hinweis: If the Informatica Pre-Installation (i10Pi) System Check Tool check finishes with failed requirements, you can still perform the Informatica installation or upgrade. However, Informatica highly recommends that you resolve the failed requirements before you proceed.

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`

If the Pre-Installation (i10Pi) System Check Tool finishes with failed requirements, resolve the failed requirements and run the Pre-Installation (i10Pi) System Check Tool again.

Hinweis: If the Informatica Pre-Installation (i10Pi) System Check Tool check finishes with failed requirements, you can still perform the Informatica installation or upgrade. However, Informatica highly recommends that you resolve the failed requirements before you proceed.

Teil III: Ausführen des Dienste-Installationsprogramms

Dieser Teil enthält die folgenden Kapitel:

KAPITEL 7

Installation von Informatica-Diensten im Konsolenmodus

Dieses Kapitel umfasst die folgenden Themen:

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 96.

  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 75.

  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 10.5.3 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. Choose whether you want to install distribution packages through the Informatica installer.
   - Press **1** if you don't need distribution packages or if you want to install them later.
   - Press **2** if you want to install distribution packages through the installer.

   Default is 1.
4. If you choose to install distribution packages, select one or more packages from the list that you want to install. Separate multiple packages with a comma.

   Default is 1.

Im Abschnitt **Installationsvoraussetzungen** werden die Installationsanforderungen angezeigt. Stellen Sie sicher, dass alle Voraussetzungen erfüllt sind, bevor Sie die Installation fortsetzen.

Optimieren des Bereitstellungstyps

Wenn Sie Data Engineering-Produkte oder Enterprise Data Catalog installieren, kann das Installationsprogramm die Anwendungsdienste für eine bessere Leistung optimieren, abhängig vom Bereitstellungstyp in Ihrer Umgebung. Wenn Sie die Optimierung der Dienste nicht während der Installation vornehmen, können Sie die Dienste später über infacmd optimieren.

Hinweis: Das Installationsprogramm kann PowerCenter-Dienste nicht optimieren.

1. Legen Sie fest, ob Sie die Dienste optimieren möchten.
   - Wählen Sie 1, wenn Sie die Dienste nicht optimieren möchten.
   - Wählen Sie 2, wenn Sie die Dienste optimieren möchten.

   Wenn Sie den Knoten einer vorhandenen Domäne hinzufügen, achten Sie darauf, dass der hier ausgewählte Bereitstellungstyp mit den Gateway-Knoten übereinstimmt.
2. Wählen Sie den der Informatica-Umgebung zugeordneten Bereitstellungstyp aus:

Eingabeaufforderung	Beschreibung
1. Sandbox	Wählen Sie diese Option aus, wenn die Umgebung für Proof of Concept oder als Sandbox-Umgebung mit minimaler Benutzerzahl verwendet wird. Sandbox-Umgebungen sind in der Regel mit 16 Kernen, 32 GB RAM und ca. 50 GB Speicherplatz konfiguriert.
2. Einfach	Wählen Sie diese Option aus, wenn die Umgebung zur Verarbeitung von geringen Datenmengen bei geringer Parallelverarbeitung verwendet wird. Bei einfachen Umgebungen handelt es sich in der Regel um Einrichtungen mit einem oder mehreren Knoten, die mit 24 Kernen, 64 GB RAM und rund 100 GB Festplattenspeicher konfiguriert sind.

Eingabeaufforderung	Beschreibung
3. Standard	Wählen Sie diese Option aus, wenn die Umgebung für die Verarbeitung von großen Datenmengen, jedoch bei geringer Parallelverarbeitung verwendet wird. Standardumgebungen sind in der Regel Konfigurationen mit mehreren Knoten, 64 GB RAM, mehr als 100 GB Speicherplatz pro Knoten und insgesamt 48 Kernen auf allen Knoten.
4. Erweitert	Wählen Sie diese Option aus, wenn die Umgebung für die Verarbeitung von großen Datenmengen bei hoher Parallelverarbeitung verwendet wird. Erweiterte Umgebungen sind in der Regel Konfigurationen mit mehreren Knoten, 128 GB RAM, mehr als 100 GB Speicherplatz pro Knoten und insgesamt 96 Kernen auf allen Knoten.

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 106 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.

Netzwerksicherheit - Kerberos-Authentifizierung

Nachdem Sie die Sicherheitsstufe konfiguriert haben, können Sie die Kerberos-Authentifizierung konfigurieren.

- Geben Sie im Abschnitt **Netzwerksicherheit – Kerberos-Authentifizierung** die Parameter ein, die für die Kerberos-Authentifizierung benötigt werden.

  In der folgenden Tabelle werden die Kerberos-Authentifizierungsparameter beschrieben, die eingerichtet werden müssen:

Eigenschaft	Beschreibung
Domänenname	Name der Domäne. Der Name darf maximal 128 Zeichen umfassen und muss im 7-Bit-ASCII-Format vorliegen. Der Name darf weder Leerzeichen noch folgende Zeichen enthalten: ` % * + ; " ? , < > \ /
Knotenname	Name des Informatica-Knotens

Eigenschaft	Beschreibung
Knoten-Hostname	Vollständig qualifizierter Hostname oder die IP-Adresse des Computers, auf dem der Knoten erstellt werden soll. Der Hostname des Knotens darf keine Unterstriche (_) enthalten. **Hinweis:** Verwenden Sie nicht *localhost*. Der Hostname muss den Computer eindeutig kennzeichnen.
Dienstbereichsname	Name des Kerberos-Bereichs, zu dem die Informatica-Domänendienste gehören. Der Bereichsname muss aus Großbuchstaben bestehen. Die Namen des Dienst- und Benutzerbereichs müssen übereinstimmen.
Benutzerbereichsname	Name des Kerberos-Bereichs, zu dem die Informatica-Domänenbenutzer gehören. Der Bereichsname muss aus Großbuchstaben bestehen. Die Namen des Dienst- und Benutzerbereichs müssen übereinstimmen.
Keytab-Verzeichnis	Verzeichnis, in dem alle Keytab-Dateien für die Informatica-Domäne gespeichert werden. Der Name einer Keytab-Datei in der Informatica-Domäne muss einem von Informatica festgelegten Format entsprechen.
Vollqualifizierter Pfad der Kerberos-Konfigurationsdatei	Pfad und Dateiname der Kerberos-Konfigurationsdatei. Informatica benötigt folgenden Namen für die Kerberos-Konfigurationsdatei: *krb5.conf*

Wichtig: Wenn Sie die Domäne zur Ausführung mit Kerberos-Authentifizierung konfigurieren, müssen der Domänen- und Knotenname sowie der Knoten-Hostname mit den Namen übereinstimmen, die beim Ausführen des Kerberos SPN-Formatgenerators von Informatica zum Erzeugen der SPNs und Keytab-Dateinamen angegeben wurden. Wenn Sie einen anderen Domänen-, Knoten- oder Hostnamen verwenden, erzeugen Sie den SPN und die Keytab-Dateinamen erneut und bitten Sie den Kerberos-Administrator, den neuen SPN zur Kerberos-Prinzipaldatenbank hinzuzufügen und die Keytab-Dateien zu erstellen.

Der Abschnitt **Vorinstallationsübersicht** wird angezeigt. Überprüfen Sie die Installationsinformationen.

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	Wählen Sie, ob eine vom Installationsprogramm generierte oder eine von Ihnen erstellte Schlüsselspeicherdatei verwendet werden soll. Sie können eine Schlüsselspeicherdatei mit einem selbstsignierten Zertifikat oder einem von einer Zertifizierungsbehörde signierten Zertifikat verwenden. 1 – Von Installationsprogramm generierten Schlüsselspeicher verwenden 2 – Schlüsselspeicherdatei und Passwort eingeben Wenn Sie eine vom Installationsprogramm generierte Schlüsselspeicherdatei verwenden möchten, wird eine selbstsignierte Schlüsselspeicherdatei mit dem Namen „Default.keystore“ in folgendem Speicherort erstellt: `<Informatica-Installationsverzeichnis>/tomcat/conf/`

   c. Wenn Sie den Schlüsselspeicher festlegen, geben Sie das Passwort und den Speicherort der Schlüsselspeicherdatei ein.
   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 111 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 109 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 Vertrauensstellungsnamen 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	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 infa_keystore.jks enthalten.
Schlüsselspeicherpasswort	Passwort für den Schlüsselspeicher „infa_keystore.jks“.
Verzeichnis der Truststore-Datei	Verzeichnis, das die Truststore-Dateien enthält. Das Verzeichnis muss Dateien mit der Bezeichnung "infa_truststore.jks" und "infa_truststore.pem" enthalten.
Truststore-Passwort	Passwort für die Datei infa_truststore.jks.

Der Abschnitt **Domänen-Konfigurations-Repository** wird angezeigt.

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:

Property	Description
Configure tablespace	In a single-partition database, if you select No, the installer creates the tables in the default tablespace. In a multi-partition database, you must select Yes. Select whether to specify a tablespace: 1 - No 2 - Yes
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single-partition database, enter the name of the tablespace in which to create the tables. In a multipartition database, specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

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:

Property	Description
Schema name	Name of the schema that will contain domain configuration tables. If this parameter is blank, the installer creates the tables in the default schema.

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:

Prompt	Description
Database host name	Host name for the database.
Database port number	Port number for the database.

Prompt	Description
Database service name	Service or database name: - Oracle: Enter the service name. - Microsoft SQL Server: Enter the database name. - IBM DB2: Enter the service name. - Sybase ASE: Enter the database name. - PostgreSQL: Enter the database name.
Configure JDBC Parameters	Select whether to add additional JDBC parameters to the connection string: 1 - Yes 2 - No If you select Yes, enter the parameters or press Enter to accept the default. If you select No, the installer creates the JDBC connection string without parameters.

- To enter the connection information using a custom JDBC connection string, type the connection string.
  Use the following syntax in the JDBC connection string:
  IBM DB2

  ```
  jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=
  ```

  Oracle

  ```
  jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=
  ```

  Use the following connection string to connect to the Oracle database through the Oracle Connection Manager:

  ```
  jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS name>;
  ```

  Microsoft SQL Server

  ```
  jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=
  ```

  Microsoft SQL Server with Windows NT credentials

  If you 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=*.d
atabase.windows.net;ValidateServerCertificate=false
```

Azure SQL Database with Active Directory authentication

```
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://<host name>:<port number>;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://<host name>:<port number>;DatabaseName=
```

Verify that the connection string contains all the connection parameters required by your database system.

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:

Property	Description
Database truststore file	Path and file name of the truststore file for the secure database.
Database truststore password	Password for the truststore file.
Custom JDBC Connection String	JDBC connection string to connect to the secure database, including the host name and port number and the security parameters for the database.

   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	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. Geben Sie an, ob Sie den vom Installationsprogramm generierten Site-Schlüssel sichern möchten oder nicht: - 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 94.

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.

   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	Hostname oder IP-Adresse des Computers, auf dem der Knoten erstellt werden soll. Wenn der Computer nur einen Netzwerknamen aufweist, verwenden Sie den Standardhostnamen. Wenn der Computer mehrere Netzwerknamen aufweist, können Sie den Standardhostnamen ändern und einen alternativen Netzwerknamen verwenden. **Hinweis:** Der Hostname des Knotens darf keine Unterstriche (_) enthalten. Verwenden Sie nicht localhost. Der Hostname muss den Computer eindeutig kennzeichnen.
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	Benutzername für den Domänenadministrator. Sie können diesen Benutzernamen für die Erstanmeldung bei Informatica Administrator verwenden. Beachten Sie folgende Richtlinien: - Beim Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden und er darf nicht 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.

   The following table describes the password complexity:

Property	Description
Password complexity	Select whether you want to enable password complexity. 1 - Yes 2 - No If you select Yes, the password must meet the following requirements: It must be at least eight characters long and contain at least one alphabetic character, one numeric character, and one special character.
Configure password policy	Select whether you want to configure a password policy. 1 - Yes 2 - No If you select Yes, you can configure password complexity rules. If you select No, the default Informatica password policy rules apply.
Number of special characters	The minimum number of special characters required in a password. You can use the following special characters: [! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ ] ^ _ ` { | } ~] You can enter a value between 0 and 255. Default is 1.

Property	Description
Number of alphabetic characters	The minimum number of alphabetic characters required in a password. You can enter a value between 0 and 255. Default is 1.
Number of numeric characters	The minimum number of numeric characters required in a password. You can enter a value between 0 and 255. Default is 1.
Minimum password length	The minimum number of characters required in a password. You can enter a value between 8 and 255. Default is 8.
Number of previous passwords to store	The number of consecutive previous passwords that can't be reused. You can enter a value between 0 and 12. Default is 0.
Password expiration in days	The duration of the validity of a password. If you don't want passwords to expire, set the value to 0. Default is 0.
Domain password	Password for the domain administrator. - If you don't enable password complexity, the password must be between 2 and 16 characters. - If you enable password complexity, the password must be at least eight characters long and contain at least one alphabetic character, one numeric character, and one special character. - If you configure a password policy, the password must meet the complexity rules that you set. Not available if you configure the Informatica domain to run on a network with Kerberos authentication.
Confirm password	Enter the password again to confirm. Not available if you configure the Informatica domain to run on a network with Kerberos authentication.

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	Description
Service Manager port	Port number used by the Service Manager on the node. The Service Manager listens for incoming connection requests on this port. Client applications use this port to communicate with the services in the domain. The Informatica command line programs use this port to communicate to the domain. This is also the port for the SQL data service JDBC/ODBC driver. Default is 6006.
Service Manager Shutdown port	Port number that controls server shutdown for the domain Service Manager. The Service Manager listens for shutdown commands on this port. Default is 6007.
Informatica Administrator port	Port number used by Informatica Administrator. Default is 6008.
Informatica Administrator HTTPS port	No default port. Enter the required port number when you create the service. Setting this port to 0 disables an HTTPS connection to the Administrator tool.
Informatica Administrator shutdown port	Port number that controls server shutdown for Informatica Administrator. Informatica Administrator listens for shutdown commands on this port. Default is 6009.
Minimum port number	Lowest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6014.
Maximum port number	Highest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 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. Wählen Sie aus, ob Sie die Clusterkonfiguration konfigurieren möchten.

Mithilfe der Clusterkonfiguration kann der Datenintegrationsdienst Mapping-Logik an den Cluster übertragen. Wenn Sie eine Integration mit der nicht nativen Umgebung durchführen, können Sie eine Clusterkonfiguration erstellen.
Lesen Sie nach der Installation das *Data Engineering Integration-Handbuch* durch, um die Domäne vollständig in die nicht native Umgebung zu integrieren.

6. Geben Sie an, ob Sie einen Metadaten-Zugriffsdienst erstellen möchten. Wenn die Domäne die Kerberos-Authentifizierung verwendet, erstellen Sie den Metadaten-Zugriffsdienst nicht.
7. 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:

Property	Description
Configure tablespace	In a single-partition database, if you select No, the installer creates the tables in the default tablespace. In a multi-partition database, you must select Yes. Select whether to specify a tablespace: 1 - No 2 - Yes
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single-partition database, enter the name of the tablespace in which to create the tables. In a multipartition database, specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

   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:

Property	Description
Schema name	Name of the schema that will contain domain configuration tables. If this parameter is blank, the installer creates the tables in the default schema.

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: - 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>;Snaps
  hotSerializable=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: - 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	Zur Verwendung der im Standardschlüsselspeicher und im Truststore enthaltenen SSL-Standardzertifikate von Informatica. **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	Zur Verwendung von benutzerdefinierten SSL-Zertifikaten. Sie müssen den Speicherort der Schlüsselspeicher- und Truststore-Dateien angeben. Sie können ein selbstsigniertes Zertifikat oder ein von einer Zertifizierungsstelle ausgegebenes Zertifikat verwenden. Sie müssen SSL-Zertifikate im PEM-Format und in Java-Schlüsselspeicherdateien (JKS) bereitstellen. Informatica benötigt bestimmte Namen für die SSL-Zertifikatsdateien in der Informatica-Domäne. Sie müssen für alle Knoten in der Domäne dieselben SSL-Zertifikate verwenden. Speichern Sie die Truststore- und Schlüsselspeicherdateien in einem Verzeichnis, auf das alle Knoten in der Domäne zugreifen können, und geben Sie für alle Knoten in derselben Domäne dasselbe Schlüsselspeicherdatei- und Truststore-Datei-Verzeichnis an.

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.

3. Wählen, ob Sie die Data Engineering-Wiederherstellung für Aufträge aktivieren möchten, die auf der Spark-Engine ausgeführt werden?

   Bei Auswahl von Ja können Sie Zuordnungsjobs wiederherstellen, die vom Datenintegrationsdienst zur Verarbeitung an die Spark-Engine gesendet werden. Standardwert ist Nein.

4. Wählen, ob Sie eine Cluster-Konfiguration erstellen möchten?

   Mithilfe der Clusterkonfiguration kann der Datenintegrationsdienst Mapping-Logik an den Cluster übertragen. Wenn Sie in die Hadoop-Umgebung integrieren, können Sie eine Cluster-Konfiguration erstellen.

   Drücken Sie 1, wenn Sie eine Cluster-Konfiguration erstellen möchten.

   Drücken Sie 2, wenn Sie keine Cluster-Konfiguration erstellen möchten. Der Standardwert ist 1.

   Lesen Sie nach der Installation das *Data Engineering-Integrationshandbuch* durch, um die Domäne vollständig in die Hadoop-Umgebung zu integrieren.

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:

Property	Description
Configure tablespace	In a single-partition database, if you select No, the installer creates the tables in the default tablespace. In a multi-partition database, you must select Yes. Select whether to specify a tablespace: 1 - No 2 - Yes
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single-partition database, enter the name of the tablespace in which to create the tables. In a multipartition database, specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

   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:

Property	Description
Schema name	Name of the schema that will contain domain configuration tables. If this parameter is blank, the installer creates the tables in the default schema.

   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: - 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>;Snaps
  hotSerializable=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: - 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: - 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.

   If you select IBM DB2, specify the tablespace for the repository tables:

Property	Description
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single partition database, if this option is not selected, the installer creates the tables in the default tablespace. In a multipartition database, select this option and specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

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: - 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://<host name>:<port number>;DatabaseName=
  ```

  Oracle

  ```
  jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=
  ```

  Use the following connection string to connect to the Oracle database through the Oracle Connection Manager:

  ```
  jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS name>;
  ```

  Microsoft SQL Server

  ```
  jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=
  ```

  Microsoft Azure SQL

  ```
  jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false
  ```

  PostgreSQL

  ```
  jdbc:Informatica:postgresql://<host name>:<port number>;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.

7. Geben Sie die Verbindungszeichenfolge für den Datenzugriff ein.

Profiling-Warehouse-Datenbank

Nachdem Sie den Content-Management-Dienst konfiguriert haben, können Sie die Datenbank für das Daten-Profiling-Warehouse konfigurieren.

1. Wählen Sie den Datenbanktyp für das Daten-Profiling-Warehouse aus.

   In der folgenden Tabelle sind die Datenbanken für das Daten-Profiling-Warehouse aufgeführt.

Eingabeaufforderung	Beschreibung
Datenbanktyp	Datenbanktyp für das Daten-Profiling-Warehouse. Wählen Sie eine der folgenden Optionen aus: - Oracle - Microsoft SQL Server - IBM DB2

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	Name für das Benutzerkonto des Daten-Profiling-Warehouse.
Passwort des Datenbankbenutzers	Passwort für das Benutzerkonto des Daten-Profiling-Warehouse.

   If you select IBM DB2, specify the tablespace for the repository tables:

Property	Description
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single partition database, if this option is not selected, the installer creates the tables in the default tablespace. In a multipartition database, select this option and specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

3. 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.
4. 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**.

   If you select IBM DB2, specify the tablespace for the repository tables:

Property	Description
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single partition database, if this option is not selected, the installer creates the tables in the default tablespace. In a multipartition database, select this option and specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

   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: - 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://<host name>:<port number>;DatabaseName=
  ```

  Oracle

  ```
  jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=
  ```

  Use the following connection string to connect to the Oracle database through the Oracle Connection Manager:

  ```
  jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS name>;
  ```

  Microsoft SQL Server

  ```
  jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=
  ```

  Microsoft Azure SQL

  ```
  jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false
  ```

  PostgreSQL

  ```
  jdbc:Informatica:postgresql://<host name>:<port number>;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.

5. Geben Sie die Verbindungszeichenfolge für den Datenzugriff ein.

Erstellen der Cluster-Konfiguration

Nach der Konfiguration der Daten-Profiling-Warehouse-Verbindung können Sie die Clusterkonfiguration für die nicht native Umgebung erstellen.

1. Geben Sie den Namen der zu erstellende Cluster-Konfiguration ein.
2. Geben Sie die nicht native Distribution für den Cluster an.

In der folgenden Tabelle werden die Optionen beschrieben, die Sie angeben können:

Eingabeaufforderung	Beschreibung
1	Cloudera. Sie können eine Clusterkonfiguration für einen Cloudera-Cluster entweder auf der Cloudera Data Platform (CDP) oder für Cloudera Distribution Hadoop (CDH) erstellen.
2	Hortonworks
3	Azure HDInsight
4	MapR. Sie müssen die Konfigurationseigenschaften für den MapR-Cluster aus einer Archivdatei importieren.
5	Amazon EMR. Sie müssen die Konfigurationseigenschaften für den Amazon EMR-Cluster aus einer Archivdatei importieren.
6	Databricks
7	Google Dataproc

3. Importieren Sie Konfigurationseigenschaften aus der nicht nativen Umgebung, um die Clusterkonfiguration zu erstellen.
   - Um die Eigenschaften aus einer Archivdatei zu importieren, drücken Sie **1**. Wenn Sie eine Cluster-Konfiguration für einen Amazon EMR-Cluster, einen MapR-Cluster oder einen Google Dataproc-Cluster erstellen, müssen Sie die Eigenschaften aus einer Archivdatei importieren.
   - Um die Eigenschaften direkt aus dem Cluster zu importieren, drücken Sie **2**.
4. Wenn Sie die Eigenschaften aus einer Archivdatei importieren möchten, müssen Sie den Namen der Konfigurationsarchivdatei und den Pfad zur Datei wählen.
5. Wenn Sie die Eigenschaften direkt aus dem Cluster importieren möchten, geben Sie die Verbindungseigenschaften an.

   Die folgende Tabelle beschreibt die angegebenen Clustereigenschaften für Cloudera, Hortonworks oder Azure HDInsight:

Eigenschaft	Beschreibung
Host	Der Hostname oder die IP-Adresse des Cluster-Managers.
Port	Der Port des Cluster-Managers.
Benutzer-ID	Benutzername des Clusters.
Passwort	Passwort für den Clusterbenutzer.

Eigenschaft	Beschreibung
Clustername	Name des Clusters. Verwenden Sie den Anzeigenamen, wenn der Cluster-Manager mehrere Cluster verwaltet. Wenn Sie keinen Cluster-Namen angeben, importiert der Assistent Informationen basierend auf dem Standard-Cluster.
Engine-Typ	Wenn Sie einen Cloudera-Cluster angegeben haben, fordert das Installationsprogramm zur Eingabe des Engine-Typs auf. Wenn Sie einen CDP-Cluster verwenden, akzeptieren Sie den Standard-Engine-Typ Tez. Wenn Sie einen CDH-Cluster verwenden, legen Sie MRv2 mit der Eingabe **2** als Engine-Typ fest. Der Standardwert ist **1**.

In der folgenden Tabelle werden die Databricks-Clustereigenschaften beschrieben, die Sie angeben können:

Eigenschaft	Beschreibung
Databricks-Domäne	Geben Sie die URL des Databricks-Clusters ein.
Databricks-Token-ID	Geben Sie die Token-ID des Databricks-Clusters ein.
Databricks-Cluster-ID	Geben Sie die Cluster-ID des Databricks-Clusters ein.

6. Um die dem Cluster zugeordneten Hadoop-, HDFS-, HBase- oder Databricks-Verbindungen zu erstellen, drücken Sie **1**.

   Das Installationsprogramm fügt den Verbindungstyp an den Namen der Clusterkonfiguration an, um einen Verbindungsnamen zu erstellen.

Metadaten-Zugriffsdienst

Der Metadaten-Zugriffsdienst ist ein Anwendungsdienst, mit dem das Developer Tool auf die Hadoop-Umgebung zugreifen kann, um Metadaten zu importieren und in der Vorschau anzuzeigen. Wenn die Domäne eine Nicht-Kerberos-Authentifizierung verwendet, können Sie den Metadaten-Zugriffsdienst erstellen und konfigurieren. Wenn die Domäne die Kerberos-Authentifizierung verwendet, erstellen Sie den Metadaten-Zugriffsdienst nicht.

1. Wenn Sie während der Installation die Erstellung eines Metadaten-Zugriffsdiensts ausgewählt haben, wird die Seite **Metadaten-Zugriffsdienst** geöffnet.
2. Konfigurieren Sie die Diensteigenschaften für den Metadaten-Zugriffsdienst.

   In der folgenden Tabelle sind die Diensteigenschaften für den Metadaten-Zugriffsdienst aufgeführt:

Eigenschaft	Beschreibung
Dienstname	Name des Metadaten-Zugriffsdiensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Er darf weder mehr als 230 Zeichen enthalten noch mit @ beginnen. Außerdem darf er weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
HTTP-Protokolltyp	Der HTTP-Protokolltyp für den Metadaten-Zugriffsdienst. Wählen Sie HTTP oder HTTPS.

3. Geben Sie die HTTP- oder HTTPS-Portnummer für den Metadaten-Zugriffsdienst ein.
4. Wenn Sie HTTPS auswählen, können Sie entweder die standardmäßigen Informatica-SSL-Zertifikatsdateien verwenden oder den Speicherort für die SSL-Zertifikatsdateien festlegen.
5. Wählen Sie aus, die sichere Kommunikation für den Metadaten-Zugriffsdienst zu aktivieren:

   In der folgenden Tabelle werden die Eigenschaften beschrieben, die die Kommunikation für den Dienst sichern:

Eigenschaft	Beschreibung
Sichere Kommunikation aktivierenden Dienst aktivieren	Wählen Sie **1**, um die vom Installationsprogramm generierte Standard-Schlüsselspeicherdatei zu verwenden. Wählen Sie **2**, um eine andere Schlüsselspeicherdatei zu verwenden.
Schlüsselspeicherdatei für den Metadaten-Zugriffsdienst	Speicherort der Schlüsselspeicherdatei, die Sie verwenden möchten. Erforderlich, wenn Sie eine andere Schlüsselspeicherdatei verwenden möchten.
Passwort für den Metadaten-Zugriffsdienst	Das Passwort der Schlüsselspeicherdatei, die Sie verwenden möchten. Erforderlich, wenn Sie eine andere Schlüsselspeicherdatei verwenden möchten.
Truststore-Datei für den Metadaten-Zugriffsdienst	Speicherort der Truststore-Datei, die Sie verwenden möchten. Erforderlich, wenn Sie eine andere Truststore-Datei verwenden möchten.
Truststore-Passwort für den Metadaten-Zugriffsdienst	Das Passwort der Schlüsselspeicherdatei, die Sie verwenden möchten. Erforderlich, wenn Sie eine andere Truststore-Datei verwenden möchten.
SSL-Protokoll	Geben Sie das SSL-Protokoll an.

6. Legen Sie die Eigenschaften des Metadaten-Zugriffsdiensts fest.

   In der folgenden Tabelle werden die Eigenschaften des Metadaten-Zugriffsdiensts beschrieben:

Eigenschaft	Beschreibung
Dienst aktivieren	Wählen Sie **1** aus, um den Metadaten-Zugriffsdienst zu deaktivieren. Wählen Sie **2** aus, um den Metadaten-Zugriffsdienst zu aktivieren. Der Metadaten-Zugriffsdienst hat keine andere Dienstabhängigkeit. Standardwert ist **1**.
Betriebssystemprofil und Identitätswechsel verwenden	Wählen Sie **1** aus, um das Betriebssystemprofil und den Identitätswechsel zu deaktivieren. Wählen Sie **2** aus, um das Betriebssystemprofil und den Identitätswechsel zu aktivieren. Standardwert ist **1**.
Angemeldeten Benutzer als Benutzer für den Identitätswechsel verwenden	Erforderlich, wenn der Hadoop-Cluster die Kerberos-Authentifizierung verwendet. Der Hadoop-Identitätswechselbenutzer ist der Benutzername, dessen Identität vom Metadaten-Zugriffsdienst übernommen wird, um Metadaten zur Entwurfszeit aus der Hadoop-Umgebung zu importieren. Wählen Sie **1** aus, um den angemeldeten Benutzer als Identitätswechselbenutzer zu deaktivieren. Wählen Sie **2** aus, um den angemeldeten Benutzer als Identitätswechselbenutzer zu aktivieren. Standardwert ist **1**.

7. Geben Sie die Protokollebene an.
   - 1. SCHWERWIEGEND
   - 2. FEHLER
   - 3. WARNUNG
   - 4. INFO
   - 5. NACHVERFOLGUNG
   - 6. DEBUG

   Standardwert ist **4**.

Wenn Sie das Konfigurieren der PowerCenter-Dienste ausgewählt haben, wird die Seite **PowerCenter-Repository-Dienst und PowerCenter-Integrationsdienst** angezeigt. Wenn Sie keine zusätzlichen Dienstkonfigurationen ausgewählt haben, wird der Abschnitt **Nach der Installation – Zusammenfassung** angezeigt.

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: - 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 10.5.3 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. Choose whether you want to install distribution packages through the Informatica installer.
   - Press **1** if you don't need distribution packages or if you want to install them later.
   - Press **2** if you want to install distribution packages through the installer.

   Default is 1.
4. If you choose to install distribution packages, select one or more packages from the list that you want to install. Separate multiple packages with a comma.

   Default is 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 144 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.

1. Drücken Sie **2**, um eine Domäne anzufügen.

   Das Installationsprogramm fügt einen Knoten auf dem Computer an, auf dem die Installation erfolgt.

2. 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.

3. 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.

4. Wenn Sie eine HTTPS-Verbindung für den Informatica Administrator aktivieren, geben Sie die zum Sichern der Verbindung zu verwendende HTTPS-Portnummer ein.

5. 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 145.

   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 infa_keystore.jks enthalten.
Schlüsselspeicherpasswort	Passwort für den Schlüsselspeicher „infa_keystore.jks“.
Verzeichnis der Truststore-Datei	Verzeichnis, das die Truststore-Dateien enthält. Das Verzeichnis muss Dateien mit der Bezeichnung "infa_truststore.jks" und "infa_truststore.pem" enthalten.
Truststore-Passwort	Passwort für die Datei infa_truststore.jks.

Der Abschnitt **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	Pfad und Dateiname des Verschlüsselungsschlüssels für die Informatica-Domäne, der Sie beitreten möchten. Alle Knoten in der Informatica-Domäne verwenden den gleichen Verschlüsselungsschlüssel. Sie müssen die Verschlüsselungsschlüsseldatei festlegen, die auf dem Gateway-Knoten für die Domäne erstellt wurde, der Sie beitreten möchten. Wenn Sie die Verschlüsselungsschlüsseldatei in ein temporäres Verzeichnis kopiert haben, damit sie für die Knoten in der Domäne zugänglich ist, geben Sie den Pfad und den Dateinamen der Verschlüsselungsschlüsseldatei im temporären Verzeichnis an.
Verzeichnis des Verschlüsselungsschlüssels	Verzeichnis zum Speichern des Verschlüsselungsschlüssels auf dem während dieser Installation erstellten Knoten. Das Installationsprogramm kopiert die Verschlüsselungsschlüsseldatei für die Domäne in das Verzeichnis des Verschlüsselungsschlüssels auf dem neuen Knoten.

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 94.

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 Standardhostnamen. Wenn der Computer mehrere Netzwerknamen aufweist, können Sie den Standardhostnamen ändern und einen alternativen Netzwerknamen verwenden. **Hinweis:** Der Hostname des Knotens darf keine Unterstriche (_) enthalten. Verwenden Sie nicht localhost. Der Hostname muss den Computer eindeutig kennzeichnen.
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	Description
Service Manager port	Port number used by the Service Manager on the node. The Service Manager listens for incoming connection requests on this port. Client applications use this port to communicate with the services in the domain. The Informatica command line programs use this port to communicate to the domain. This is also the port for the SQL data service JDBC/ODBC driver. Default is 6006.
Service Manager Shutdown port	Port number that controls server shutdown for the domain Service Manager. The Service Manager listens for shutdown commands on this port. Default is 6007.
Informatica Administrator port	Port number used by Informatica Administrator. Default is 6008.
Informatica Administrator HTTPS port	No default port. Enter the required port number when you create the service. Setting this port to 0 disables an HTTPS connection to the Administrator tool.
Informatica Administrator shutdown port	Port number that controls server shutdown for Informatica Administrator. Informatica Administrator listens for shutdown commands on this port. Default is 6009.
Minimum port number	Lowest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6014.
Maximum port number	Highest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 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:

Property	Description
Configure tablespace	In a single-partition database, if you select No, the installer creates the tables in the default tablespace. In a multi-partition database, you must select Yes. Select whether to specify a tablespace: 1 - No 2 - Yes
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single-partition database, enter the name of the tablespace in which to create the tables. In a multipartition database, specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

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:

Property	Description
Schema name	Name of the schema that will contain domain configuration tables. If this parameter is blank, the installer creates the tables in the default schema.

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

d. Geben Sie die JDBC-Verbindungsdaten ein.

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

Eingabeaufforderung	Beschreibung
Datenbank-Hostname	Der Hostname für die Datenbank.
Datenbank-Portnummer	Portnummer der Datenbank.

Eingabeaufforderung	Beschreibung
Datenbankdienstname	Dienst- oder Datenbankname: - Oracle: Geben Sie den Dienstnamen ein. - Microsoft SQL Server: Geben Sie den Datenbanknamen ein. - IBM DB2: Geben Sie den Dienstnamen ein. - 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>;Snaps
  hotSerializable=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: - 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	Zur Verwendung der im Standardschlüsselspeicher und im Truststore enthaltenen SSL-Standardzertifikate von Informatica. **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	Zur Verwendung von benutzerdefinierten SSL-Zertifikaten. Sie müssen den Speicherort der Schlüsselspeicher- und Truststore-Dateien angeben. Sie können ein selbstsigniertes Zertifikat oder ein von einer Zertifizierungsstelle ausgegebenes Zertifikat verwenden. Sie müssen SSL-Zertifikate im PEM-Format und in Java-Schlüsselspeicherdateien (JKS) bereitstellen. Informatica benötigt bestimmte Namen für die SSL-Zertifikatsdateien in der Informatica-Domäne. Sie müssen für alle Knoten in der Domäne dieselben SSL-Zertifikate verwenden. Speichern Sie die Truststore- und Schlüsselspeicherdateien in einem Verzeichnis, auf das alle Knoten in der Domäne zugreifen können, und geben Sie für alle Knoten in derselben Domäne dasselbe Schlüsselspeicherdatei- und Truststore-Datei-Verzeichnis an.

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.

3. Wählen, ob Sie die Data Engineering-Wiederherstellung für Aufträge aktivieren möchten, die auf der Spark-Engine ausgeführt werden?

   Bei Auswahl von Ja können Sie Zuordnungsjobs wiederherstellen, die vom Datenintegrationsdienst zur Verarbeitung an die Spark-Engine gesendet werden. Standardwert ist Nein.

4. Wählen, ob Sie eine Cluster-Konfiguration erstellen möchten?

   Mithilfe der Clusterkonfiguration kann der Datenintegrationsdienst Mapping-Logik an den Cluster übertragen. Wenn Sie in die Hadoop-Umgebung integrieren, können Sie eine Cluster-Konfiguration erstellen.

   Drücken Sie 1, wenn Sie eine Cluster-Konfiguration erstellen möchten.

   Drücken Sie 2, wenn Sie keine Cluster-Konfiguration erstellen möchten. Der Standardwert ist 1.

   Lesen Sie nach der Installation das *Data Engineering-Integrationshandbuch* durch, um die Domäne vollständig in die Hadoop-Umgebung zu integrieren.

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: - 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 8

Ausführen des automatischen Installationsprogramms

Dieses Kapitel umfasst die folgenden Themen:

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 automatischen 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 Standardeigenschaftenwerten 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 9

Fehlerbehebung

Dieses Kapitel umfasst die folgenden Themen:

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 Objektdatei installInst.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	- 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	- 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	Zeichnet Ereignisse von der Java Virtual Machine (JVM) auf, die den Dienstmanager ausführt. Beispiel: Ein Port ist während der Installation verfügbar, jedoch beim Start des Dienstmanager in Gebrauch. In diesem Protokoll finden Sie weitere Informationen dazu, welcher Port während des Starts des Dienstmanager nicht verfügbar war. Die catalina.out-Datei befindet sich im folgenden Verzeichnis: `<Informatica-Installationsverzeichnis>/logs/< Knotenname>/catalina.out`
node.log	Zeichnet Ereignisse auf, die während des Starts des Dienstmanager auf einem Knoten generiert wurden. In diesem Protokoll finden Sie weitere Informationen dazu, warum der Dienstmanager zu einem Knoten nicht gestartet wurde. Beispiel: Wenn der Dienstmanager nach 30 Sekunden keine Verbindung zur Domänen-Konfigurations-Datenbank herstellen kann, schlägt das Starten des Dienstmanager fehl. Die Datei node.log befindet sich im Verzeichnis /tomcat/logs.

Hinweis: Der Dienstmanager verwendet die Datei „node.log“ außerdem zum Aufzeichnen von Ereignissen, bei denen der Protokokllmanager 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 Datenbankverfügen. 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:

KAPITEL 10

Durchführen der Domänenkonfiguration

Dieses Kapitel umfasst die folgenden Themen:

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.

❑ Integrieren Sie die Domäne mit der Hadoop-Umgebung.

❑ 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 Repositorys 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.

Integrieren der Domäne mit der Hadoop- oder Databricks-Umgebung

Wenn Sie die Cluster-Konfiguration während der Installation aus der Hadoop- oder Databricks-Umgebung importiert haben, müssen Sie die Integration zwischen der Domäne und der Hadoop-Umgebung abschließen. Integrationsaufgaben sind sowohl in der Hadoop-Umgebung als auch in der Umgebung der Informatica-Domäne erforderlich.

Um die Domäne mit der Hadoop-Umgebung zu integrieren, führen Sie die folgenden allgemeinen Aufgaben aus:

1. Bereiten Sie Verzeichnisse, Benutzer und Berechtigungen vor.
2. Konfigurieren Sie *-site.xml-Dateien in der Hadoop- oder Databricks-Umgebung. Die *-site.xml-Eigenschaftendateien müssen mit Werten aktualisiert werden, die für die Informatica-Verarbeitung in der Umgebung des Drittanbieters erforderlich sind.
3. Aktualisieren Sie die Cluster-Konfiguration im Administrator Tool. Aktualisieren Sie die Cluster-Konfiguration, um die aktualisierten Eigenschaften aus den *-site.xml-Dateien in den Cluster abzurufen.
4. Aktualisieren Sie Verbindungen im Administrator Tool. Aktualisieren Sie Verbindungen, wenn Sie andere Eigenschaftenwerte als die Standardwerte verwenden möchten. Außerdem müssen Sie Umgebungsvariablen in den Verbindungseigenschaften konfigurieren.

Weitere Informationen zum Importieren einer Hadoop-Cluster-Konfiguration finden Sie im *Handbuch zu Data Engineering Integration*.

Überprüfen der Gebietsschemaeinstellungen und der Codepage-Kompatibilität

Die Codepages für Anwendungsdienste müssen mit den Codepages in der Domäne kompatibel sein.

Überprüfen und konfigurieren Sie die Gebietsschemaeinstellungen und Codepages:

Stellen Sie sicher, dass die Domänen-Konfigurationsdatenbank mit den Codeseiten der Anwendungsdienste, die Sie in der Domäne erstellen, kompatibel ist.

Der Dienstmanager synchronisiert die Liste der Benutzer in der Domäne mit der Liste der Benutzer und Gruppen in allen Anwendungsdiensten Wenn ein Benutzername in der Domäne Zeichen enthält, die die Codepage des Anwendungsdiensts nicht erkennt, werden diese Zeichen nicht ordnungsgemäß umgewandelt, was zu Inkonsistenzen führt.

Stellen Sie sicher, dass die Gebietsschemaeinstellungen auf Computern mit Zugriff auf das Administrator-Tool und die Informatica-Client-Tools mit den Codepages der Repositorys in der Domäne kompatibel sind.

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

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 Gebietsschemavariable 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}”

Datenbank	Wert
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 11

Vorbereiten zum Erstellen der Anwendungsdienste

Dieses Kapitel umfasst die folgenden Themen:

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 Objektanhänge

Erstellen Sie ein Verzeichnis, um die Dateien zu speichern, die von Content-Managern als Anhänge zu Glossarobjekten hinzugefügt werden können. Erstellen Sie das Verzeichnis auf dem Knoten, auf dem der Analyst-Dienst ausgeführt wird.

Beispiel: Sie können ein Verzeichnis namens "attachmentdirectory" an dem folgenden Speicherort erstellen: `<Informatica-Installationsverzeichnis>/server`.

Erstellen eines Schlüsselspeichers für eine sichere Verbindung zu einem Web-Anwendungsdienst

Sie können eine sichere Verbindung zwischen der Informatica-Domäne und einem Web-Anwendungsdienst wie Analyst-Dienst herstellen. Informatica verwendet das SSL/TLS-Protokoll zum Verschlüsseln von Netzwerkverkehr. Um die Verbindung zu sichern, müssen Sie die erforderlichen Dateien erstellen.

Bevor Sie die Verbindung zu einem Web-Anwendungsdienst sichern, überprüfen Sie, ob die folgenden Anforderungen erfüllt sind:

Sie haben eine Zertifikatssignieranfrage und einen privaten Schlüssel erstellt.

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

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

Sie haben ein signiertes SSL-Zertifikat.

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

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

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

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

Der Schlüsselspeicher befindet sich in einem Verzeichnis, auf das zugegriffen werden kann.

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

Anmelden beim Informatica Administrator

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

Wenn die Informatica-Domäne in einem Netzwerk mit Kerberos-Authentifizierung ausgeführt wird, müssen Sie den Browser 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/
     ```

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

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

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

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

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

Fehlerbehebung bei der Anmeldung bei Informatica Administrator

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

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

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

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

Wenn nach Ihrer Anmeldung beim Administrator-Tool eine leere Seite angezeigt wird, überprüfen Sie, ob Sie die Delegierung für alle Benutzerkonten mit in der Informatica-Domäne verwendeten Dienstprinzipalen aktiviert haben. Zum Aktivieren der Delegierung legen Sie im Microsoft Active Directory Service die Option **Benutzer bei Delegierungen aller Dienste vertrauen (nur Kerberos)** für jedes Benutzerkonto fest, für das Sie einen SPN festgelegt haben.

Erstellen von Verbindungen

Erstellen Sie im Administrator Tool Verbindungen zu den Datenbanken, die die Anwendungsdienste verwenden. Sie müssen die Verbindungsdetails beim Konfigurieren des Anwendungsdiensts angeben.

Wenn Sie die Datenbankverbindung erstellen, geben Sie die Eigenschaften der Datenbankverbindung an, und testen Sie die Verbindung.

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.

Datenbankverbindung	Beschreibung
Profiling-Warehouse-Datenbank	Zum Erstellen und Ausführen von Profilen und Scorecards erstellen Sie die Profiling-Warehouse-Datenbankverbindung für den Datenintegrationsdienst. Verwenden Sie diese Instanz des Datenintegrationsdiensts bei der Konfiguration der Laufzeiteigenschaften des Analyst-Diensts. **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**.
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.
Wiederholungszeitraum	Diese Eigenschaft ist für die zukünftige Verwendung reserviert.
Tablespace	Tablespace-Name der DB2 für LUW-Datenbank.

Eigenschaft	Beschreibung
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	Benutzername für die Datenbank
Passwort	Das Passwort für den Benutzernamen.
Vertrauenswürdige Verbindung verwenden	Optional. Bei Aktivierung verwendet der Datenintegrationsdienst die Windows-Authentifizierung, um auf die Microsoft SQL Server-Datenbank zuzugreifen. Der Benutzername, mit dem der Datenintegrationsdienst gestartet wird, muss ein gültiger Windows-Benutzer mit Zugriff auf die Microsoft SQL Server-Datenbank sein.
Verbindungszeichenfolge für den Metadatenzugriff	Die Verbindungszeichenfolge für das Importieren von physischen Datenobjekten. Verwenden Sie die folgende Verbindungszeichenfolge: `jdbc:informatica:sqlserver://<host>:<port>;databaseName=<dbname>`
Verbindungszeichenfolge für den Datenzugriff	Die Verbindungszeichenfolge für die Datenvorschau und das Ausführen von Mappings. Geben Sie `<ServerName>@<DBName>` ein
Domänenname	Optional. Der Name der Domäne, in der Microsoft SQL Server ausgeführt wird.
Paketgröße	Erforderlich. Optimieren Sie die ODBC-Verbindung zum Microsoft SQL Server. Erhöhen Sie die Paketgröße, um die Leistung zu erhöhen. Standardwert ist 0.
Codepage	Datenbank-Codepage
Eigentümername	Der Name des Eigentümers des Schemas. Geben Sie ihn für die Verbindungen zur Profiling Warehouse-Datenbank oder zur Datenobjekt-Cache-Datenbank an.
Schemaname	Der Name des Schemas in der Datenbank. Geben Sie ihn für die Verbindungen zum Profiling Warehouse oder zur Datenobjekt-Cache-Datenbank an. Sie müssen den Schemanamen für das Profiling Warehouse angeben, wenn der Schemaname anders lautet als der Benutzername der Datenbank. Sie müssen den Schemanamen für die Datenobjekt-Cache-Datenbank angeben, wenn der Schemaname anders lautet als der Benutzername für die Datenbank und Sie den Cache mit einem externen Tool verwalten.
Umgebungs-SQL	Optional. Geben Sie die SQL-Befehle zum Einrichten der Datenbankumgebung ein, wenn Sie eine Verbindung zur Datenbank herstellen. Der Datenintegrationsdienst führt die SQL-Befehle zur Verbindungsumgebung jedes Mal aus, wenn er eine Verbindung zur Datenbank herstellt.
Transaktions-SQL	Optional. Geben Sie die SQL-Befehle zum Einrichten der Datenbankumgebung ein, wenn Sie eine Verbindung zur Datenbank herstellen. Der Datenintegrationsdienst führt die Transaktionsumgebungs-SQL am Anfang jeder Transaktion aus.

Eigenschaft	Beschreibung
Wiederholungszeitraum	Diese Eigenschaft ist für die zukünftige Verwendung reserviert.
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.

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	Verbindungszeichenfolge für das Importieren von physischen Datenobjekten.
	Verwenden Sie die folgende Verbindungszeichenfolge:
	`jdbc:informatica:oracle://<host>:1521;SID=<sid>`
	Verwenden Sie die folgende Verbindungszeichenfolge, um eine Verbindung zu Oracle über den Oracle Connection Manager herzustellen:
	`jdbc:Informatica:oracle:TNSNamesFile=<vollqualifizierter Pfad zur Datei tnsnames.ora>;TNSServerName=<TNS-Servername>;`

Verbindungszeichenfolge für den Datenzugriff	Die Verbindungszeichenfolge für die Datenvorschau und das Ausführen von Zuordnungen. Geben Sie `dbname.world` aus dem TNSNAMES-Eintrag ein.
Codepage	Datenbank-Codepage
Umgebungs-SQL	Optional. Geben Sie die SQL-Befehle zum Einrichten der Datenbankumgebung ein, wenn Sie eine Verbindung zur Datenbank herstellen. Der Datenintegrationsdienst führt 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 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.

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: `jdbc:informatica:postgresql://<host>:<port>;Database=<id>`
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 12

Erstellen und Konfigurieren von Anwendungsdiensten

Dieses Kapitel umfasst die folgenden Themen:

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. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Er darf weder mehr als 128 Zeichen enthalten noch mit @ beginnen. Außerdem darf er weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Beschreibung	Beschreibung des Diensts. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Domäne und Ordner, in der/dem der Dienst erstellt wurde. Um einen anderen Ordner auszuwählen, klicken Sie auf **Durchsuchen**. Sie können den Dienst nach dessen Erstellung verschieben.
Lizenz	Lizenzobjekt für die Verwendung des Diensts.
Knoten	Knoten, auf dem der Dienst ausgeführt wird.
Backup-Knoten	Wenn die Lizenz hohe Verfügbarkeit einschließt, sind dies die Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist.

4. Klicken Sie auf **Weiter**.

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

5. Geben Sie die folgenden Eigenschaften für die Modellrepository-Datenbank ein:

Eigenschaft	Beschreibung
Datenbanktyp	Der Typ der Repository-Datenbank.
Benutzername	Der Datenbankbenutzername für das Repository. 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	- 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>"` **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. - 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"`
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= "`

7. Wenn die Modellrepository-Datenbank mit dem SSL-Protokoll gesichert ist, müssen Sie die sicheren Datenbankparameter im Feld **Sichere JDBC-Parameter** eingeben.

   Geben Sie die Parameter als `name=value`-Paare, getrennt durch ein Semikolon (;) ein. Beispiel:

   ```
   param1=value1;param2=value2
   ```

Geben Sie die folgenden sicheren Datenbankparameter ein:

Sicherer Datenbankparameter	Beschreibung
EncryptionMethod	Erforderlich. Gibt an, ob Daten bei der Netzwerkübertragung verschlüsselt werden. Dieser Parameter muss auf `SSL` festgelegt werden.
ValidateServerCertificate	Optional. Gibt an, ob Informatica das Zertifikat validiert, das der Datenbankserver sendet. Wenn dieser Parameter auf TRUE gesetzt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat. Wenn Sie den HostNameInCertificate-Parameter angeben, validiert Informatica ebenfalls den Hostnamen im Zertifikat. Wenn dieser Parameter auf FALSE gesetzt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat nicht. Informatica ignoriert alle Truststore-Informationen, die Sie angeben.
HostNameInCertificate	Optional. Hostname des Computers, auf dem die sichere Datenbank gehostet wird. Wenn Sie einen Hostnamen angeben, validiert Informatica den Hostnamen in der Verbindungszeichenfolge mit dem Hostnamen im SSL-Zertifikat.
cryptoProtocolVersion	Erforderlich. Gibt das Kryptografieprotokoll an, das für die Verbindung mit einer sicheren Datenbank verwendet werden soll. Sie können je nach dem vom Datenbankserver verwendeten Kryptografieprotokoll den Parameter auf `cryptoProtocolVersion=TLSv1.1` oder `cryptoProtocolVersion=TLSv1.2` einstellen.
TrustStore	Erforderlich. Pfad und Dateiname der Truststore-Datei, die das SSL-Zertifikat für die Datenbank enthält. Wenn Sie den Pfad für die Truststore-Datei nicht hinzufügen, sucht Informatica im folgenden Standardverzeichnis nach der Datei: `<Informatica-Installationsverzeichnis>/tomcat/bin`
TrustStorePassword	Erforderlich. Passwort der Truststore-Datei für die sichere Datenbank.

Hinweis: Informatica hängt die sicheren JDBC-Parameter an den JDBC-Verbindungsstring an. Wenn Sie die sicheren JDBC-Parameter direkt zur Verbindungszeichenfolge hinzufügen, geben Sie im Feld **Sichere JDBC-Parameter** keinen Parameter ein.

8. Klicken Sie auf **Testverbindung**, um zu überprüfen, ob Sie eine Verbindung zur Datenbank herstellen können.
9. Wählen Sie **Die angegebene Verbindungszeichenfolge weist keinen Inhalt auf. Erstellen Sie neue Inhalte.** aus.
10. Klicken Sie auf **Fertig stellen**.

    Die Domäne erstellt den Modellrepository-Dienst, erstellt Inhalt für das Modellrepository in der angegebenen Datenbank und aktiviert den Dienst.

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. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Er darf weder mehr als 128 Zeichen enthalten noch mit @ beginnen. Außerdem darf er weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Beschreibung	Beschreibung des Diensts. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Domäne und Ordner, in der/dem der Dienst erstellt wurde. Um einen anderen Ordner auszuwählen, klicken Sie auf **Durchsuchen**. Sie können den Dienst nach dessen Erstellung verschieben.
Lizenz	Lizenzobjekt für die Verwendung des Diensts.
Zuweisen	Wählen Sie **Knoten** aus, um den Dienst zur Ausführung auf einem Knoten zu konfigurieren. Wenn die Lizenz Gitter einschließt, können Sie ein Gitter erstellen und den auf dem Gitter auszuführenden Dienst zuweisen, nachdem Sie den Dienst erstellt haben.
Knoten	Knoten, auf dem der Dienst ausgeführt wird.
Backup-Knoten	Wenn die Lizenz hohe Verfügbarkeit einschließt, sind dies die Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist.
Modellrepository-Dienst	Modellrepository-Dienst zum Zuweisen zum Dienst.
Benutzername	Benutzername, den der Dienst für den Zugriff auf den Modellrepository-Dienst verwendet. Geben Sie den Modellrepository-Benutzer ein, den Sie erstellt haben.
Passwort	Passwort für den Modellrepository-Benutzer.
Sicherheitsdomäne	LDAP-Sicherheitsdomäne für den Benutzer des Modellrepository. Das Feld wird angezeigt, wenn die Informatica-Domäne eine LDAP-Sicherheitsdomäne enthält. Nicht verfügbar für eine Domäne mit Kerberos-Authentifizierung.

6. Klicken Sie auf **Weiter**.

   Die Seite **Neuer Datenintegrationsdienst - Schritt 2 von 14** wird angezeigt.
7. Geben Sie die HTTP-Portnummer für den Datenintegrationsdienst ein.
8. Akzeptieren Sie für die restlichen Sicherheitseigenschaften die Standardwerte. Sie können die Sicherheitseigenschaften nach dem Erstellen des Datenintegrationsdiensts konfigurieren.
9. Wählen Sie **Dienst aktivieren** aus.

   Zum Aktivieren des Datenintegrationsdiensts muss der Modellrepository-Dienst ausgeführt werden.
10. Stellen Sie sicher, dass **Zur Plugin-Konfigurationsseite wechseln** nicht ausgewählt ist.
11. Klicken Sie auf **Weiter**.

    Die Seite **Neuer Datenintegrationsdienst - Schritt 3 von 14** wird angezeigt.
12. Stellen Sie die Eigenschaft **Joboptionen starten** auf einen der folgenden Werte ein:

- Im Dienstprozess. Konfigurieren Sie diesen Wert, wenn Sie SQL-Datendienst- und Webdienstjobs ausführen. Die SQL-Datendienst- und Webdienstjobs erreichen in der Regel eine bessere Leistung, wenn der Datenintegrationsdienst Jobs im Dienstprozess ausführt.
- In separaten lokalen Prozessen. Konfigurieren Sie diesen Wert, wenn Sie Mapping-, Profil- und Arbeitsablaufjobs ausführen. Wenn der Datenintegrationsdienst Jobs in separaten lokalen Prozessen ausführt, erhöht sich die Stabilität, weil eine unerwartete Unterbrechung eines Jobs keine Auswirkungen auf alle anderen Jobs hat.

Wenn Sie den Datenintegrationsdienst nach der Erstellung des Diensts zur Ausführung auf einem Gitter konfigurieren, können Sie den Dienst zur Ausführung von Jobs in separaten Remoteprozessen konfigurieren.

13. Akzeptieren Sie die Standardwerte für die verbleibenden Ausführungsoptionen und klicken Sie auf **Weiter**.

    Die Seite **Neuer Datenintegrationsdienst - Schritt 4 von 14** wird angezeigt.

14. Wenn Sie die Datenobjekt-Cache-Datenbank für den Datenintegrationsdienst erstellt haben, klicken Sie auf **Auswählen** und wählen Sie die Cache-Verbindung aus. Wählen Sie die Datenobjekt-Cache-Verbindung aus, die Sie für den Dienst erstellt haben, um auf die Datenbank zuzugreifen.

15. Akzeptieren Sie für die restlichen Eigenschaften auf dieser Seite die Standardwerte und klicken Sie auf **Weiter**.

    Die Seite **Neuer Datenintegrationsdienst - Schritt 5 von 14** wird angezeigt.

16. Für eine optimale Leistung aktivieren Sie die Datenintegrationsdienst-Module, die Sie verwenden möchten.

    In der folgenden Tabelle werden die Datenintegrationsdienst-Module aufgelistet, die Sie aktivieren können:

Modul	Beschreibung
Webdienstmodul	Führt Vorgangs-Mappings für Webdienste durch.
Zuordnungsdienstmodul	Führt Mappings und Vorschauen aus.
Profilerstellungsdienst-Modul	Führt Profile und Scorecards aus.
SQL-Dienstmodul	Führt SQL-Abfragen von Client-Tools anderer Hersteller an einen SQL-Datendienst aus.
Arbeitsablauf-Orchestration-Dienstmodul	Führt Arbeitsabläufe aus.

17. Klicken Sie auf **Weiter**.

    Die Seite **Neuer Datenintegrationsdienst - Schritt 6 von 14** wird angezeigt.

    Sie können Sie die HTTP-Proxyservereigenschaften so konfigurieren, dass die HTTP-Anfragen an den Datenintegrationsdienst umgeleitet werden. Sie können Sie die HTTP-Konfigurationseigenschaften so konfigurieren, dass Webdienst-Client-Computer, die Anfragen an den Datenintegrationsdienst senden können, gefiltert werden. Diese Eigenschaften können Sie nach dem Erstellen des Diensts konfigurieren.

18. Akzeptieren Sie die Standardwerte für die HTTP-Proxyserver- und HTTP-Konfigurationseigenschaften und klicken Sie auf **Weiter**.

    Die Seite **Neuer Datenintegrationsdienst - Schritt 7 von 14** wird angezeigt.

Der Datenintegrationsdienst nutzt die Ergebnissatz-Cache-Eigenschaften, um zwischengespeicherte Ergebnisse für SQL-Datendienstabfragen und -Webdienstanfragen zu verwenden. Sie können die Eigenschaften nach dem Erstellen des Diensts konfigurieren.

19. Akzeptieren Sie die Standardwerte für die Eigenschaften des Ergebnissatz-Cache und klicken Sie auf **Weiter**.

    Die Seite **Neuer Datenintegrationsdienst - Schritt 8 von 14** wird angezeigt.

20. Wenn Sie die Profiling-Warehouse-Datenbank für den Datenintegrationsdienst erstellt haben, wählen Sie das Profilerstellungsdienst-Modul aus.

21. Wenn Sie die Arbeitsablauf-Datenbank für den Datenintegrationsdienst erstellt haben, wählen Sie das Arbeitsablauf-Orchestration-Dienstmodul aus.

22. Stellen Sie sicher, dass die restlichen Module nicht ausgewählt sind.

    Sie können die Eigenschaften für die restlichen Module nach dem Erstellen des Diensts konfigurieren.

23. Klicken Sie auf **Weiter**.

    Die Seite **Neuer Datenintegrationsdienst - Schritt 11 von 14** wird angezeigt.

24. Wenn Sie die Profiling-Warehouse-Datenbank für den Datenintegrationsdienst erstellt haben, klicken Sie auf **Auswählen**, um die Datenbankverbindung auszuwählen. Wählen Sie die Profiling-Warehouse-Verbindung aus, die Sie für den Dienst erstellt haben, um auf die Datenbank zuzugreifen.

25. Wählen Sie aus, ob die Profiling-Warehouse-Datenbank Inhalt aufweist oder nicht.

    Wenn Sie eine neue Profiling-Warehouse-Datenbank erstellt haben, wählen Sie **Die angegebene Verbindungszeichenfolge weist keinen Inhalt auf** aus.

26. Klicken Sie auf **Weiter**.

    Die Seite **Neuer Datenintegrationsdienst - Schritt 12 von 14** wird angezeigt.

27. Akzeptieren Sie die Standardwerte für die erweiterten Profiling-Eigenschaften und klicken Sie auf **Weiter**.

    Die Seite **Neuer Datenintegrationsdienst - Schritt 14 von 14** wird angezeigt.

28. Wenn Sie die Arbeitsablauf-Datenbank für den Datenintegrationsdienst erstellt haben, klicken Sie auf **Auswählen**, um die Datenbankverbindung auszuwählen. Wählen Sie die Arbeitsablauf-Datenbankverbindung aus, die Sie für den Dienst erstellt haben, um auf die Datenbank zuzugreifen.

29. Klicken Sie auf **Fertig stellen**.

    Die Domäne erstellt und aktiviert den Datenintegrationsdienst.

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

Nach dem Erstellen des Datenintegrationsdienstes

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

- Überprüfen der Hostdateikonfiguration
- 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. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Er darf weder mehr als 128 Zeichen enthalten noch mit @ beginnen. Außerdem darf er weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Beschreibung	Beschreibung des Diensts. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Domäne und Ordner, in der/dem der Dienst erstellt wurde. Um einen anderen Ordner auszuwählen, klicken Sie auf **Durchsuchen**. Sie können den Dienst nach dessen Erstellung verschieben.

Eigenschaft	Beschreibung
Lizenz	Lizenzobjekt für die Verwendung des Diensts.
Knoten	Knoten, auf dem der Dienst ausgeführt wird.
Primärer Knoten	Wenn die Lizenz hohe Verfügbarkeit einschließt, ist dies der Knoten, auf dem der Dienst standardmäßig ausgeführt wird. Erforderlich, wenn Sie eine Lizenz mit hoher Verfügbarkeit ausgewählt haben.
Backup-Knoten	Wenn die Lizenz hohe Verfügbarkeit einschließt, sind dies die Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist.

4. Klicken Sie auf **Weiter**.

   Die Seite **Neuer PowerCenter-Repository-Dienst – Schritt 2 von 2** wird angezeigt.

5. Geben Sie die folgenden Eigenschaften für die PowerCenter-Repository-Datenbank ein:

Eigenschaft	Beschreibung
Datenbanktyp	Der Typ der Repository-Datenbank.
Benutzername	Der Datenbankbenutzername für das Repository.
Passwort	Passwort für den PowerCenter-Repository-Datenbankbenutzer. Muss in 7-Bit-ASCII kodiert sein.
Verbindungszeichenfolge	Native Verbindungszeichenfolge, die der PowerCenter-Repository-Dienst verwendet, um auf die Repository-Datenbank zuzugreifen. Verwenden Sie die folgende native Syntax der Verbindungszeichenfolge für jede unterstützte Datenbank: - `servername@databasename` für Microsoft SQL Server und Sybase. - `databasename.world` für Oracle - `databasename` für IBM DB2
Codepage	Codepage der Repository-Datenbank. Der PowerCenter-Repository-Dienst verwendet zum Schreiben von Daten den in der Datenbank kodierten Datensatz. Nachdem Sie den PowerCenter-Repository-Dienst erstellt haben, können Sie die Codepage in den Eigenschaften des PowerCenter-Repository-Dienstes nicht mehr ändern.
Tablespace-Name	Name des Tablespace, in dem alle Repository-Datenbanktabellen erstellt werden sollen. Sie können im Tablespace-Namen keine Leerzeichen verwenden. Für IBM DB2- und Sybase-Datenbanken verfügbar. Um die Repository-Leistung bei IBM DB2 EEE-Repositorys zu verbessern, geben Sie einen Tablespace-Namen mit einem Knoten an.

6. Wählen Sie **Die angegebene Verbindungszeichenfolge weist keinen Inhalt auf. Erstellen Sie neue Inhalte.** aus.
7. Optional können Sie ein globales Repository auswählen.

   Nachdem Sie den Dienst erstellen, können Sie ein lokales Repository zu einem globalen Repository hochstufen. Ein globales Repository kann jedoch nicht in ein lokales Repository geändert werden
8. Wenn Ihre Lizenz über die teambasierte Entwicklungsoption verfügt, können Sie optional die Versionskontrolle des Repository aktivieren.

Nachdem Sie den Dienst erstellt haben, können Sie ein versionsloses Repository in ein Repository mit Versionsangabe konvertieren. Ein Repository mit Versionsangabe in ein versionsloses Repository zu konvertieren, ist jedoch nicht möglich.

9. Klicken Sie auf **Fertig stellen**.

   Die Domäne erstellt den PowerCenter-Repository-Dienst, startet den Dienst und erstellt Inhalt für das PowerCenter-Repository.

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

Nach dem Erstellen des PowerCenter-Repository-Dienstes

Führen Sie nach dem Erstellen des PowerCenter-Repository-Dienstes die folgenden Aufgaben durch:

- Konfigurieren des PowerCenter-Repository-Dienstes zur Ausführung im normalen Modus
- Erstellen des PowerCenter-Repository-Benutzers, wenn die Domäne keine Kerberos-Authentifizierung verwendet
- Erstellen anderer Anwendungsdienste

Führen Sie den PowerCenter-Repository-Dienst im Normalmodus aus.

Nachdem Sie den PowerCenter-Repository-Dienst erstellt haben, wird er im exklusiven Modus gestartet. Der Zugriff ist auf den Administrator beschränkt. Bearbeiten Sie die Diensteigenschaften, um den Dienst im normalen Betriebsmodus auszuführen und anderen Benutzern Zugriff zu gewähren.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten**.
2. Im Navigator wählen Sie den PowerCenter-Repository-Dienst.
3. Klicken Sie auf **Eigenschaften**.
4. Klicken Sie auf **Repository-Eigenschaften bearbeiten**.
5. Wählen Sie „Normal“ im Feld **Betriebsmodus** aus.
6. Klicken Sie auf **OK.**

   Sie müssen den PowerCenter-Repository-Dienst recyceln, damit die Änderungen wirksam werden.
7. Wählen Sie **Aktionen** > **Dienst recyceln**.

Erstellen des PowerCenter-Repository-Benutzers

Wenn die Domäne keine Kerberos-Authentifizierung verwendet, wird die Authentifizierung anderer Anwendungsdienste, die Anfragen an den PowerCenter-Repository-Dienst stellen, mit einem Benutzerkonto durchgeführt. Sie müssen ein Benutzerkonto erstellen und dem Benutzer die Administratorrolle für den PowerCenter-Repository-Dienst zuweisen.

Wenn Sie einen Anwendungsdienst erstellen, der vom PowerCenter-Repository-Dienst abhängig ist, geben Sie den Namen des PowerCenter-Repository-Dienstes und des PowerCenter-Repository-Benutzers an.

1. Klicken Sie im Administrator-Tool auf die Registerkarte **Sicherheit**.
2. Klicken Sie im Menü „Sicherheitsaktionen“ auf **Benutzer erstellen** , um ein natives Benutzerkonto zu erstellen.

   Hinweis: Wenn Sie die LDAP-Authentifizierung in der Domäne einrichten, können Sie ein LDAP-Benutzerkonto für den PowerCenter-Repository-Benutzer verwenden.

3. Geben Sie folgende Eigenschaften für den Benutzer ein:

Eigenschaft	Beschreibung
Anmeldename	Der Anmeldename für das Benutzerkonto. Der Anmeldename für ein Benutzerkonto muss innerhalb der Sicherheitsdomäne, zu der er gehört, eindeutig sein. Beim Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden. Er darf nicht länger als 128 Zeichen sein. Er darf weder einen Tabulator noch ein Zeilenende-Zeichen noch folgende Sonderzeichen enthalten: „ + " \ < > ; / * % ? & Der Name kann ein ASCII-Leerzeichen enthalten, jedoch nicht als erstes oder letztes Zeichen. Alle anderen Leerzeichen sind nicht zulässig.
Passwort	Das Passwort für das Benutzerkonto. Das Passwort kann zwischen 1 und 80 Zeichen lang sein.
Passwort bestätigen	Geben Sie das Passwort zur Bestätigung erneut ein. Sie müssen das Passwort noch einmal eingeben. Das Passwort darf nicht mit Kopieren und Einfügen eingegeben werden.
Vollständiger Name	Der vollständige Name für das Benutzerkonto. Der vollständige Name darf folgende Sonderzeichen nicht enthalten: < > “
Beschreibung	Die Beschreibung des Benutzerkontos. Die Beschreibung darf nicht länger als 765 Zeichen sein und keines der folgenden Sonderzeichen enthalten: < > “

4. Klicken Sie auf **OK**.

   Die Benutzereigenschaften werden angezeigt.
5. Klicken Sie auf die Registerkarte **Berechtigungen**.
6. Klicken Sie auf **Bearbeiten**.

   Das Dialogfeld **Rollen und Rechte bearbeiten** wird eingeblendet.
7. Erweitern Sie auf der Registerkarte **Rollen** den PowerCenter-Repository-Dienst.
8. Wählen Sie unter **Systemdefinierte Rollen** „Administrator“ aus und klicken Sie auf **OK**.

Erstellen weiterer Dienste

Nach dem Erstellen des PowerCenter-Repository-Dienstes erstellen Sie die Anwendungsdienste, die vom PowerCenter-Repository-Dienst abhängig sind.

Sie können die folgenden Anwendungsdienste erstellen:

1. PowerCenter-Integrationsdienst
2. Metadata Manager-Dienst
3. Webdienst-Hub-Dienst

Erstellen und Konfigurieren des PowerCenter-Integrationsdienstes

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

Wenn Sie einen Arbeitsablauf im PowerCenter Client ausführen, sendet der Client die Anfragen an den PowerCenter-Integrationsdienst. Der PowerCenter-Integrationsdienst stellt eine Verbindung zum PowerCenter-Repository-Dienst zum Abrufen von Metadaten aus dem PowerCenter-Repository her und führt anschließend die Sitzungen und Arbeitsabläufe aus und überwacht sie.

Erstellen des PowerCenter-Integrationsdienstes

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

Stellen Sie vor dem Erstellen des PowerCenter-Integrationsdiensts 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. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Er darf weder mehr als 128 Zeichen enthalten noch mit @ beginnen. Außerdem darf er weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Beschreibung	Beschreibung des Diensts. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Domäne und Ordner, in der/dem der Dienst erstellt wurde. Um einen anderen Ordner auszuwählen, klicken Sie auf **Durchsuchen**. Sie können den Dienst nach dessen Erstellung verschieben.
Lizenz	Lizenzobjekt für die Verwendung des Diensts.
Knoten	Knoten, auf dem der Dienst ausgeführt wird.
Zuweisen	Wählen Sie **Knoten** aus, um den Dienst zur Ausführung auf einem Knoten zu konfigurieren. Wenn die Lizenz Gitter einschließt, können Sie ein Gitter erstellen und den auf dem Gitter auszuführenden Dienst zuweisen, nachdem Sie den Dienst erstellt haben.

Eigenschaft	Beschreibung
Primärer Knoten	Wenn die Lizenz hohe Verfügbarkeit einschließt, ist dies der Knoten, auf dem der Dienst standardmäßig ausgeführt wird. Erforderlich, wenn Sie eine Lizenz mit hoher Verfügbarkeit ausgewählt haben.
Backup-Knoten	Wenn die Lizenz hohe Verfügbarkeit einschließt, sind dies die Knoten, auf denen der Dienst ausgeführt werden kann, wenn der primäre Knoten nicht verfügbar ist.

4. Klicken Sie auf **Weiter**.
5. Geben Sei auf der Seite **Neuer PowerCenter-Integrationsdienst – Schritt 2 von 2** die folgenden Eigenschaften ein:

Eigenschaft	Beschreibung
PowerCenter-Repository-Dienst	PowerCenter-Repository-Dienst, der dem Dienst zugeordnet werden soll.
Benutzername	Benutzername, den der Dienst für den Zugriff auf den PowerCenter-Repository-Dienst verwendet. Geben Sie den PowerCenter-Repository-Benutzer ein, den Sie erstellt haben. Erforderlich, wenn Sie dem Dienst einen PowerCenter-Repository-Dienst zuordnen. Nicht verfügbar für eine Domäne mit Kerberos-Authentifizierung.
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. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Er darf weder mehr als 128 Zeichen enthalten noch mit @ beginnen. Außerdem darf er weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Beschreibung	Beschreibung des Diensts. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Domäne und Ordner, in der/dem der Dienst erstellt wurde. Um einen anderen Ordner auszuwählen, klicken Sie auf **Durchsuchen**. Sie können den Dienst nach dessen Erstellung verschieben.
Lizenz	Lizenzobjekt für die Verwendung des Diensts.
Knoten	Knoten, auf dem der Dienst ausgeführt wird.

4. Geben Sie die folgenden Eigenschaften des zugehörigen Repository-Dienstes:

Eigenschaft	Beschreibung
Zugehöriger Integrationsdienst	Wählen Sie den PowerCenter-Integrationsdienst aus, über den der Metadata Manager Metadaten in das Metadata Manager-Warehouse lädt.
Repository-Benutzername	Benutzername, den der Dienst für den Zugriff auf den PowerCenter-Repository-Dienst verwendet. Geben Sie den PowerCenter-Repository-Benutzer ein, den Sie erstellt haben. Erforderlich, wenn Sie dem Dienst einen PowerCenter-Repository-Dienst zuordnen. Nicht verfügbar für eine Domäne mit Kerberos-Authentifizierung.
Repository-Passwort	Dem PowerCenter-Repository-Benutzer zugeordnetes Passwort. Nicht verfügbar für eine Domäne mit Kerberos-Authentifizierung.
Sicherheitsdomäne	LDAP-Sicherheitsdomäne für den Benutzer des PowerCenter-Repository. Das Feld **Sicherheitsdomäne** wird eingeblendet, wenn die Informatica-Domäne eine LDAP-Sicherheitsdomäne enthält. Erforderlich, wenn Sie dem Dienst einen PowerCenter-Repository-Dienst zuordnen. Nicht verfügbar für eine Domäne mit Kerberos-Authentifizierung.

5. Klicken Sie auf **Weiter**.

   Die Seite **Neuer Metadata Manager-Dienst – Schritt 2 von 3** wird angezeigt.

6. Geben Sie die folgenden Datenbankeigenschaften für das Metadata Manager-Repository ein:

Eigenschaft	Beschreibung
Datenbanktyp	Der Typ der Repository-Datenbank.
Codepage	Codepage für 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.
Verbindungszeichenfolge	Native Verbindungszeichenfolge für die Metadata Manager-Repository-Datenbank. Der Metadata Manager-Dienst verwendet die Verbindungszeichenfolge, um ein Verbindungsobjekt zum Metadata Manager-Repository im PowerCenter-Repository zu erstellen. Verwenden Sie die folgende native Syntax der Verbindungszeichenfolge für jede unterstützte Datenbank: - `servername@databasename` für Microsoft SQL Server - `databasename.world` für Oracle - `databasename` für IBM DB2
Datenbankbenutzer	Der Datenbankbenutzername für das Repository.
Datenbankpasswort	Passwort für den Metadata Manager-Repository-Datenbankbenutzer. Muss in 7-Bit-ASCII kodiert sein.
Tablespace-Name	Name des Tablespace, in dem alle Repository-Datenbanktabellen erstellt werden sollen. Sie können im Tablespace-Namen keine Leerzeichen verwenden. Für IBM DB2-Datenbanken. Um die Repository-Leistung bei IBM DB2 EEE-Repositorys zu verbessern, geben Sie einen Tablespace-Namen mit einem Knoten an.
Datenbankhostname	Name des Computers, der als Host für den Datenbankserver dient.
Datenbankport	Die Portnummer, mit der Sie den Listenerdienst für den Datenbankserver konfigurieren.
SID/Dienstname	Für Oracle-Datenbanken. Gibt an, ob die SID oder der Dienstname in der JDBC-Verbindungszeichenfolge verwendet werden soll. Für Oracle RAC-Datenbanken wählen Sie Oracle-SID oder Oracle-Dienstname. Für andere Oracle-Datenbanken wählen Sie die Oracle-SID aus.
Datenbankname	Der Name des Datenbankservers. Geben Sie den vollständigen Dienstnamen oder die SID für Oracle-Datenbanken, den Dienstnamen für IBM DB2-Datenbanken und den Datenbanknamen für Microsoft SQL Server-Datenbanken an.

7. Wenn Sie Parameter an die Datenbankverbindungs-URL anhängen, konfigurieren Sie zusätzliche Parameter im Feld **Zusätzliche JDBC-Parameter**. Geben Sie die Parameter als Name = Wertpaare, getrennt durch ein Semikolon (;) ein. Beispiel: `param1=value1;param2=value2`

Sie können diese Eigenschaft verwenden, um die folgenden Parameter anzugeben:

Parameter	Beschreibung
Speicherort des Sicherungsservers	Wenn Sie einen hochverfügbaren Datenbankserver wie zum Beispiel Oracle RAC verwenden, geben Sie den Speicherort eines Sicherungsservers ein.
Oracle ASO (Advanced Security Option)-Parameter	Wenn die Metadata Manager-Repository-Datenbank eine Oracle-Datenbank ist, die ASO verwendet, geben Sie die folgenden zusätzlichen Parameter ein: `EncryptionLevel=[encryption level];EncryptionTypes=[encryption types];DataIntegrityLevel=[data integrity level];DataIntegrityTypes=[data integrity types]` **Hinweis:** Die Parameterwerte müssen den Werten in der Datei `sqlnet.ora` auf dem Computer entsprechen, auf dem der Metadata Manager-Dienst ausgeführt wird.

Authentifizierungsinformationen für Microsoft SQL Server	Zum Authentifizieren der Benutzeranmeldedaten und Einrichten einer vertrauenswürdigen Verbindung zu einem Microsoft SQL Server-Repository geben Sie den folgenden Text ein:
	`AuthenticationMethod=ntlm;LoadLibraryPath=[directory containing DDJDBCx64Auth04.dll].`
	`jdbc:informatica:sqlserver://[host]:[port];DatabaseName=[DB name];AuthenticationMethod=ntlm;LoadLibraryPath=[directory containing DDJDBCx64Auth04.dll]`
	Wenn Sie eine vertrauenswürdige Verbindung verwenden, um eine Verbindung zu einer Microsoft SQL Server-Datenbank herzustellen, stellt der Metadata Manager-Dienst eine Verbindung zum Repository mit den Anmeldeinformationen des Benutzers her, der auf dem Computer angemeldet ist, auf dem der Dienst ausgeführt wird.
	Um den Metadata Manager-Dienst als Windows-Dienst mithilfe einer vertrauenswürdigen Verbindung zu starten, konfigurieren Sie die Eigenschaften des Windows-Dienstes so, dass die Anmeldung mit einem vertrauenswürdigen Benutzerkonto erfolgt.

8. Wenn das Metadata Manager-Repository für die sichere Kommunikation konfiguriert ist, können Sie zusätzliche JDBC-Parameter im Feld **Sichere JDBC-Parameter** konfigurieren.

   Verwenden Sie diese Eigenschaft, um sichere Verbindungsparameter wie Passwörter anzugeben. Das Administrator Tool zeigt keine sicheren Parameter bzw. die Parameterwerte in den Eigenschaften des Metadata Manager-Diensts an. Geben Sie die Parameter als Name = Wertpaare, getrennt durch ein Semikolon (;) ein. Beispiel: `param1=value1;param2=value2`.
   Geben Sie die folgenden sicheren Datenbankparameter ein:

Sicherer Datenbankparameter	Beschreibung
EncryptionMethod	Erforderlich. Gibt an, ob Daten bei der Netzwerkübertragung verschlüsselt werden. Dieser Parameter muss auf `SSL` festgelegt werden.
TrustStore	Erforderlich. Pfad und Dateiname der TrustStore-Datei, die das SSL-Zertifikat des Datenbankservers enthält.
TrustStorePassword	Erforderlich. Passwort für den Zugriff auf die Truststore-Datei.

Sicherer Datenbankparameter	Beschreibung
HostNameInCertificate	Hostname des Computers, auf dem die sichere Datenbank gehostet wird. Wenn Sie einen Hostnamen angeben, vergleicht der Metadata Manager-Dienst den Hostnamen in der Verbindungszeichenfolge mit dem Hostnamen im SSL-Zertifikat.
ValidateServerCertificate	Optional. Gibt an, ob Informatica das Zertifikat validiert, das der Datenbankserver sendet. Wenn dieser Parameter auf TRUE gesetzt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat. Wenn Sie den HostNameInCertificate-Parameter angeben, validiert Informatica ebenfalls den Hostnamen im Zertifikat. Wenn dieser Parameter auf FALSE gesetzt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat nicht. Informatica ignoriert alle Truststore-Informationen, die Sie angeben.
KeyStore	Pfad und Dateiname der Schlüsselspeicherdatei mit den SSL-Zertifikaten, die der Metadata Manager-Dienst an den Datenbankserver sendet.
KeyStorePassword	Passwort für den Zugriff auf die Schlüsselspeicherdatei.

9. Klicken Sie auf **Weiter.**

   Die Seite **Neuer Metadata Manager-Dienst – Schritt 3 von 3** wird angezeigt.

10. Geben Sie die HTTP-Portnummer für den Dienst ein.

11. Zum Aktivieren der sicheren Kommunikation mit dem Metadata Manager-Dienst wählen Sie **Secured Socket Layer aktivieren** aus.

    Geben Sie die folgenden Eigenschaften ein, um die sichere Kommunikation für den Dienst zu konfigurieren:

Eigenschaft	Beschreibung
HTTPS-Port	Zu verwendende Portnummer für eine sichere Verbindung zum Dienst. Verwenden Sie eine Portnummer, die sich von der HTTP-Portnummer unterscheidet.
Schlüsselspeicherdatei	Pfad und Dateiname der Schlüsselspeicherdatei, die die privaten oder öffentlichen Schlüsselpaare und die zugeordneten Zertifikate enthält. Erforderlich, wenn Sie HTTPS-Verbindungen für den Dienst verwenden.
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-Diensts erstellen Sie die Repository-Tabellen und importieren Modelle für Metadatenquellen.

1. Wählen Sie im Navigator den Metadata Manager-Dienst aus.
2. Klicken Sie auf **Aktionen** > **Repository-Inhalte** > **Erstellen**.
3. Klicken Sie auf **OK**.

Nach dem Erstellen des Metadata Manager-Dienstes erstellen Sie die Anwendungsdienste, die vom Metadata Manager-Dienst abhängig sind.

Erstellen und Konfigurieren des 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 Referenztabellen und externen Datenquellen übertragen. Der Content-Managementdienst enthält auch Umwandlungen, Mapping-Spezifikationen und Regelspezifikationen mit den folgenden Typen von Referenzdaten:

- Adressreferenzdaten
- Identitätspopulationen
- Probabilistische Modelle und Klassifizierungsmodelle
- Referenztabellen

Erstellen des Content-Management-Diensts

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

Stellen Sie vor dem Erstellen des Content-Management-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** > **Content-Management-Dienst**.

   Das Dialogfeld **Neuer Content-Management-Dienst** wird angezeigt.

3. Geben Sie auf der Seite **Neuer Content-Management-Dienst – Schritt 1 von 2** die folgenden Eigenschaften ein:

Eigenschaft	Beschreibung
Name	Name des Diensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Er darf weder mehr als 128 Zeichen enthalten noch mit @ beginnen. Außerdem darf er weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Beschreibung	Beschreibung des Diensts. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Domäne und Ordner, in der/dem der Dienst erstellt wurde. Um einen anderen Ordner auszuwählen, klicken Sie auf **Durchsuchen**. Sie können den Dienst nach dessen Erstellung verschieben.
Lizenz	Lizenzobjekt für die Verwendung des Diensts.
Knoten	Knoten, auf dem der Dienst ausgeführt wird.
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. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Er darf weder mehr als 128 Zeichen enthalten noch mit @ beginnen. Außerdem darf er weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Beschreibung	Beschreibung des Diensts. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Domäne und Ordner, in der/dem der Dienst erstellt wurde. Um einen anderen Ordner auszuwählen, klicken Sie auf **Durchsuchen**. Sie können den Dienst nach dessen Erstellung verschieben.
Lizenz	Lizenzobjekt für die Verwendung des Diensts.
Knoten	Knoten, auf dem der Dienst ausgeführt wird.

4. Klicken Sie auf **Weiter**.

   Die Seite **Neuer Analyst-Dienst – Schritt 2 von 6** wird angezeigt.
5. Geben Sie die HTTP-Portnummer für die Kommunikation des Analyst Tools mit dem Analyst-Dienst ein.
6. Zum Aktivieren der sicheren Kommunikation zwischen dem Analyst Tool und dem Analyst-Dienst wählen Sie **Sichere Kommunikation aktivieren** aus.

Geben Sie folgende Eigenschaften ein, um die sichere Kommunikation für den Analyst-Dienst zu konfigurieren:

Eigenschaft	Beschreibung
HTTPS-Port	Portnummer, auf der das Analyst Tool bei Aktivierung der sicheren Kommunikation ausgeführt wird. Verwenden Sie eine Portnummer, die sich von der HTTP-Portnummer unterscheidet.
Schlüsselspeicherdatei	Verzeichnis, in dem die Schlüsselspeicherdatei gespeichert wird, die die digitalen Zertifikate enthält.
Schlüsselspeicherpasswort	Klartext-Passwort für die Schlüsselspeicherdatei. Wenn diese Eigenschaft nicht festgelegt ist, verwendet der Analyst-Dienst das Standardpasswort `changeit`.
SSL-Protokoll	Optional. Gibt das zu verwendende Protokoll an. Legen Sie diese Eigenschaft auf `SSL` fest.

7. Wählen Sie **Dienst aktivieren** aus.

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

8. Klicken Sie auf **Weiter**.

   Die Seite **Neuer Analyst-Dienst – Schritt 3 von 6** wird angezeigt.

9. Geben Sie die folgenden Eigenschaften ein, um den Modellrepository-Dienst mit dem Analyst-Dienst zu verbinden:

Beschreibung	Eigenschaft
Modellrepository-Dienst	Modellrepository-Dienst zum Zuweisen zum Dienst.
Benutzername	Benutzername, den der Dienst für den Zugriff auf den Modellrepository-Dienst verwendet. Geben Sie den Modellrepository-Benutzer ein, den Sie erstellt haben.
Passwort	Passwort für den Modellrepository-Benutzer.
Sicherheitsdomäne	LDAP-Sicherheitsdomäne für den Benutzer des Modellrepository. Das Feld wird angezeigt, wenn die Informatica-Domäne eine LDAP-Sicherheitsdomäne enthält. Nicht verfügbar für eine Domäne mit Kerberos-Authentifizierung.

10. Damit Benutzer des Analyst Tool mit Human-Task-Daten arbeiten können, legen Sie die **Datenintegrationsdienst**-Eigenschaft mit dem Datenintegrationsdienst fest, den Sie für das Ausführen von Arbeitsabläufen konfigurieren.

    Wenn die Benutzer des Analyst Tools keine Human Task-Datensätze bearbeiten müssen, konfigurieren Sie diese Eigenschaft nicht.

11. Klicken Sie auf **Weiter**.

    Die Seite **Neuer Analyst-Dienst – Schritt 4 von 6** wird angezeigt.

12. Geben Sie die folgenden Laufzeiteigenschaften für den Analyst-Dienst ein:

Eigenschaft	Beschreibung
Datenintegrationsdienst	Datenintegrationsdienst für die Zuordnung zum Dienst. Der Analyst-Dienst verwaltet die Verbindung zu einem Datenintegrationsdienst, mit dem Benutzer Datenvorschau-, Mappingspezifikations-, Scorecard- und Profil-Jobs im Analyst Tool durchführen können. Sie können den Analyst-Dienst mit dem Datenintegrationsdienst verbinden, den Sie für die Ausführung von Arbeitsabläufen konfiguriert haben. Oder Sie können den Analyst-Dienst für verschiedene Vorgänge verschiedenen Datenintegrationsdiensten zuordnen.
Verzeichnis des Einfachdatei-Cache	Verzeichnis des Einfachdatei-Cache, in dem das Analyst Tool hochgeladene Einfachdateien speichert. Der Datenintegrationsdienst muss auch in der Lage sein, auf dieses Verzeichnis zuzugreifen. Wenn der Analyst-Dienst und der Datenintegrationsdienst auf verschiedenen Knoten ausgeführt werden, konfigurieren Sie das Einfachdateiverzeichnis zur Verwendung eines freigegebenen Verzeichnisses.

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. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Er darf weder mehr als 128 Zeichen enthalten noch mit @ beginnen. Außerdem darf er weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Beschreibung	Beschreibung des Diensts. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Domäne und Ordner, in der/dem der Dienst erstellt wurde. Um einen anderen Ordner auszuwählen, klicken Sie auf **Durchsuchen**. Sie können den Dienst nach dessen Erstellung verschieben.
Lizenz	Lizenzobjekt für die Verwendung des Diensts.
Knoten	Knoten, auf dem der Dienst ausgeführt wird.

4. Klicken Sie auf **Weiter**.

   Die Seite **Neuer Suchdienst – Schritt 2 von 2** wird angezeigt.
5. Geben Sie die folgenden Sucheigenschaften für den Suchdienst ein:

Beschreibung	Eigenschaft
Portnummer	Die Portnummer für den Suchdienst.
Indexspeicherort	Das Verzeichnis, das die Suchindex-Dateien enthält. Geben Sie ein Verzeichnis auf dem Computer ein, auf dem der Suchdienst ausgeführt wird. Wenn das Verzeichnis nicht existiert, erstellt Informatica das Verzeichnis beim Erstellen des Suchdienstes.
Extraktionsintervall	Das Intervall in Sekunden, in dem der Suchdienst aktualisierten Inhalt extrahiert und indiziert. Standardwert ist 60 Sekunden.
Modellrepository-Dienst	Modellrepository-Dienst zum Zuweisen zum Dienst.

Beschreibung	Eigenschaft
Benutzername	Benutzername, den der Dienst für den Zugriff auf den Modellrepository-Dienst verwendet. Geben Sie den Modellrepository-Benutzer ein, den Sie erstellt haben.
Passwort	Passwort für den Modellrepository-Benutzer.
Sicherheitsdomäne	LDAP-Sicherheitsdomäne für den Benutzer des Modellrepository. Das Feld wird angezeigt, wenn die Informatica-Domäne eine LDAP-Sicherheitsdomäne enthält. Nicht verfügbar für eine Domäne mit Kerberos-Authentifizierung.

6. Klicken Sie auf **Fertig stellen**.

   Die Domäne erstellt den Suchdienst. Die Domäne aktiviert den Suchdienst während des Diensterstellungsprozesses nicht. Sie müssen den Dienst aktivieren, bevor Benutzer Suchen im Analyst-Tool und im Business Glossary-Desktop durchführen können.

7. Wählen Sie zum Aktivieren des Suchdienstes den Dienst im Navigator aus und klicken Sie auf **Aktionen** > **Dienst aktivieren**.

   Sie können den Suchdienst nur aktivieren, wenn der Modellrepository-Dienst, der Datenintegrationsdienst und der Analyst-Dienst ausgeführt werden.

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

Erstellen und Konfigurieren des Metadaten-Zugriffsdiensts

Der Metadaten-Zugriffsdienst ist ein Anwendungsdienst, mit dem das Developer Tool auf die Hadoop-Umgebung zugreifen kann, um Metadaten zu importieren und in der Vorschau anzuzeigen. Wenn die Domäne eine Nicht-Kerberos-Authentifizierung verwendet, können Sie den Metadaten-Zugriffsdienst erstellen und konfigurieren. Wenn die Domäne die Kerberos-Authentifizierung verwendet, erstellen Sie den Metadaten-Zugriffsdienst nicht.

Um den Metadaten-Zugriffsdienst zu erstellen, verwenden Sie den Diensterstellungs-Assistenten im Administrator Tool. Geben Sie bei entsprechender Aufforderung die erforderlichen Dienstinformationen an, wie z. B. die Lizenz, den Speicherort und den Knoten, auf dem der Dienst ausgeführt wird.

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** > **Metadaten-Zugriffsdienst**.

   Der Assistent **Neuer Metadaten-Zugriffsdienst** wird angezeigt.

5. Geben Sie auf der Seite **Neuer Metadaten-Zugriffsdienst – Schritt 1 von 3** die folgenden Eigenschaften ein:

Eigenschaft	Beschreibung
Name	Name des Diensts. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Er darf weder mehr als 128 Zeichen enthalten noch mit @ beginnen. Außerdem darf er weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Beschreibung	Beschreibung des Diensts. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Domäne und Ordner, in der/dem der Dienst erstellt wurde. Um einen anderen Ordner auszuwählen, klicken Sie auf **Durchsuchen**. Sie können den Dienst nach dessen Erstellung verschieben.
Lizenz	Lizenzobjekt für die Verwendung des Diensts.
Knoten	Knoten, auf dem der Dienst ausgeführt wird.
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.

6. Klicken Sie auf **Weiter**.

   Die Seite **Neuer Metadaten-Zugriffsdienst – Schritt 2 von 3** wird angezeigt.
7. Wählen Sie den Protokolltyp HTTP aus und geben Sie die entsprechende Portnummer ein, die für den Metadaten-Zugriffsdienst verwendet werden soll.
8. Akzeptieren Sie für die restlichen Sicherheitseigenschaften die Standardwerte. Sie können die Sicherheitseigenschaften nach dem Erstellen des Metadaten-Zugriffsdiensts konfigurieren.
9. Wählen Sie **Dienst aktivieren** aus.

   Der Metadaten-Zugriffsdienst weist keine anderen Dienstabhängigkeiten auf.
10. Klicken Sie auf **Weiter**.

    Die Seite **Neuer Metadaten-Zugriffsdienst – Schritt 3 von 3** wird angezeigt.
11. Geben Sie gegebenenfalls die Ausführungsoptionen für Benutzer für den Identitätswechsel, Kerberos-Cluster sowie Protokollierungsoptionen an und klicken Sie auf **Weiter**.
12. Klicken Sie auf **Fertig stellen**.

    Die Domäne erstellt und aktiviert den Metadaten-Zugriffsdienst.

Teil V: Installation des Informatica-Client

Dieser Teil enthält die folgenden Kapitel:

KAPITEL 13

Installieren der Clients

Dieses Kapitel umfasst die folgenden Themen:

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.

Verify Installer Package Checksum

Before you run the client installer, verify the install package integrity through the cksum command. The cksum command calculates the checksum value for the installer.

Verify the checksum for the specific installer files against the checksum of the installation files downloaded from the Informatica Electronic Software Download site.

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

Datei	Prüfsummenwert	Dateigröße
informatica_1053_client_winem-64t.zip	590321451	3139423400

A checksum mismatch can occur when there are data errors during download due to network issues or when data corruption occurs in the file on disk. For more information about the checksum errors, see 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. If you want to install distribution packages through the Informatica installer, select the check box.
7. If you choose to install distribution packages, select one or more packages from the list that you want to install.
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 Repositorys, die eine UTF-8-Codepage nutzen, müssen unter Windows weitere Sprachen für die Verwendung mit den Informatica-Clients installiert werden.

Außerdem müssen Sie Sprachen für die Verwendung des Windows Input Method Editor (IME) installieren.

1. Klicken Sie auf **Starten** > **Einstellungen** > **Systemsteuerung**.
2. Klicken Sie auf **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.

Sie müssen unter Umständen die folgenden Umgebungsvariablen auf allen Client-Hosts einrichten:

INFA_TRUSTSTORE

Legen Sie diese Variable auf das Verzeichnis fest, das die Truststore-Dateien für die SSL-Zertifikate enthält. Das Verzeichnis muss Truststore-Dateien mit der Bezeichnung `infa_truststore.jks` und `infa_truststore.pem` enthalten.

INFA_TRUSTSTORE_PASSWORD

Legen Sie diese Variable auf das Passwort für die Datei `infa_truststore.jks` fest. Das Passwort muss verschlüsselt werden. Verwenden Sie das Befehlszeilenprogramm pmpasswd zum Verschlüsseln des Passworts.

Informatica stellt ein SSL-Zertifikat zur Verfügung, das Sie zum Sichern der Domäne verwenden können. Wenn Sie die Informatica-Clients installieren, legt das Installationsprogramm die Umgebungsvariablen fest und installiert die TrustStore-Dateien standardmäßig im folgenden Verzeichnis: `<Informatica-Installationsverzeichnis>\clients\shared\security`.

Wenn Sie das SSL-Standardzertifikat von Informatica verwenden und `infa_truststore.jks` und `infa_truststore.pem` sich im Standardverzeichnis befinden, brauchen Sie die Umgebungsvariablen INFA_TRUSTSTORE oder INFA_TRUSTSTORE_PASSWORD nicht festzulegen.

Sie müssen die Umgebungsvariablen INFA_TRUSTSTORE und INFA_TRUSTSTORE_PASSWORD auf allen Client-Hosts in folgenden Szenarien einrichten:

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.

Wichtig: Wenn Sie die Verarbeitung an einen Computecluster übergeben und der Datenintegrationsdienst in einem Gitter ausgeführt wird, importieren Sie die Zertifikate einmal und kopieren Sie sie dann auf jeden Datenintegrationsdienst im Gitter. Bei jedem Import eines Zertifikats stimmen die Inhalte des Zertifikats überein, die Hexwerte sind jedoch verschieden. Deshalb schlagen gleichzeitige Zuordnungen im Gitter mit Initialisierungsfehlern fehl.

Konfigurieren des Workspace-Verzeichnisses für das Developer-Tool

Konfigurieren Sie Informatica Developer so, dass die Workspace-Metadaten in den Computer geschrieben werden, auf dem der Benutzer angemeldet ist.

1. Wechseln Sie zum folgenden Verzeichnis: `<Informatica-Installationsverzeichnis>\clients\DeveloperClient\configuration\`
2. Suchen Sie die Datei config.ini.
3. Erstellen Sie eine Sicherungskopie der Datei config.ini.
4. Öffnen Sie die Datei config.ini in einem Texteditor.
5. Fügen Sie die Variable `osgi.instance.area.default` an das Ende der Datei config.ini an, und stellen Sie die Variable auf den Verzeichnisort ein, wo Sie die Workspace-Metadaten speichern möchten. Der Dateipfad darf keine Nicht-ANSI-Zeichen enthalten. Ordnernamen im Workspace-Verzeichnis dürfen nicht das Nummernzeichen (#) enthalten. Wenn Ordnernamen im Workspace-Verzeichnis Leerzeichen enthalten, umschließen Sie das gesamte Verzeichnis mit doppelten Anführungszeichen.
   - Wenn Sie Informatica Developer vom lokalen Computer aus ausführen, stellen Sie die Variable auf den absoluten Pfad des Workspace-Verzeichnisses ein:

     ```
     osgi.instance.area.default=<Drive>/<WorkspaceDirectory>
     ```

     oder

     ```
     osgi.instance.area.default=<Drive>\\<WorkspaceDirectory>
     ```
   - Wenn Sie Informatica Developer von einem Remote-Computer aus ausführen, stellen Sie die Variable auf den Verzeichnisort des lokalen Computers ein:

     ```
     osgi.instance.area.default=\\\\<LocalMachine>/<WorkspaceDirectory>
     ```

     oder

     ```
     osgi.instance.area.default=\\\\<LocalMachine>\\<WorkspaceDirectory>
     ```

     Der Benutzer muss über eine Schreibberechtigung für das Workspace-Verzeichnis verfügen.

Informatica Developer schreibt die Workspace-Metadaten in das Workspace-Verzeichnis. Wenn Sie sich in Informatica Developer von einem lokalen Computer aus anmelden, schreibt Informatica Developer die Workspace-Metadaten in den lokalen Computer. Wenn das Workspace-Verzeichnis nicht auf dem Computer existiert, auf dem Sie angemeldet sind, erstellt Informatica Developer das Verzeichnis beim Schreiben der Dateien.

Sie können das Workspace-Verzeichnis überschreiben, wenn Sie Informatica Developer starten.

Starten von PowerCenter Client

Beim Starten von PowerCenter Client wird eine Verbindung zu einem PowerCenter-Repository hergestellt.

1. Klicken Sie im Windows-Startmenü auf **Programme** > **Informatica[Version]** > **Client** > **[Name des Client-Tools]**.

   Beim ersten Ausführen eines PowerCenter Client-Tools müssen Sie ein Repository hinzufügen und eine Verbindung dazu herstellen
2. Klicken Sie auf **Repository** > **Repository hinzufügen**.

   Das Dialogfeld **Repository hinzufügen** wird angezeigt.
3. Geben Sie den Repository- und den Benutzernamen ein.

4. Klicken Sie auf **OK**.

   Das Repository wird im Navigator angezeigt.
5. Klicken Sie auf **Repository** > **Verbinden**.

   Das Dialogfeld für das Verbinden mit dem Repository wird angezeigt.
6. Klicken Sie im Abschnitt mit den Verbindungseinstellungen auf **Hinzufügen**, um die Informationen zur Domänenverbindung einzugeben.

   Das Dialogfeld **Domäne hinzufügen** wird angezeigt.
7. Geben Sie den Domänennamen, den Gateway-Host und die Gateway-Portnummer ein.
8. Klicken Sie auf **OK**.
9. Geben Sie in das Dialogfeld **Mit Repository verbinden** das Passwort für den Administrator-Benutzer ein.
10. Wählen Sie die Sicherheitsdomäne.
11. Klicken Sie auf **Verbinden**.

    Nachdem die Verbindung zum Repository hergestellt wurde, können Sie Objekte erstellen.

Starten des Developer Tools

Beim Starten des Developer Tools wird eine Verbindung zu einem Model-Repository hergestellt. Im Model-Repository werden im Developer Tool erstellte Metadaten gespeichert. Der Model Repository Service verwaltet das Model Repository. Stellen Sie daher eine Verbindung zum Repository her, bevor Sie ein Projekt erstellen.

1. Klicken Sie im Windows-Startmenü auf **Programme** > **Informatica[Version]** > **Client** > **Developer Client** > **Informatica Developer starten**.

   Beim ersten Ausführen des Developer Tools wird die Begrüßungsseite mit mehreren Symbolen angezeigt. Beim nachfolgenden Ausführen des Developer Tools wird die Begrüßungsseite nicht mehr angezeigt.
2. Klicken Sie auf **Workbench.**

   Beim ersten Starten des Entwiocklertools müssen Sie das Repository auswählen, in dem die Objekte, die Sie erstellen, gespeichert werden sollen
3. Klicken Sie auf **Datei** > **Mit Repository verbinden**.

   Das Dialogfeld **Mit Repository verbinden** wird eingeblendet.
4. Wenn Sie im Developer Tool keine Domäne konfiguriert haben, klicken Sie auf **Domänen konfigurieren**, um eine Domäne zu konfigurieren.

   Sie müssen eine Domäne konfigurieren, um auf einen Model Repository Service zugreifen zu können.
5. Klicken Sie auf **Hinzufügen**, um eine Domäne hinzuzufügen.

   Das Dialogfeld **Neue Domäne** wird eingeblendet
6. Geben Sie den Domänennamen, den Hostnamen und die Portnummer ein.
7. Klicken Sie auf **Fertigstellen**.
8. Klicken Sie auf **OK**.
9. Klicken Sie im Dialogfeld **Mit Repository verbinden** auf **Durchsuchen** und wählen Sie den Model Repository Service aus.
10. Klicken Sie auf **OK**.

11. Klicken Sie auf **Weiter**.
12. Geben Sie einen Benutzernamen und ein Passwort ein.
13. Klicken Sie auf **Fertigstellen**.

    Das Model Repository wird der Objekt-Explorer-Ansicht hinzugefügt. Beim nächsten Ausführen des Developer-Tools können Sie eine Verbindung zum selben Repository herstellen.

KAPITEL 14

Installation im automatischen Modus

Dieses Kapitel umfasst die folgenden Themen:

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.

Configure the Properties File

Informatica provides a sample properties file that includes the properties required by the installer. Customize the sample properties file to create a properties file and specify the options for your installation. Then run the silent installation.

The sample SilentInput.properties file is stored in the installer download location.

1. Go to the root of the directory that contains the installation files.
2. Locate the sample `SilentInput.properties` file.
3. Create a backup copy of the SilentInput.properties file.

4. Use a text editor to open and modify the values of the properties in the file.

   The following table describes the installation properties that you can modify:

Property Name	Description
INSTALL_TYPE	Indicates whether to install or upgrade the Informatica clients. If the value is 0, the Informatica clients are installed in the directory you specify. If the value is 1, the Informatica clients are upgraded. Default is 0.
USER_INSTALL_DIR	Informatica client installation directory.
DXT_COMP	Indicates whether to install Informatica Developer. If the value is 1, the Developer tool will be installed. If the value is 0, the Developer tool will not be installed. Default is 1.
INSTALL_HADOOP_LIBRARIES	Determines whether to install distribution packages through the installer. Set the value to true if you want to install distribution packages through the installer. Set the value to false if you don't need distribution packages or if you want to install them later.
SELECTED_HADOOP_LIBRARIES	Determines the distribution packages that you want to install from the supported packages list. Enter the distribution packages that you want to install, separating multiple packages with a comma.

5. Save the properties file.

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

KAPITEL 15

Deinstallation

Dieses Kapitel umfasst die folgenden Themen:

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 von mithilfe der Informatica Developer Platform-APIs erstellten Drittanbieteradaptern benötigt werden, der folgende Ordner erstellt:
  `<Informatica-Installationsverzeichnis>/services/shared/extensions`

  Bei der Deinstallation des Informatica-Servers werden dieser Ordner und alle erstellten Unterordner gelöscht. Wenn Sie 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-Ordner 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

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 Beispieleigenschaftendatei 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

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 und Stoppen 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: Wenn Sie den Speicherort von infaservice.sh mithilfe eines Softlinks festlegen, stellen Sie die Umgebungsvariable INFA_HOME auf den Speicherort des Informatica-Installationsverzeichnisses 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**.

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:

Managing Distribution Packages Overview

You can use Integration Package Manager (the package manager) to install and remove distribution packages from the Informatica service and client machines.

A distribution package is a set of distribution binaries that you install within the domain for the following processing requirements:

- To push processing to the Hadoop or Databricks environment.
- To process complex files within the Informatica domain.
- To connect to the Hadoop or Databricks environment when you process within the Informatica domain.

You can install distribution packages if you didn't do so during the upgrade or install process or if you want to add a distribution package. You can remove a distribution package if you want to use a different package or if you installed a package that you don't use.

When you install or remove distribution packages, verify that you perform the operation on all service and client machines.

Before You Begin

Before you run the package manager, perform tasks such as setting environment variables and downloading files.

1. Shut down the Informatica services.

2. Set one of the following environment variables:

Variable	Description
INFA_JDK_HOME	Location of the folder containing the supported Java Development Kit (JDK). Set the INFA_JDK_HOME environment variable in the following scenarios: - Informatica domain is on Windows or Linux - Informatica client
INFA_JRE_HOME	Location of the folder containing the supported Java Runtime Environment (JRE). If the Informatica domain is on AIX, set the INFA_JRE_HOME environment variable.

3. Verify that the user that runs the package manager has read and write permissions on the Informatica installation directory and execute permissions on the executable file.
4. Download the following files from the Informatica Electronic Software Download site:
   - Integration Package Manager
   - Distribution packages
5. Extract the Integration Package Manager ZIP files to a local drive.
6. Copy the ZIP files of distribution packages that you need to the following location: `<Integration Package Manager directory>/source`

   Hinweis: The package manager fails if the ZIP files for distribution packages aren't available in the source directory.

Install or Remove Distribution Packages in Console Mode

You can run the package manager in console mode to install or remove distribution packages.

1. From the package manager directory, run one of the following commands:
   - `./Server.sh console` for Linux or UNIX
   - `Server.bat console` for Windows
   - `Client.bat console` for client

   Hinweis: To run the command on Windows, use the administrator command prompt.
2. Enter the installation directory of the services or client and press **Enter**.
3. Choose the operation type and press **Enter**.
   - Select 1 to remove existing distribution packages.
   - Select 2 to install one or more distribution packages.

   The console lists the distribution packages that you can install or remove.
4. Enter the distribution packages that you want to install or remove, separating multiple packages with a comma, and press **Enter**.
5. Verify the installation or removal status in the package manager log file.

   You can find the log file in the following location: `<Integration Package Manager directory>/IntegrationPackageManager_<date and timestamp>.log`

Install or Remove Distribution Packages in Silent Mode

You can run the package manager in silent mode to install or remove distribution packages. The silent input properties file contains the properties for the package manager to run in silent mode for service and clients. Set the appropriate value for each property in the file.

1. Find the IntegrationPackageManager.properties file in the following location: `<Integration Package Manager directory>/`
2. Edit the properties file in a text editor.

   The following table describes the properties that you can modify:

Property Name	Description
USER_INSTALL_DIR	The installation directory of the service or client.
OPERATION_TYPE	The operation that you want to perform: - Set to DELETE to remove existing distribution packages. - Set to EXTRACT to install one or more distribution packages.
SELECTED_HADOOP_LIBRARIES	Lists the distribution packages and versions. Enter the distribution packages that you want to install or remove. Separate multiple packages with a comma.

3. Save the properties file.
4. From the package manager directory, run one of the following commands:
   - `./Server.sh silent` for Linux or UNIX
   - `Server.bat silent` for Windows
   - `Client.bat silent` for client

   Hinweis: To run the command on Windows, use the administrator command prompt.
5. Verify the installation or removal status in the package manager log file.

   You can find the log file in the following location: `<Integration Package Manager directory>/IntegrationPackageManager_<date and timestamp>.log`

After You Install

To use the distribution packages that are installed using the package manager, configure the property or environment variable in service and client machines.

Configure the Developer Tool

After you install the distribution packages in the Developer tool, update the developerCore.ini file with the installed distribution package.

1. Find the developerCore.ini file in the following location: `<Informatica installation directory>\clients\DeveloperClient`

2. Edit the file to update the following property:

   ```
   -DINFA_HADOOP_DIST_DIR=hadoop\<Hadoop distribution name>_<version>
   ```

   For example,

   ```
   -DINFA_HADOOP_DIST_DIR=hadoop\CDH_7.1
   ```

3. Restart the Developer tool.

Configure Environment Variables

Some adapters require environment variables for the Data Integration Service and Metadata Access Service to access the distribution packages. For more information, see 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

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.

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 bei Aktivierung der SSL-Verschlüsselung gesendete Zertifikat validiert. Legen Sie den Wert für den Treiber auf 1 fest, um das Serverzertifikat zu validieren.

Attribut	Beschreibung
TrustStore	Der Speicherort und der Name der Truststore-Datei. Die Truststore-Datei enthält eine Liste mit Zertifizierungsstellen, die der Treiber für die SSL-Serverauthentifizierung verwendet.
TrustStorePassword	Das Passwort für den Zugriff auf den Inhalt der Truststore-Datei.
HostNameInCertificate	Optional. Der Hostname, der vom SSL-Administrator für den Treiber eingerichtet ist, um den im Zertifikat enthaltenen Hostnamen zu validieren.

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.

TNS_ADMIN. Wenn sich die Datei tnsnames.ora nicht in demselben Speicherort wie das Oracle-Installationsverzeichnis befindet, legen Sie die TNS_ADMIN-Umgebungsvariable tnsnames.ora für das Verzeichnis fest, in dem sich die Datei tnsnames.ora befindet. Wenn sich die Datei beispielsweise im Verzeichnis /HOME2/oracle/files befindet, legen Sie die Variable wie folgt fest:

Bei Verwendung einer Bourne-Shell:

```
$ TNS_ADMIN=$HOME2/oracle/files; export TNS_ADMIN
```

Bei Verwendung einer C-Shell:

```
$ setenv TNS_ADMIN=$HOME2/oracle/files
```

Hinweis: Die Datei `tnsnames.ora` ist standardmäßig in folgendem Verzeichnis gespeichert: `$ORACLE_HOME/network/admin`.

PATH. Zum Ausführen der Oracle-Befehlszeilenprogramme, legen Sie die Variable so fest, dass sie das Oracle-bin-Verzeichnis enthält.

Bei Verwendung einer Bourne-Shell:

```
$ PATH=${PATH}:$ORACLE_HOME/bin; export PATH
```

Bei Verwendung einer C-Shell:

```
$ setenv PATH ${PATH}:ORACLE_HOME/bin
```

3. Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek fest.

   Die Oracle-Clientsoftware enthält eine Reihe von gemeinsam genutzten Bibliothekskomponenten, die die Datenintegrationsdienst-, PowerCenter-Integrationsdienst- und PowerCenter-Repository-Dienst-Prozesse dynamisch laden. Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek fest, um die gemeinsam genutzten Bibliotheken während der Laufzeit zu suchen.

   Der Pfad der gemeinsam genutzten Bibliothek muss außerdem das Informatica-Installationsverzeichnis `(server_dir)` enthalten.

   Legen Sie die Umgebungsvariable der gemeinsamen Bibliothek auf LD_LIBRARY_PATH fest.

   Verwenden Sie zum Beispiel die folgende Syntax:

   - Bei Verwendung einer Bourne-Shell:

     ```
     $ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:$HOME/server_dir:$ORACLE_HOME/lib; export LD_LIBRARY_PATH
     ```

   - Bei Verwendung einer C-Shell:

     ```
     $ setenv LD_LIBRARY_PATH ${LD_LIBRARY_PATH}:$HOME/server_dir:$ORACLE_HOME/lib
     ```

4. Bearbeiten Sie die .cshrc- oder die .profile-Datei, um den gesamten Satz der Shell-Befehle einzubeziehen. Speichern Sie die Datei und melden Sie sich entweder erneut an oder führen Sie den Quellbefehl aus.

   Bei Verwendung einer Bourne-Shell:

   ```
   $ source .profile
   ```

   Bei Verwendung einer C-Shell:

   ```
   $ source .cshrc
   ```

5. Vergewissern Sie sich, dass der Orcale-Client so konfiguriert ist, dass er auf die Datenbank zugreifen kann.

   Verwenden Sie das Dienstprogramm SQL*Net Easy Configuration oder kopieren Sie eine bestehende `tnsnames.ora`-Datei in das Basisverzeichnis und verändern Sie diese.

   Die Datei `tnsnames.ora` ist in folgendem Verzeichnis gespeichert: `$ORACLE_HOME/network/admin`.

Geben Sie die richtige Syntax für die Oracle-Verbindungszeichenfolge ein. Diese lautet normalerweise `databasename.world`.

Hier ist eine `tnsnames.ora`-Beispieldatei. Geben Sie die Informationen für die Datenbank ein.

```
mydatabase.world =
   (DESCRIPTION
   (ADDRESS_LIST =
        (ADDRESS =
           (COMMUNITY = mycompany.world
           (PROTOCOL = TCP)
           (Host = mymachine)
           (Port = 1521)
        )
   )
   (CONNECT_DATA =
      (SID = MYORA7)
      (GLOBAL_NAMES = mydatabase.world)
```

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=inrh74ocm.mycompany.com)(port=1521))
(address=(protocol=tcp)(host=inrh74oradb.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.

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. 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 enthalten eine Richtlinie zum Konfigurieren der ODBC-Konnektivität. Spezifische Anweisungen finden Sie in der Dokumentation zur Datenbank.

1. Um die Konnektivität für den Integration-Service-Prozess zu konfigurieren, melden Sie sich am Computer als Benutzer an, der einen Dienstprozess starten kann.
2. Setzen Sie die Umgebungsvariablen TERADATA_HOME, ODBCHOME und PATH.

TERADATA_HOME. Legen Sie die Variable so fest, dass sie auf das Installationsverzeichnis des Teradata-Treibers verweist. Die Standardeinstellungen sind wie folgt:

Bei Verwendung einer Bourne-Shell:

```
$ TERADATA_HOME=/opt/teradata/client/<version>; export TERADATA_HOME
```

Bei Verwendung einer C-Shell:

```
$ setenv TERADATA_HOME /opt/teradata/client/<version>
```

ODBCHOME. Legen Sie die Variable so fest, dass sie auf das ODBC-Installationsverzeichnis verweist. Beispiel:

Bei Verwendung einer Bourne-Shell:

```
$ ODBCHOME=$INFA_HOME/ODBC<version>; export ODBCHOME
```

Bei Verwendung einer C-Shell:

```
$ setenv ODBCHOME $INFA_HOME/ODBC<version>
```

PATH. Um das Hilfsprogramm *ddtestlib* auszuführen, damit überprüft wird, ob der DataDirect ODBC-Treibermanager die Treiberdateien laden kann, legen Sie die Variable folgendermaßen fest:

Bei Verwendung einer Bourne-Shell:

```
PATH="${PATH}:$ODBCHOME/bin:$TERADATA_HOME/bin"
```

Bei Verwendung einer C-Shell:

```
$ setenv PATH ${PATH}:$ODBCHOME/bin:$TERADATA_HOME/bin
```

3. Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek fest.

   Die Teradata-Clientsoftware enthält mehrere gemeinsam genutzte Bibliothekkomponenten, die der Integrationsdienst-Prozess dynamisch lädt. Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek so fest, dass die Dienste die gemeinsam genutzten Bibliotheken zur Laufzeit suchen können.

   Der Pfad der gemeinsam genutzten Bibliothek muss außerdem das Installationsverzeichnis des Informatica-Dienstes *(server_dir)* enthalten.

   Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek basierend auf dem Betriebssystem fest.

   In der folgenden Tabelle werden die Variablen der gemeinsam genutzten Bibliothek für jedes Betriebssystem beschrieben:

Betriebssystem	Variable
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
```

4. Bearbeiten Sie die vorhandene odbc.ini-Datei oder kopieren Sie die odbc.ini-Datei in das Basisverzeichnis und bearbeiten Sie sie.

   Die Datei befindet sich im Verzeichnis $ODBCHOME.

   ```
   $ cp $ODBCHOME/odbc.ini $HOME/.odbc.ini
   ```

   Fügen Sie einen Eintrag zu der Teradata-Datenquelle unter dem Abschnitt [ODBC-Datenquellen] hinzu und konfigurieren Sie die Datenquelle.

   Beispiel für Teradata Parallel Transporter-Dienstprogramme der Version 15.10:

   ```
   MY_TERADATA_SOURCE=Teradata Driver
   [MY_TERADATA_SOURCE]
   Driver=/opt/teradata/client/15.10/lib64/tdata.so
   Description=NCR 3600 running Teradata V1R5.2
   DBCName=208.199.59.208
   DateTimeFormat=AAA
   SessionMode=ANSI
   DefaultDatabase=
   Username=
   Password=
   ```

   Beispiel für Teradata Parallel Transporter-Dienstprogramme der Version 16.20:

   ```
   MY_TERADATA_SOURCE=Teradata Driver
   [dwtera]
   Driver=/opt/teradata/client/16.20/lib64/tdataodbc_sb64.so
   Description=NCR 3600 running Teradata V1R5.2
   DBCName=tdvbe1510
   LastUser=
   Username=
   Password=
   Database=
   DefaultDatabase=
   UseNativeLOBSupport=Yes
   CharacterSet=UTF8
   SessionMode=ANSI
   ```

5. Setzen Sie das DateTimeFormat in der Teradata-Daten-ODBC-Konfiguration auf AAA.
6. Optional können Sie den SessionMode auf ANSI setzen. Wenn Sie den ANSI-Sitzungsmodus verwenden, führt Teradata bei einem Zeilenfehler kein Rollback der Transaktion aus.

   Wenn Sie den Teradata-Sitzungsmodus verwenden, führt Teradata bei einem Zeilenfehler ein Rollback der Transaktion aus. Der Integration-Service-Prozess kann im Teradata-Modus das Rollback nicht entdecken und meldet dies nicht im Sitzungs-Log.
7. Um eine Verbindung zu einer einzelnen Teradata-Datenbank zu konfigurieren, geben Sie den Namen der Standarddatenbank ein. Um eine einzelne Verbindung zu der Standard-Datenbank herzustellen, geben Sie den Benutzernamen und das Passwort ein. Lassen Sie das Feld für die Standarddatenbank leer, um eine Verbindung zu mehreren Datenbanken mit dem gleichen ODBC-DSN herzustellen.

   Weitere Informationen zur Teradata-Konnektivität finden Sie in der Teradata-ODBC-Treiber-Dokumentation.
8. Prüfen Sie, ob der letzte Eintrag in der odbc.ini-Datei InstallDir ist und lassen Sie ihn auf das ODBC-Installationsverzeichnis verweisen.

Beispiel:

```
InstallDir=<Informatica installation directory>/ODBC<version>
```

9. Bearbeiten Sie die .cshrc- oder die .profile-Datei, um den gesamten Satz der Shell-Befehle einzubeziehen.
10. Speichern Sie die Datei und melden Sie sich entweder erneut an oder führen Sie den Quellbefehl aus.

    Bei Verwendung einer Bourne-Shell:

    ```
    $ source .profile
    ```

    Bei Verwendung einer C-Shell:

    ```
    $ source .cshrc
    ```

11. Machen Sie sich für jede Datenquelle, die Sie verwenden, eine Notiz des Dateinamens unter „Driver=<parameter>“ in dem Datenquelleneintrag in odbc.ini. Verwenden Sie das Hilfsprogramm *ddtestlib*, um sicherzustellen, dass der DataDirect ODBC-Treibermanager die Treiberdatei laden kann.

    Sie haben zum Beispiel den Treibereintrag:

    ```
    Driver=/u01/app/teradata/td-tuf611/odbc/drivers/tdata.so
    ```

    Führen Sie den folgenden Befehl aus:

    ```
    ddtestlib /u01/app/teradata/td-tuf611/odbc/drivers/tdata.so
    ```

12. Testen Sie die Verbindung mit BTEQ oder einem anderen Teradata-Client-Tool.

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 Bibliothekkomponenten, die die Dienstprozesse dynamisch laden. Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek so fest, dass die Dienste die gemeinsam genutzten Bibliotheken zur Laufzeit suchen können.

   Der Pfad der gemeinsam genutzten Bibliothek muss außerdem das Informatica-Installationsverzeichnis *(server_dir)* enthalten.

   Legen Sie die Umgebungsvariable der gemeinsam genutzten Bibliothek basierend auf dem Betriebssystem fest.

   In der folgenden Tabelle werden die Variablen der gemeinsam genutzten Bibliothek für jedes Betriebssystem beschrieben:

Betriebssystem	Variable
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_SQLSERVER_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=odbctrace.out
TraceDll=/<Informatica installation directory>/ODBC7.1/lib/DWtrc27.so

[DB2 Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWdb227.so
Description=DataDirect 7.1 DB2 Wire Protocol
AccountingInfo=
AddStringToCreateTable=
AlternateID=
AlternateServers=
ApplicationName=
ApplicationUsingThreads=1
AuthenticationMethod=0
BulkBinaryThreshold=32
BulkCharacterThreshold=-1
BulkLoadBatchSize=1024
BulkLoadFieldDelimiter=
BulkLoadRecordDelimiter=
CatalogSchema=
CharsetFor65535=0
ClientHostName=
ClientUser=
#Collection applies to z/OS and iSeries only
Collection=
ConcurrentAccessResolution=0
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
CurrentFuncPath=
#Database applies to DB2 UDB only
```

```
Database=<database_name>
DefaultIsolationLevel=1
DynamicSections=1000
EnableBulkLoad=0
EncryptionMethod=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
GrantAuthid=PUBLIC
GrantExecute=1
GSSClient=native
HostNameInCertificate=
IpAddress=<DB2_server_host>
KeyPassword=
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
#Location applies to z/OS and iSeries only
Location=<location_name>
LogonID=
MaxPoolSize=100
MinPoolSize=0
Password=
PackageCollection=NULLID
PackageNamePrefix=DD
PackageOwner=
Pooling=0
ProgramID=
QueryTimeout=0
ReportCodePageConversionErrors=0
TcpPort=50000
TrustStore=
TrustStorePassword=
UseCurrentSchema=0
ValidateServerCertificate=1
WithHold=1
XMLDescribeType=-10

[Informix Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWifcl27.so
Description=DataDirect 7.1 Informix Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
CancelDetectInterval=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
HostName=<Informix_host>
LoadBalancing=0
LogonID=
Password=
PortNumber=<Informix_server_port>
ServerName=<Informix_server>
TrimBlankFromIndexName=1
UseDelimitedIdentifiers=0

[Oracle Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/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>
TimestampeEscapeMapping=0
TNSNamesFile=<tnsnames.ora_filename>
TrustStore=
TrustStorePassword=
UseCurrentSchema=1
ValidateServerCertificate=1
WireProtocolMode=2

[Sybase Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWase27.so
Description=DataDirect 7.1 Sybase Wire Protocol
AlternateServers=
ApplicationName=
```

```
ApplicationUsingThreads=1
ArraySize=50
AuthenticationMethod=0
BulkBinaryThreshold=32
BulkCharacterThreshold=-1
BulkLoadBatchSize=1024
BulkLoadFieldDelimiter=
BulkLoadRecordDelimiter=
Charset=
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
CursorCacheSize=1
Database=<database_name>
DefaultLongDataBuffLen=1024
EnableBulkLoad=0
EnableDescribeParam=0
EnableQuotedIdentifiers=0
EncryptionMethod=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
GSSClient=native
HostNameInCertificate=
InitializationString=
Language=
LoadBalancing=0
LoadBalanceTimeout=0
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
NetworkAddress=<Sybase_host,Sybase_server_port>
OptimizePrepare=1
PacketSize=0
Password=
Pooling=0
QueryTimeout=0
RaiseErrorPositionBehavior=0
ReportCodePageConversionErrors=0
SelectMethod=0
ServicePrincipalName=
TruncateTimeTypeFractions=0
TrustStore=
TrustStorePassword=
ValidateServerCertificate=1
WorkStationID=

[SQL Server Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWsqls28.so
Description=DataDirect 8.0 SQL Server Wire Protocol
AlternateServers=
AlwaysReportTriggerResults=0
AnsiNPW=1
ApplicationName=
ApplicationUsingThreads=1
AuthenticationMethod=1
BulkBinaryThreshold=32
BulkCharacterThreshold=-1
BulkLoadBatchSize=1024
BulkLoadOptions=2
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
EnableBulkLoad=0
EnableQuotedIdentifiers=0
EncryptionMethod=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
```

```
FetchTSWTZasTimestamp=0
FetchTWFSasTime=1
GSSClient=native
HostName=<SQL_Server_host>
HostNameInCertificate=
InitializationString=
Language=
LoadBalanceTimeout=0
LoadBalancing=0
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
PacketSize=-1
Password=
Pooling=0
PortNumber=<SQL_Server_server_port>
QueryTimeout=0
ReportCodePageConversionErrors=0
SnapshotSerializable=0
TrustStore=
TrustStorePassword=
ValidateServerCertificate=1
WorkStationID=
XML Describe Type=-10

[MySQL Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWmysql27.so
Description=DataDirect 7.1 MySQL Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
DefaultLongDataBuffLen=1024
EnableDescribeParam=0
EncryptionMethod=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
HostName=<MySQL_host>
HostNameInCertificate=
InteractiveClient=0
LicenseNotice=You must purchase commercially licensed MySQL database software or
a MySQL Enterprise subscription in order to use the DataDirect Connect for ODBC
for MySQL Enterprise driver with MySQL software.
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
LogonID=
LoginTimeout=15
MaxPoolSize=100
MinPoolSize=0
Password=
Pooling=0
PortNumber=<MySQL_server_port>
QueryTimeout=0
ReportCodepageConversionErrors=0
TreatBinaryAsChar=0
TrustStore=
TrustStorePassword=
ValidateServerCertificate=1

[PostgreSQL Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWpsql27.so
Description=DataDirect 7.1 PostgreSQL Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
ConnectionReset=0
```

```
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
DefaultLongDataBuffLen=2048
EnableDescribeParam=1
EncryptionMethod=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
FetchTSWTZasTimestamp=0
FetchTWFSasTime=0
HostName=<Greenplum_host>
InitializationString=
KeyPassword=
KeysetCursorOptions=0
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
Password=
Pooling=0
PortNumber=<Greenplum_server_port>
QueryTimeout=0
```

```
ReportCodepageConversionErrors=0
TransactionErrorBehavior=1
XMLDescribeType=-10
```

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.

ANHANG D

Aktualisieren des DynamicSections-Parameters einer DB2-Datenbank

Dieser Anhang umfasst die folgenden Themen:

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;ReplacePackag
   e=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

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z