Informatica®
9.6.1 HotFix 4

Handbuch für Sicherheit

Informatica Handbuch für Sicherheit
9.6.1 HotFix 4
März 2016

Publikationsdatum: 2018-06-09

Inhalt

Einleitung

Das Informatica-Handbuch für Sicherheit enthält Informationen über die Sicherheit in der Informatica-Domäne. Es enthält wichtige Informationen zum Verwalten der Sicherheit in der Informatica-Domäne und in den Informatica-Clients, die eine Verbindung zur Domäne herstellen. In diesem Handbuch wird vorausgesetzt, dass Sie mit der Informatica-Domäne und dem Informatica Administrator vertraut sind. Außerdem wird vorausgesetzt, dass Sie mit den Authentifizierungsservern und -Prozessen für Ihr Netzwerk vertraut sind.

Informatica-Ressourcen

Informatica-Portal „My Support“

Als Informatica-Kunde haben Sie Zugriff auf das „My Support“-Portal unter http://mysupport.informatica.com.

Die Site enthält Produktinformationen, Benutzergruppeninformationen sowie Newsletters und bietet Zugriff auf das Informatica-Verwaltungssystem für den Kundensupport (ATLAS), die Informatica How-To Library, die Informatica-Wissensdatenbank, die Informatica-Produktdokumentation und die Informatica User Community.

Die Site enthält Produktinformationen, Benutzergruppeninformationen sowie Newsletters und bietet Zugriff auf die Informatica How-To Library, die Informatica-Wissensdatenbank, die Informatica-Produktdokumentation und die Informatica User Community.

Informatica-Dokumentation

Das Informatica-Dokumentationsteam ist sehr um genaue, nützliche Dokumentationen bemüht. Wenn Sie Fragen, Kommentare oder Ideen zu dieser Dokumentation haben, wenden Sie sich bitte per E-Mail an das Informatica-Dokumentationsteam unter infa_documentation@informatica.com. Mithilfe Ihrer Rückmeldungen können wir unsere Dokumentationen verbessern. Bitte teilen Sie uns mit, ob wir Sie bezüglich Ihrer Kommentare kontaktieren dürfen.

Das Dokumentationsteam aktualisiert die Dokumentation nach Bedarf. Um die neueste Dokumentation zu erhalten, navigieren Sie von http://mysupport.informatica.com zur Produktdokumentation.

Informatica-Produktverfügbarkeitsmatrizen

Produktverfügbarkeitsmatrizen (PAMs) geben die Versionen der Betriebssysteme, Datenbanken und anderen Typen von Datenquellen und Zielen an, die in einer Produktversion unterstützt werden. Der Zugriff auf die PAMs erfolgt über das Informatica My Support-Portal unter https://mysupport.informatica.com/community/my-support/product-availability-matrices.

Informatica-Website

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

Informatica How-To Library

Als Informatica-Kunde können Sie auf die Informatica How-To Library unter http://mysupport.informatica.com zugreifen. Die Informatica How-To Library ist eine Ressourcensammlung, die Ihnen hilft, mehr über Informatica-Produkte und -Funktionen zu erfahren. Sie umfasst Artikel und interaktive Demonstrationen, die Lösungen für häufige Probleme bieten, Funktionen und Verhaltensweisen vergleichen und Sie durch spezifische realitätsnahe Aufgaben führen.

Informatica-Wissensdatenbank

Als Informatica-Kunde können Sie auf die Informatica-Wissensdatenbank unter http://mysupport.informatica.com zugreifen. In der Knowledge-Datenbank können Sie nach dokumentierten Lösungen zu bekannten technischen Problemen mit Informatica-Produkten suchen. Außerdem finden Sie dort Antworten auf häufig gestellte Fragen sowie technische Whitepapers und Tipps. Wenn Sie Fragen, Kommentare oder Ideen zur Knowledge-Datenbank haben, wenden Sie sich bitte per E-Mail an das Informatica-Wissensdatenbankteam unter KB_Feedback@informatica.com.

YouTube-Kanal des Informatica-Supports

Den vom Informatica-Supportteam betreuten YouTube-Kanal erreichen Sie unter http://www.youtube.com/user/INFASupport. Der YouTube-Kanal des Informatica-Supports bietet verschiedene Videos, die Ihnen erklären, wie Sie spezifische Aufgaben erfolgreich bewältigen. Wenn Sie Fragen, Anregungen oder Ideen zum YouTube-Kanal des Informatica-Supports haben, wenden Sie sich per E-Mail an das YouTube-Team der Supportabteilung unter supportvideos@informatica.com oder senden Sie einen Tweet an @INFASupport.

Informatica Marketplace

Der Informatica Marketplace ist ein Forum, in dem Entwickler und Partner Lösungen zur Steigerung, Erweiterung oder Verbesserung der Implementierungen von Datenintegrationen teilen können. Hunderte von Lösungen im Marketplace bieten Ihnen die Möpglichkeit, Ihre Produktivität zu steigern und die Implementierung in Ihre Projekte zu beschleunigen. Zugriff auf den Informatica Marketplace erhalten Sie unter http://www.informaticamarketplace.com.

Informatica Velocity

Der Zugang zu Informatica Velocity erfolgt über http://mysupport.informatica.com. Informatica Velocity basiert auf der Praxiserfahrung aus Hunderten von Datenmanagementprojekten und umfasst das kollektive Wissen unserer Berater, die mit Unternehmen aus der ganzen Welt an der Planung, Entwicklung, Bereitstellung und Wartung erfolgreicher Datenmanagementlösungen gearbeitet haben. Wenn Sie Fragen, Anregungen oder Ideen zu Informatica Velocity haben, wenden Sie sich an die professionellen Informatica-Dienste unter ips@informatica.com.

Informatica – Weltweiter Kundensupport

Sie können sich telefonisch oder über den Online-Support an ein Kundensupport-Center wenden.

Der Online-Support erfordert einen Benutzernamen und ein Passwort. Sie erhalten einen Benutzernamen und ein Passwort unter http://mysupport.informatica.com.

Die Telefonnummern für den globalen Kundensupport von Informatica (Informatica Global Customer Support) finden Sie auf der Informatica-Website unter http://www.informatica.com/us/services-and-training/support-services/global-support-centers/.

KAPITEL 1

Einführung in die Informatica-Sicherheit

Dieses Kapitel umfasst die folgenden Themen:

Übersicht über die Informatica-Sicherheit

Sie können die Informatica-Domäne sichern, um sich vor Gefahren in- und außerhalb des Netzwerks zu schützen, auf dem die Domäne ausgeführt wird.

Die Sicherheit für die Informatica-Domäne enthält die folgenden Sicherheitstypen:

Infrastruktur-Sicherheit

Die Infrastruktur-Sicherheit schützt die Informatica-Domäne gegen unbefugten Zugriff zu oder Änderungen von Diensten und Ressourcen in der Informatica-Domäne. Die Infrastruktur-Sicherheit beinhaltet die folgenden Aspekte:

- Schutz von übertragenen und gespeicherten Daten innerhalb der Informatica-Domäne
- Authentifizierung von Benutzern und Diensten beim Verbinden mit der Informatica-Domäne
- Sicherheit von Verbindungen für externe Komponenten, einschließlich Client-Anwendungen und relationaler Datenbanken für Repositorys, Quellen und Ziele.

Operationssicherheit

Die Operationssicherheit steuert den Zugriff auf die Daten und Dienste in der Informatica-Domäne. Die Operationssicherheit beinhaltet die folgenden Aspekte:

- Einrichten von Einschränkungen für den Benutzerzugriff auf Daten und Metadaten basierend auf der Rolle des Benutzers im Unternehmen
- Einrichten von Einschränkungen für Benutzer zum Ausführen von Vorgängen innerhalb der Informatica-Domäne basierend auf der Benutzerrolle im Unternehmen

Informatica speichert die Domänenkonfigurationsinformationen und die Liste von Benutzern, die für die Domäne im Domänenkonfigurations-Repository zugriffsberechtigt sind. Das Domänenkonfigurations-

Repository enthält auch die Gruppen, Rollen und Berechtigungen, die jedem Benutzer in der Informatica-Domäne zugewiesen sind.

Informatica organisiert die Liste der Benutzer nach Sicherheitsdomänen. Eine Sicherheitsdomäne enthält eine Sammlung von Benutzerkonten. Eine Domäne kann mehrere Sicherheitsdomänen enthalten.

Infrastruktur-Sicherheit

Zur Infrastruktursicherheit gehören Benutzer- und Dienstauthentifizierung, sichere Kommunikation innerhalb der Domäne und sichere Datenspeicherung.

Authentifizierung

Der Dienstmanager authentifiziert die Dienste, die in der Domäne ausgeführt werden, und die Benutzer, die sich bei den Informatica-Client-Tools anmelden.

Sie können die Informatica-Domäne konfigurieren, um die folgenden Authentifizierungstypen zu verwenden:

Native Authentifizierung

Die native Authentifizierung ist ein Authentifizierungsmodus, der nur für Benutzerkonten in der Informatica-Domäne verfügbar ist. Wenn die Informatica-Domäne die native Authentifizierung verwendet, speichert der Dienstmanager die Benutzeranmeldedaten und Berechtigungen im Domänenkonfigurations-Repository und führt alle Benutzerauthentifizierungen innerhalb der Informatica-Domäne durch.

Wenn die Informatica-Domäne die native Authentifizierung verwendet, enthält die Domäne eine native Sicherheitsdomäne und alle Benutzerkonten gehören zur nativen Sicherheitsdomäne.

Informatica verwendet den Benutzernamen und Passwörter, um Benutzer und Dienste in der Informatica-Domäne zu authentifizieren.

LDAP-Authentifizierung (Lightweight Directory Access Protocol)

LDAP ist ein Software-Protokoll für den Zugriff auf Benutzer und Ressourcen in einem Netzwerk. Wenn die Informatica-Domäne die LDAP-Authentifizierung verwendet, werden die Benutzerkonten und Benutzeranmeldedaten im LDAP-Verzeichnisdienst gespeichert. Die Benutzerberechtigungen werden im Domänenkonfigurations-Repository gespeichert. Sie müssen die Benutzerkonten regelmäßig im Domänenkonfigurations-Repository mit den Benutzerkonten im LDAP-Verzeichnisdienst synchronisieren.

Informatica verwendet den Benutzernamen und Passwörter, um Informatica-Benutzer und -Dienste in der Informatica-Domäne zu authentifizieren.

Kerberos-Authentifizierung

Kerberos ist ein Netzwerk-Authentifizierungsprotokoll, das Tickets zum Authentifizieren von Benutzern und Diensten in einem Netzwerk verwendet. Wenn die Informatica-Domäne die Kerberos-Authentifizierung verwendet, werden die Benutzerkonten und Benutzeranmeldedaten in der Kerberos-Prinzipaldatenbank gespeichert, bei der es sich um ein LDAP-Verzeichnisdienst handeln kann. Die Benutzerberechtigungen werden im Domänenkonfigurations-Repository gespeichert. Sie müssen die Benutzerkonten regelmäßig im Domänenkonfigurations-Repository mit den Benutzerkonten in der Kerberos-Prinzipaldatenbank synchronisieren.

Informatica verwendet die Kerberos-Tickets, um Informatica-Benutzer und -Dienste in der Informatica-Domäne zu authentifizieren.

Sichere Domänenkommunikation

Die Informatica-Domäne enthält verschiedene Optionen zum Sichern der Daten und Metadaten, die zwischen dem Dienstmanager und Diensten in der Domäne und den Client-Anwendungen übertragen werden. Informatica verwendet die TCP/IP- und HTTP-Protokolle, um zwischen Komponenten in der Domäne zu kommunizieren, und verwendet SSL-Zertifikate, um die Kommunikation zwischen Diensten und dem Dienstmanager in der Domäne zu sichern.

Das SSL/TLS-Protokoll verwendet die Verschlüsselung öffentlicher Schlüssel, um Netzwerkverkehr zu ver- und entschlüsseln. Der zum Ver- und Entschlüsseln des Verkehrs verwendete öffentliche Schlüssel ist in einem SSL-Zertifikat gespeichert, das selbstsigniert oder signiert sein kann. Ein selbstsigniertes Zertifikat wird vom Ersteller des Zertifikats signiert. Da die Identität des Unterzeichners nicht überprüft wird, ist ein selbstsigniertes Zertifikat weniger sicher als ein signiertes Zertifikat. Ein signiertes Zertifikat ist ein SSL-Zertifikat, bei dem die Identität der Person, die das Zertifikat angefordert hat, von einer Zertifizierungsstelle (CA) überprüft wird. Informatica empfiehlt von einer Zertifizierungsstelle signierte Zertifikate, um die Sicherheit zu erhöhen.

Ein Schlüsselspeicher enthält private Schlüssel und Zertifikate. Er wird verwendet, um Zugangsdaten bereitzustellen. Ein Truststore enthält das Zertifikat vertrauenswürdiger SSL/TLS-Server. Es wird verwendet, um Zugangsdaten zu überprüfen.

Informatica benötigt Schlüsselspeicher und Truststores im PEM- und JKS-Format, um Verbindungen in der Domäne zu sichern. Sie können die folgenden Programme zum Erstellen der erforderlichen Dateien verwenden:

keytool

Verwenden Sie keytool, um ein SSL-Zertifikat oder eine Zertifikatssignieranfrage sowie Schlüsselspeicher und Truststores im JKS-Format zu erstellen.

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

http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html

OpenSSL

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

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

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

Der Typ der gesicherten Verbindung bestimmt die benötigten Dateien.

Sicherer Datenspeicher

Informatica verschlüsselt vertrauliche Daten wie Passwörter und sichere Verbindungsparameter, bevor die Daten im Domänenkonfigurations-Repository gespeichert werden. Informatica speichert auch vertrauliche Dateien wie Konfigurationsdateien in einem sicheren Verzeichnis.

Operationssicherheit

Sie können Berechtigungen und Rollen zu Benutzern oder Gruppen von Benutzern zuweisen, um die Ebene des Zugriffs, über die Benutzer und Gruppen verfügen können, und den Bereich der Aktionen, die die Benutzer und Gruppen in der Domäne durchführen können, zu verwalten.

Sie können die folgenden Methoden verwenden, um den Benutzer- und Gruppenzugriff in der Domäne zu verwalten:

Berechtigungen

Berechtigungen bestimmen die Aktionen, die Benutzer in den Informatica-Client-Tools durchführen können. Sie können einen Satz von Berechtigungen zu einem Benutzer zuweisen, um den Zugriff auf die in der Domäne verfügbaren Dienste einzuschränken. Sie können Berechtigungen auch an eine Gruppe zuordnen, damit alle Benutzer in der Gruppe auf dieselben Dienste zugreifen können.

Rollen

Eine Rolle ist ein Satz von Berechtigungen, die Sie Benutzern bzw. Gruppen zuordnen können. Sie können Rollen verwenden, um Zuweisungen von Berechtigungen zu Benutzern einfacher zu verwalten. Sie können eine Rolle mit beschränkten Berechtigungen erstellen und sie Benutzern und Gruppen mit eingeschränktem Zugriff auf Domänendienste zuweisen. Sie können auch Rollen mit zugehörigen Berechtigungen erstellen, um sie Benutzern und Gruppen zuzuweisen, die dieselbe Zugriffsebene erfordern.

Berechtigungen

Berechtigungen definieren die Zugriffsebene von Benutzern für ein Objekt. Ein Benutzer, der über die Berechtigung zum Durchführen einer bestimmten Aktion verfügt, benötigt möglicherweise eine Berechtigung zum Durchführen der Aktion für ein bestimmtes Objekt. Beispiel: Zum Verwalten eines Anwendungsdienstes muss ein Benutzer über die Berechtigung verfügen, Dienste und Berechtigungen für den bestimmten Anwendungsdienst zu verwalten.

Standardmäßige Administratorgruppe

Die Informatica-Domäne verfügt über eine systemdefinierte Administratorgruppe, die alle Berechtigungen für einen Dienst enthält. Alle Benutzerkonten, die Sie zur Administrator-Gruppe hinzufügen, verfügen über Berechtigungen für alle Dienste und Objekte in der Domäne. Wenn Sie Informatica-Dienste installieren, erstellt das Installationsprogramm ein Benutzerkonto, das zur Administrator-Gruppe gehört. Für die Erstanmeldung beim Administrator-Tool können Sie das Standardadministratorkonto verwenden.

Domänenkonfigurations-Repository

Das Domänenkonfigurations-Repository enthält Informationen über die Domänenkonfiguration und Benutzerberechtigungen.

Wenn die Informatica-Domäne die native Benutzerauthentifizierung verwendet, enthält das Domänenkonfigurations-Repository auch die Benutzeranmeldedaten. Wenn die Domäne die LDAP- bzw. Kerberos-Authentifizierung verwendet, enthält das Domänenkonfigurations-Repository nicht die Benutzeranmeldedaten. Alle LDAP- und Kerberos-Benutzeranmeldedaten werden außerhalb der Informatica-Domäne, d. h. im LDAP-Verzeichnisdienst oder Kerberos-Prinzipaldatenbank, gespeichert.

Wenn Sie die Informatica-Domäne während der Installation erstellen, erstellt das Installationsprogramm ein Domänenkonfigurations-Repository in einer relationalen Datenbank. Sie müssen die Datenbank angeben, in

der das Domänenkonfigurations-Repository erstellt werden soll. Sie können das Repository in einer mit dem SSL-Protokoll gesicherten Datenbank erstellen.

Sicherheitsdomäne

Eine Sicherheitsdomäne ist eine Sammlung von Benutzerkonten und Gruppen in der Informatica-Domäne.

Die Informatica-Domäne kann die folgenden Typen von Sicherheitsdomänen enthalten:

Native Sicherheitsdomäne

Die native Sicherheitsdomäne enthält die Benutzer und Gruppen, die im Administrator-Tool erstellt und verwaltet werden. Informatica speichert alle Anmeldedaten für Benutzerkonten in der nativen Sicherheitsdomäne im Domänenkonfigurations-Repository. Standardmäßig wird die native Sicherheitsdomäne während der Installation erstellt. Nach der Installation können Sie weder zusätzliche native Sicherheitsdomänen erstellen noch die native Sicherheitsdomäne löschen.

Wenn die Informatica-Domäne die Kerberos-Authentifizierung verwendet, verwendet die Domäne nicht die native Sicherheitsdomäne.

LDAP-Sicherheitsdomäne

Eine LDAP-Sicherheitsdomäne enthält Benutzer und Gruppen, die aus einem LDAP-Verzeichnisdienst importiert werden. Wenn die Informatica-Domäne die LDAP- bzw. Kerberos-Authentifizierung verwendet, können Sie eine LDAP-Sicherheitsdomäne erstellen und Benutzer sowie Gruppen hinzufügen, die Sie aus dem LDAP-Verzeichnisdienst importieren.

Wenn Sie Informatica-Dienste installieren und eine Domäne erstellen, die die native oder LDAP-Authentifizierung verwendet, erstellt das Installationsprogramm die native Sicherheitsdomäne, jedoch keine LDAP-Sicherheitsdomäne. Sie können LDAP-Sicherheitsdomänen nach der Installation erstellen.

Wenn Sie Informatica-Dienste installieren und eine Domäne erstellen, die die Kerberos-Authentifizierung verwendet, erstellt das Installationsprogramm die folgenden LDAP-Sicherheitsdomänen:

- Interne Sicherheitsdomäne. Das Installationsprogramm erstellt eine LDAP-Sicherheitsdomäne mit dem Namen *_infaInternalNamespace*. Die Sicherheitsdomäne _infaInternalNamespace enthält das Standard-Administrator-Benutzerkonto, das Sie während der Installation erstellen. Nach der Installation können Sie Benutzer nicht zur Sicherheitsdomäne _infaInternalNamespace hinzufügen oder die Sicherheitsdomäne löschen.
- Sicherheitsdomäne des Benutzerbereichs. Das Installationsprogramm erstellt eine leere LDAP-Sicherheitsdomäne mit demselben Namen des Kerberos-Benutzerbereichs, den Sie während der Installation angeben. Nach der Installation können Sie Benutzer aus der Kerberos-Prinzipaldatenbank in die Sicherheitsdomäne des Benutzerbereichs importieren. Sie können die Sicherheitsdomäne des Benutzerbereichs nicht löschen.
  Beim Ausführen von Befehlszeilenprogrammen in einer Domäne, die Kerberos-Authentifizierung verwendet, wird als Sicherheitsdomäne standardmäßig die Sicherheitsdomäne des Benutzerbereichs angegeben, die während der Installation erstellt wird.

Sie können LDAP-Sicherheitsdomänen, unabhängig davon, ob die Informatica-Domäne die LDAP- bzw. Kerberos-Authentifizierung verwendet, auf dieselbe Weise erstellen und verwalten.

KAPITEL 2

Benutzerauthentifizierung

Dieses Kapitel umfasst die folgenden Themen:

Benutzerauthentifizierung - Übersicht

Die Benutzerauthentifizierung in der Informatica-Domäne hängt vom Authentifizierungstyp ab, den Sie beim Installieren der Informatica-Dienste konfigurieren.

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

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

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

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

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

Sie können die native Authentifizierung und LDAP-Authentifizierung zusammen in der Informatica-Domäne verwenden. Der Dienstmanager authentifiziert die Benutzer basierend auf der Sicherheitsdomäne. Wenn ein Benutzer zur nativen Sicherheitsdomäne gehört, authentifiziert der Dienstmanager den Benutzer im

Domänenkonfigurations-Repository. Wenn der Benutzer zu einer LDAP-Sicherheitsdomäne gehört, übergibt der Dienstmanager den Benutzernamen und das Passwort zur Authentifizierung an den LDAP-Server.

Sie können eine native Authentifizierung nicht mit der Kerberos-Authentifizierung verwenden. Wenn die Informatica-Domäne die Kerberos-Authentifizierung verwendet, müssen alle Benutzerkonten zu LDAP-Sicherheitsdomänen gehören. Der Kerberos-Server authentifiziert ein Benutzerkonto, wenn sich der Benutzer beim Netzwerk anmeldet. Die Informatica-Client-Anwendungen verwenden die Anmeldedaten aus der Netzwerkanmeldung, um Benutzer in der Informatica-Domäne zu authentifizieren. Native Gruppen und Rollen werden weiterhin unterstützt.

Native Benutzerauthentifizierung

Wenn die Informatica-Domäne die native Authentifizierung verwendet, speichert der Dienstmanager alle Benutzerkontoinformationen und führt alle Benutzerauthentifizierungen innerhalb der Informatica-Domäne aus. Wenn sich ein Benutzer anmeldet, verwendet der Dienstmanager die native Sicherheitsdomäne zur Authentifizierung des Benutzernamens und Passworts.

Wenn Sie die Informatica-Domäne nicht für die Verwendung der Kerberos-Netzwerk-Authentifizierung konfigurieren, enthält die Informatica-Domäne standardmäßig eine native Sicherheitsdomäne. Die native Sicherheitsdomäne wird bei der Installation erstellt und kann nicht gelöscht werden. Eine Informatica-Domäne kann nur eine native Sicherheitsdomäne besitzen. Sie können Benutzerkonten in der nativen Sicherheitsdomäne im Administrator-Tool erstellen und verwalten. Der Dienstmanager speichert die Details über die Benutzerkonten, einschließlich der Benutzeranmeldedaten und Berechtigungen, im Domänenkonfigurations-Repository.

LDAP-Benutzerauthentifizierung

Sie können die Informatica-Domäne konfigurieren, um Benutzern in einem LDAP-Verzeichnisdienst die Anmeldung bei Informatica-Client-Anwendungen zu erlauben. Die Informatica-Domäne kann die LDAP-Benutzerauthentifizierung zusätzlich zur nativen Benutzerauthentifizierung verwenden.

Um die Informatica-Domäne für die Verwendung der LDAP-Benutzerauthentifizierung zu aktivieren, müssen Sie eine Verbindung zu einem LDAP-Server einrichten und die Benutzer und Gruppen aus dem LDAP-Verzeichnisdienst angeben, die Zugriff auf die Informatica-Domäne erhalten können. Sie können das Administrator-Tool zum Einrichten der Verbindung zum LDAP-Server verwenden.

Beim Synchronisieren der LDAP-Sicherheitsdomänen mit dem LDAP-Verzeichnisdienst importiert der Dienstmanager die Liste von LDAP-Benutzerkonten mit Zugriff auf die Informatica-Domäne in die LDAP-Sicherheitsdomänen. Wenn Sie Benutzern in LDAP-Sicherheitsdomänen Berechtigungen zuweisen, speichert der Dienstmanager die Informationen im Domänenkonfigurations-Repository. Der Dienstmanager speichert die Benutzeranmeldedaten nicht im Domänenkonfigurations-Repository.

Beim Anmelden eines Benutzers übergibt der Dienstmanager den Benutzernamen und das Passwort zur Authentifizierung an den LDAP-Server.

Hinweis: Der Dienstmanager erfordert, dass LDAP-Benutzer sich mit einem Passwort bei einer Client-Anwendung anmelden, auch wenn bei einem LDAP-Verzeichnisdienst ein leeres Passwort für den anonymen Anmeldemodus zulässig ist.

Kerberos-Authentifizierung

Sie können die Informatica-Domäne so konfigurieren, dass Benutzer und Dienste auf einem Netzwerk mit der Kerberos-Netzwerkauthentifizierung authentifiziert werden.

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.

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

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

KAPITEL 3

LDAP-Sicherheitsdomänen

Dieses Kapitel umfasst die folgenden Themen:

LDAP-Sicherheitsdomänen - Übersicht

Eine LDAP-Sicherheitsdomäne enthält eine Reihe von Benutzern und Gruppen, die aus einem LDAP-Verzeichnisdienst importiert werden. Sie können eine LDAP-Sicherheitsdomäne erstellen, wenn Sie die LDAP-Benutzerauthentifizierung oder die Kerberos-Netzwerk-Authentifizierung verwenden.

Sie können LDAP-Sicherheitsdomänen konfigurieren, um die Liste von Benutzern aus einem LDAP-Verzeichnisdienst zu speichern, dem Sie Zugriff auf Informatica-Client-Anwendungen erlauben möchten. Die Sicherheitsdomäne speichert keine Anmeldedaten des Benutzerkontos. Wenn sich ein Benutzer bei einem Informatica-Client anmeldet, überprüft der Dienstmanager, ob sich das Benutzerkonto in einer Sicherheitsdomäne befindet. Wenn das Benutzerkonto zu einer LDAP-Sicherheitsdomäne gehört, authentifiziert der Dienstmanager den Benutzer mit dem LDAP-Verzeichnisdienst.

Wenn Sie Informatica-Dienste installieren und die Kerberos-Authentifizierung nicht aktivieren, erstellt das Informatica-Installationsprogramm standardmäßig die native Sicherheitsdomäne. Nach der Installation können Sie Benutzer und Gruppen zur nativen Sicherheitsdomäne hinzufügen. Wenn Sie Benutzern in einem LDAP-Verzeichnisdienst Zugriff auf Informatica-Client-Anwendungen geben möchten, können Sie LDAP-Sicherheitsdomänen zusätzlich zur nativen Sicherheitsdomäne einrichten. Konfigurieren Sie eine Verbindung zum LDAP-Server und importieren Sie die Benutzer und Gruppen in die LDAP-Sicherheitsdomänen.

Wenn Sie Informatica-Dienste installieren und die Kerberos-Authentifizierung aktivieren, erstellt das Informatica-Installationsprogramm eine LDAP-Sicherheitsdomäne mit dem Namen des Kerberos-Bereichs, den Sie während der Installation angeben. Nach der Installation können Sie eine Verbindung zum LDAP-Server konfigurieren und Benutzer und Gruppen aus dem LDAP-Verzeichnisdienst in die LDAP-Sicherheitsdomäne importieren. Wenn Sie die Kerberos-Authentifizierung verwenden, können Sie die native Sicherheitsdomäne nicht verwenden.

Einrichten einer LDAP-Sicherheitsdomäne

Sie können eine LDAP-Sicherheitsdomäne für Benutzerkonten erstellen, die Sie aus einem LDAP-Verzeichnisdienst importieren. Um verschiedene Gruppen von Benutzern zu organisieren, können Sie mehrere LDAP-Sicherheitsdomänen verwenden.

Sie können LDAP-Benutzer und -Gruppen im LDAP-Verzeichnisdienst erstellen und verwalten. Richten Sie eine Verbindung zum LDAP-Server ein und verwenden Sie Suchfilter, um die Benutzer und Gruppen anzugeben, denen Zugriff auf die Informatica-Domäne gewährt werden kann. Importieren Sie anschließend die Benutzerkonten in die LDAP-Sicherheitsdomänen. Wenn der LDAP-Server das SSL-Protokoll verwendet, müssen Sie außerdem den Speicherplatz des SSL-Zertifikats angeben.

Sie können Benutzer aus den folgenden LDAP-Verzeichnisdiensten importieren:

- Microsoft Active Directory Service

  Hinweis: Wenn Sie die Kerberos-Authentifizierung importieren, können Sie Benutzer nur aus einem Microsoft Active Directory-Verzeichnisdienst importieren.
- Sun Java System-Verzeichnisdienst
- Novell e-Directory Service
- IBM Tivoli-Verzeichnisdienst
- LDAP-Verzeichnisdienst öffnen

Nach dem Importieren von Benutzern in eine LDAP-Sicherheitsdomäne können Sie Rollen und Berechtigungen zu den Benutzern zuweisen. Sie können LDAP-Benutzerkonten zu nativen Gruppen zuzuordnen, um sie anhand ihrer Rollen in der Informatica-Domäne zu ordnen. Sie können zum Erstellen, Bearbeiten oder Löschen von Benutzern und Gruppen in einer LDAP-Sicherheitsdomäne nicht das Administrator Tool verwenden.

Verwenden Sie das Dialogfeld „LDAP-Konfiguration“, um die Verbindung zum LDAP-Verzeichnisdienst einzurichten und die LDAP-Sicherheitsdomäne zu erstellen. Sie können das Dialogfeld „LDAP-Konfiguration“ auch verwenden, um einen Synchronisationszeitplan einzurichten.

Führen Sie zum Einrichten der LDAP-Sicherheitsdomäne die folgenden Schritte durch:

1. Richten Sie die Verbindung zum LDAP-Verzeichnisdienst ein.
2. Sicherheitsdomäne konfigurieren.
3. Synchronisierungszeiten planen.

Schritt 1. Verbindung zum LDAP-Server einrichten

Konfigurieren Sie die Verbindung zum LDAP-Server, der den Verzeichnisdienst enthält, aus dem Sie die Benutzerkonten für die Informatica-Domäne importieren möchten.

Geben Sie beim Konfigurieren der Verbindung zum LDAP-Server an, dass der Dienstmanager die Groß- und Kleinschreibung bei DN-Attributen der LDAP-Benutzerkonten während der Zuordnung von Benutzern zu Gruppen in der Informatica-Domäne ignorieren muss. Wenn der Dienstmanager die Groß- und Kleinschreibung nicht ignoriert, weist der Dienstmanager möglicherweise nicht alle Benutzer zu, die zu einer Gruppe gehören.

Wenn Sie die LDAP-Verbindungseigenschaften ändern, um eine Verbindung zu verschiedenen LDAP-Verzeichnisdiensten herzustellen, stellen Sie sicher, dass die Benutzer- und Gruppenfilter in den LDAP-Sicherheitsdomänen für den neuen LDAP-Verzeichnisdienst korrekt sind. Stellen Sie sicher, dass die Filter die Benutzer und Gruppen enthalten, die Sie in der Informatica-Domäne verwenden möchten.

Zum Einrichten einer Verbindung zum LDAP-Verzeichnisdienst führen Sie die folgenden Aufgaben durch:

1. Klicken Sie im Administrator-Tool auf die Registerkarte **Sicherheit**.
2. Klicken Sie auf das Menü **Aktionen** und wählen Sie **LDAP-Konfiguration** aus.
3. Klicken Sie im Dialogfeld **LDAP-Konfiguration** auf die Registerkarte **LDAP-Konnektivität**.
4. Konfigurieren Sie die Verbindungseigenschaften für den LDAP-Server.

   Möglicherweise müssen Sie den LDAP-Administrator konsultieren, um die Informationen über den LDAP-Server zu erhalten.

   Die folgende Tabelle beschreibt die LDAP-Konfigurationseigenschaften:

Eigenschaft	Beschreibung
Servername	Name des Computers, der den LDAP-Verzeichnisdienst hostet
Port	Listenerport für den LDAP-Server. Dies ist die Portnummer für die Kommunikation mit dem LDAP-Verzeichnisdienst. Normalerweise hat der LDAP-Server die Portnummer 389. Wenn der LDAP-Server SSL nutzt, ist die Portnummer 636. Die maximale Portnummer ist 65535.
LDAP-Verzeichnisdienst	Typ des LDAP-Verzeichnisdiensts. Wählen Sie einen der folgenden Verzeichnisdienste: - Microsoft Active Directory-Dienst - Sun Java System-Verzeichnisdienst - Novell e-Directory-Dienst - IBM Tivoli-Verzeichnisdienst - LDAP-Verzeichnisdienst öffnen **Hinweis:** Wenn Sie die Kerberos-Authentifizierung verwenden, müssen Sie den Microsoft Active Directory-Dienst auswählen.
Name	Distinguished Name (DN) für den Prinzipal-Benutzer. Der Benutzername besteht häufig aus einem Common Name (CN), einer Organisation (O), und einem Land (C). Der Prinzipal-Benutzername ist ein administrativer Benutzer mit Zugriff auf das Verzeichnis. Geben Sie einen Benutzer an, der über die Berechtigung zum Lesen anderer Benutzereinträge in einem LDAP-Verzeichnisdienst verfügt. Lassen Sie die Angabe für eine anonyme Anmeldung leer. Weitere Informationen finden Sie in der Dokumentation zum LDAP-Verzeichnisdienst.
Passwort	Passwort für den Prinzipal-Benutzer. Lassen Sie die Angabe für eine anonyme Anmeldung leer. Nicht verfügbar, wenn Sie die Kerberos-Authentifizierung verwenden.
SSL-Zertifikat verwenden	Zeigt an, dass der LDAP-Server das SSL (Secure Socket Layer)-Protokoll verwendet.
LDAP-Zertifikat vertrauen	Legt fest, ob der Dienstmanager dem SSL-Zertifikat des LDAP-Servers vertrauen kann. Wenn diese Option aktiviert ist, stellt der Dienstmanager die Verbindung zum LDAP-Server ohne Überprüfung des SSL-Zertifikats her. Wenn diese Option nicht aktiviert ist, prüft der Dienstmanager, ob das SSL-Zertifikat von einer Zertifizierungsstelle signiert ist, bevor die Verbindung mit dem LDAP-Server hergestellt wird. Damit der Dienstmanager ein selbst signiertes Zertifikat als gültig anerkennen kann, geben Sie die zu verwendende Truststore-Datei und das Passwort an.
Ohne Beachtung der Groß-/Kleinschreibung	Gibt an, dass der Dienstmanager bei der Zuordnung von Benutzern zu Gruppen Groß- und Kleinschreibung bei DN-Attributen ignorieren muss. Aktivieren Sie diese Option.

Eigenschaft	Beschreibung
Gruppenmitgliedschaft sattribut	Name des Attributs, das die die Gruppenmitgliedschaft für einen Benutzer enthält. Dies ist das Attribut im LDAP-Gruppenobjekt, das die DNs der Benutzer oder Gruppen enthält, die Mitglieder einer Gruppe sind. Zum Beispiel *member* oder *memberof*.
Maximale Größe	Maximale Anzahl an Gruppen und Benutzerkonten für den Import in eine Sicherheitsdomäne. Zum Beispiel: Wenn der Wert auf 100 gesetzt ist, können Sie maximal 100 Gruppen und 100 Benutzerkonten in die Sicherheitsdomäne importieren. Wenn die Anzahl der zu importierenden Benutzer und Gruppen den Wert für diese Eigenschaft übersteigt, generiert der Dienstmanager eine Fehlermeldung und importiert keine Benutzer. Setzen Sie diese Eigenschaft auf einen höheren Wert, wenn Sie viele Benutzer und Gruppen importieren müssen. Standardwert ist „1000“.

5. Klicken Sie auf „Verbindung testen“, um sicherzustellen, dass die Verbindung zum LDAP-Server gültig ist.

Schritt 2. Konfigurieren einer Sicherheitsdomäne

Erstellen Sie eine Sicherheitsdomäne für jeden Satz von Benutzerkonten und Gruppen, die Sie aus dem LDAP-Verzeichnisdienst importieren möchten. Richten Sie Suchbasen und Filter ein, um den Satz von Benutzerkonten und Gruppen zu definieren, die in eine Sicherheitsdomäne aufgenommen werden sollen. Der Service Manager verwendet die Benutzersuchbasen und Filter zum Importieren von Benutzern und die Gruppensuchbasen zum Importieren von Gruppen. Die Service Manager importiert Gruppen und die Liste der Benutzer, die zu den Gruppen gehören. Er importiert die Gruppen, die im Gruppenfilter enthalten sind, und die Benutzerkonten, die im Benutzerfilter enthalten sind.

Die Namen der aus dem LDAP-Verzeichnisdienst zu importierenden Benutzer und Gruppen müssen den gleichen Regeln entsprechen, wie die Namen der nativen Benutzer und Gruppen. Der Service Manager importiert keine LDAP-Benutzer oder Gruppen, wenn die Namen nicht an die Regeln der nativen Benutzer- und Gruppennamen entsprechen.

Hinweis: Im Gegensatz zu nativen Benutzernamen können LDAP-Benutzernamen Groß- und Kleinschreibung unterscheiden.

Beim Einrichten des LDAP-Verzeichnisdienstes können Sie verschiedene Attribute für die eindeutige Kennung (UID) verwenden. Der Service Manager benötigt eine bestimmte UID zur Identifizierung von Benutzern in jedem LDAP-Verzeichnisdienst. Überprüfen Sie, bevor Sie die Sicherheitsdomäne konfigurieren, dass der LDAP-Verzeichnisdienst die erforderliche UID verwendet.

Die folgende Tabelle listet die erforderliche UID für jeden LDAP-Verzeichnisdienst auf:

LDAP-Verzeichnisdienst	UID
IBMTivoliDirectory	UID
Microsoft Active Directory	sAMAccountName
NovellE	UID
OpenLDAP	UID
SunJavaSystemDirectory	UID

Der Service Manager importiert nicht das LDAP-Attribut, das angibt, ob ein Benutzerkonto aktiviert oder deaktiviert ist. Sie müssen ein LDAP-Benutzerkonto im Administrator Tool aktivieren oder deaktivieren. Der Status des Benutzerkontos im LDAP-Verzeichnisdienst beeinflusst die Benutzerauthentifizierung in Anwendungs-Clients. Zum Beispiel: Ein LDAP-Benutzerkonto ist in der Informatica-Domäne aktiviert, im LDAP-Verzeichnisdienst jedoch deaktiviert. Wenn der LDAP-Verzeichnisdienst deaktivierten Benutzerkonten gestattet, sich anzumelden, dann kann sich der Benutzer bei Anwendungs-Clients anmelden. Wenn der LDAP-Verzeichnisdienst deaktivierten Benutzerkonten nicht gestattet, sich anzumelden, dann kann sich der Benutzer nicht bei Anwendungs-Clients anmelden.

Hinweis: Wenn Sie die LDAP-Verbindungseigenschaften ändern, um eine Verbindung zu einem anderen LDAP-Server herzustellen, löscht der Service Manager die vorhandenen Sicherheitsdomänen nicht. Sie müssen sicherstellen, dass die LDAP-Sicherheitsdomänen für die das neue LDAP-Server richtig sind. Ändern Sie die Benutzer-und Gruppen-Filter in den Sicherheitsdomänen oder erstellen Sie zusätzliche Sicherheitsdomänen, sodass der Dienstmanager die Benutzer und Gruppen korrekt importiert, die Sie in der Informatica-Domäne verwenden möchten.

Führen Sie zum Konfigurieren einer LDAP-Sicherheitsdomäne die folgenden Schritte durch:

1. Klicken Sie im Administrator-Tool auf die Registerkarte **Sicherheit**.
2. Klicken Sie auf das Menü **Aktionen** und wählen Sie **LDAP-Konfiguration** aus.
3. Klicken Sie im Dialogfeld **LDAP-Konfiguration** auf die Registerkarte **Sicherheitsdomänen**.
4. Klicken Sie auf **Hinzufügen**.
5. Verwenden Sie die LDAP-Abfragesyntax für die Erstellung von Filtern, um die Benutzer und Gruppen anzugeben, die in die Sicherheitsdomäne, die Sie erstellen, aufgenommen werden sollen.

   Möglicherweise müssen Sie den LDAP-Administrator konsultieren, um die Informationen zu den im LDAP-Verzeichnisdienst verfügbaren Benutzern und Gruppen zu erhalten.

   In der nachstehenden Tabelle sind die Filtereigenschaften beschrieben, die Sie für eine Sicherheitsdomäne einrichten können:

Eigenschaft	Beschreibung
Sicherheitsdomäne	Name der LDAP-Sicherheitsdomäne. Beim Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden, und er muss in der Domäne eindeutig sein. Er darf nicht länger als 128 Zeichen sein oder die folgenden Sonderzeichen enthalten: , + / < > @ ; \ % ? Der Name kann ein ASCII-Leerzeichen enthalten, jedoch nicht als erstes oder letztes Zeichen. Alle anderen Leerzeichen sind nicht zulässig.
Benutzersuchbasis	Distinguished Name (DN) des Eintrags, der als Ausgangspunkt für die Suche nach Benutzernamen im LDAP-Verzeichnisdienst dient. Die Suche findet ein Objekt im Verzeichnis anhand des Pfads im Distinguished Name des Objekts. Zum Beispiel: In Microsoft Active Directory könnte der Distinguished Name des Benutzers cn=UserName,ou=OrganizationalUnit,dc=DomainName sein, wobei die Reihe der durch dc=DomainName benannten relativen Distinguished Names die DNS-Domäne des Objekts kennzeichnet.
Benutzerfilter	Ein LDAP-Abfragestring, der die Kriterien für die Suche nach Benutzern im Verzeichnisdienst festgelegt. Der Filter kann Attributtypen, Assertionswerte und Abgleichkriterien angeben. Beispiel: `(objectclass=*)` sucht alle Objekte. `(&(objectClass=user)(!(cn=susan)))` sucht alle Benutzerobjekte außer “susan.” Weitere Informationen über Suchfilter finden Sie in der Dokumentation für den LDAP-Verzeichnisdienst:

Eigenschaft	Beschreibung
Gruppensuchbasis	Distinguished Name (DN) des Eintrags, der als Ausgangspunkt für die Suche nach Gruppennamen im LDAP-Verzeichnisdienst dient.
Gruppenfilter	Ein LDAP-Abfragestring, der die Kriterien für die Suche nach Gruppen im Verzeichnisdienst festgelegt.

6. Klicken Sie auf **Vorschau**, um eine Teilmenge der Liste von Benutzern und Gruppen anzuzeigen, die innerhalb der Filterparameter liegen.

   Wenn die Vorschau nicht den richtigen Satz von Benutzern und Gruppen zeigt, ändern Sie die Benutzer- bzw. Gruppenfilter und Suchbasen, um die richtigen Benutzer und Gruppen erhalten.
7. Um eine weitere LDAP-Sicherheitsdomäne hinzuzufügen, wiederholen Sie die Schritte 4 bis 6.
8. Zur sofortigen Synchronisation von Benutzern und Gruppen in den Sicherheitsdomänen mit den Benutzern und Gruppen im LDAP-Verzeichnisdienst klicken Sie auf **Jetzt synchronisieren**.

   Der Dienstmanager synchronisiert die Benutzer in allen LDAP-Sicherheitsdomänen mit den Benutzern im LDAP-Verzeichnisdienst. Die Dauer des Synchronisationsvorgangs hängt von der Anzahl der zu synchronisierenden Benutzer und Gruppen ab.
9. Klicken Sie zum Speichern der Sicherheitsdomänen auf **OK**.

Schritt 3. Synchronisierungszeiten planen

Sie können einen Zeitplan für den Dienstmanager erstellen, damit er die Liste der Benutzer und Gruppen in der LDAP-Sicherheitsdomäne regelmäßig mit der Liste der Benutzer und Gruppen im LDAP-Verzeichnisdienst synchronisiert.

Wichtig: Bevor Sie den Synchronisierungsprozess starten, stellen Sie sicher, dass die Datei „/etc/hosts“ einen Eintrag für den Hostnamen des LDAP-Servers enthält. Wenn der Dienstmanager den Hostnamen für den LDAP-Server nicht auflösen kann, kann die Benutzersynchronisierung fehlschlagen.

Während der Synchronisation importiert der Dienstmanager Benutzer und Gruppen aus dem LDAP-Verzeichnisdienst. Der Dienstmanager löscht alle Benutzer oder Gruppen aus der LDAP-Sicherheitsdomäne, die nicht mehr in den Suchfiltern enthalten sind, die für den Import verwendet werden.

Standardmäßig ist für den Dienstmanager keine Zeit zur Synchronisation mit dem LDAP-Verzeichnisdienst geplant. Um sicherzustellen, dass die Liste der Benutzer und Gruppen in den LDAP-Sicherheitsdomänen genau ist, können Sie einen Zeitplan erstellen, um festzulegen, wie oft am Tag der Dienstmanager die LDAP-Sicherheitsdomänen synchronisieren soll. Der Dienstmanager synchronisiert die LDAP-Sicherheitsdomänen mit dem LDAP-Verzeichnisdienst jeden Tag zu den von Ihnen festgelegten Zeiten.

Hinweis: Während der Synchronisation sperrt der Dienstmanager das Benutzerkonto, das er synchronisiert. Wenn das Benutzerkonto gesperrt ist, kann der Dienstmanager das Benutzerkonto nicht authentifizieren. Benutzer können sich möglicherweise nicht bei Anwendungs-Clients anmelden. Wenn Benutzer zu Beginn der Synchronisierung bei Anwendungs-Clients angemeldet sind, können die Benutzer möglicherweise keine Aufgaben ausführen. Die Dauer des Synchronisationsvorgangs hängt von der Anzahl der zu synchronisierenden Benutzer und Gruppen ab. Um Nutzungsunterbrechungen zu vermeiden, synchronisieren Sie die Sicherheitsdomänen während Zeiten, in denen die meisten Benutzer nicht angemeldet sind. Um mehr als 100 Benutzer oder Gruppen zu synchronisieren, aktivieren Sie das Paging des LDAP-Verzeichnisdiensts, bevor Sie die Synchronisierung ausführen. Wenn Sie das Paging für den LDAP-Verzeichnisdienst nicht aktivieren, kann die Synchronisierung fehlschlagen.

Um einen Zeitplan zum Synchronisieren der LDAP-Sicherheitsdomänen mit dem LDAP-Verzeichnisdienst einzurichten, führen Sie die folgenden Schritte durch:

1. Klicken Sie im Administrator-Tool auf die Registerkarte **Sicherheit**.
2. Klicken Sie auf das Menü **Aktionen** und wählen Sie **LDAP-Konfiguration** aus.
3. Klicken Sie im Dialogfeld **LDAP-Konfiguration** auf die Registerkarte **Zeitplan**.
4. Klicken Sie auf die Schaltfläche **Hinzufügen** (+), um eine Zeit hinzuzufügen.

   Der Zeitplan für die Synchronisierung wird ein 24-Stunden-Format verwendet.

   Sie können so viele Synchronisationszeiten am Tag hinzufügen, wie Sie benötigen. Wenn die Liste der Benutzer und Gruppen in den LDAP-Sicherheitsdomänen häufig geändert wird, können Sie einen Zeitplan für den Dienstmanager erstellen, um die Benutzer und Gruppen mehrmals täglich zu synchronisieren.
5. Zur sofortigen Synchronisation von Benutzern und Gruppen in den Sicherheitsdomänen mit den Benutzern und Gruppen im LDAP-Verzeichnisdienst klicken Sie auf **Jetzt synchronisieren**.
6. Klicken Sie zum Speichern des Synchronisationszeitplans auf **OK**.

   Hinweis: Wenn Sie die Informatica-Domäne neu starten, bevor der Dienstmanager eine Synchronisierung mit dem LDAP-Verzeichnisdienst durchführt, gehen die von Ihnen hinzugefügten Synchronisierungszeiten verloren.

Geschachtelte Gruppen im LDAP-Verzeichnisdienst verwenden

Eine LDAP-Sicherheitsdomäne kann verschachtelte LDAP-Gruppen enthalten. In den Service Manager lassen sich verschachtelte Gruppen importieren, wenn dies wie folgt erstellt wurden:

- Die Gruppen müssen unter denselben Organisationseinheiten (OE) erstellt werden.
- Definieren Sie eine Beziehung zwischen den Gruppen.

Angenommen, Sie möchten eine verschachtelte Gruppe erstellen, in der GruppeB ein Mitglied von GruppeA, und GruppeD ein Mitglied von GruppeC ist.

1. Erstellen Sie GroupA, GroupB, GroupC und GroupD innerhalb derselben Organisationseinheit.
2. Bearbeiten Sie GroupA und fügen Sie GroupB als Mitglied hinzu.
3. Bearbeiten Sie GroupC und fügen Sie GroupD als Mitglied hinzu.

LDAP-Gruppen, die auf andere Art erstellt wurden, lassen sich nicht in eine LDAP-Sicherheitsdomäne importieren.

Ein selbstsigniertes SSL-Zertifikat verwenden

Sie können die Verbindung zu einem LDAP-Server herstellen, der ein SSL-Zertifikat verwendet, das von einer Zertifizierungsstelle signiert wurde. In der Standardeinstellung, stellt der Dienstmanager keine Verbindung zu einem LDAP-Server her, der ein selbstsigniertes Zertifikat verwendet.

Wenn Sie ein selbstsigniertes Zertifikat verwenden möchten, importieren Sie dieses in eine Truststore-Datei und verwenden die Umgebungsvariable INFA_JAVA_OPTS, um die Truststore-Datei und das Passwort anzugeben:

```
setenv INFA_JAVA_OPTS -Djavax.net.ssl.trustStore=<TrustStoreFile>
-Djavax.net.ssl.trustStorePassword=<TrustStorePassword>
```

Konfigurieren Sie INFA_JAVA_OPTS unter Windows als Systemvariable.

Starten Sie den Knoten neu, damit die Änderungen wirksam werden. Der Dienstmanager greift auf die Truststore-Datei zu, um das SSL-Zertifikat zu überprüfen.

Keytool ist ein Dienstprogramm zum Erstellen und Verwalten von Schlüsseln und Zertifikaten, die zusammen mit dem Sicherheitsprotokoll SSL verwendet werden. Mit Keytool können Sie eine Truststore-Datei erstellen oder ein Zertifikat in eine vorhandene Truststore-Datei importieren. Das Keytool-Dienstprogramm befindet sich in einem der folgenden Verzeichnisse:

```
<PowerCenterClientDir>\CMD_Utilities\PC\java\bin
```

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

Die über die angegebenen Links zum Download verfügbare Software wird nicht von Informatica Corporation 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.

Löschen einer LDAP-Sicherheitsdomäne

Wenn Sie die Benutzer einer LDAP-Sicherheitsdomäne dauerhaft daran hindern möchten, auf Anwendungs-Clients zuzugreifen, können Sie die LDAP-Sicherheitsdomäne löschen. Beim Löschen einer LDAP-Sicherheitsdomäne löscht der Service Manager alle Benutzerkonten und Gruppen in der LDAP-Sicherheitsdomäne aus der Domänenkonfigurations-Datenbank.

1. Klicken Sie im Dialogfenster LDAP-Konfiguration auf die Registerkarte Sicherheitsdomänen.

   Im Dialogfenster LDAP-Konfiguration wird die Liste der Sicherheitsdomänen eingeblendet.
2. Damit gewährleistet ist, dass Sie die richtige Sicherheitsdomäne löschen, klicken Sie auf den Namen der Sicherheitsdomäne, um den zum Importieren der Benutzer und Gruppen benutzten Filter anzuzeigen, und überprüfen Sie, ob die Sicherheitsdomäne wirklich diejenige ist, die Sie löschen möchten.
3. Um die Sicherheitsdomäne zu löschen, klicken Sie auf die Schaltfläche Löschen neben der Sicherheitsdomäne.
4. Klicken Sie auf OK, um zu bestätigen, dass Sie die Sicherheitsdomäne löschen möchten.

KAPITEL 4

Einrichtung der Kerberos-Authentifizierung

Einrichtung der Kerberos-Authentifizierung

Beim Erstellen der Informatica-Domäne während der Installation können Sie die Option zum Aktivieren von Kerberos-Authentifizierung auswählen. Wenn Sie die Kerberos-Authentifizierung nicht während der Installation aktivieren, können Sie die Informatica-Befehlszeilenprogramme verwenden, um die Domäne für die Verwendung der Kerberos-Authentifizierung zu konfigurieren.

Führen Sie zum Konfigurieren der Kerberos-Authentifizierung für die Informatica-Domäne in der Befehlszeile die folgenden Schritte durch:

1. Erstellen Sie eine LDAP-Benutzerdomäne mit Benutzern aus Microsoft Active Directory.
2. Migrieren Sie native Benutzer auf eine LDAP-Sicherheitsdomäne.
3. Richten Sie die Kerberos-Konfiguration ein und kopieren Sie die Konfigurationsdatei in das Informatica-Verzeichnis.
4. Generieren Sie den SPN und den Keytab-Dateinamen in dem von der Informatica-Domäne erforderten Format.
5. Überprüfen Sie die Textdatei mit dem SPN- und Keytab-Dateiformat.
6. Erstellen Sie die SPNs und die Keytab-Dateien.
7. Konfigurieren Sie Kerberos-Authentifizierung für die Informatica-Domäne.
8. Aktualisieren Sie die Knoten in der Informatica-Domäne.
9. Aktualisieren Sie die Client-Computer.
10. Starten Sie die Informatica-Domäne und führen Sie das Administrator-Tool aus.

Nachdem Sie die Kerberos-Authentifizierung und die LDAP-Sicherheitsdomänen konfiguriert haben, stellen Sie sicher, dass die Benutzerkonten über die richtigen Berechtigungen verfügen. Stellen Sie sicher, dass die Dienste in der Domäne ordnungsgemäß funktionieren und die Benutzer sich mit Single-Sign-On anmelden können.

Hinweis: Die zur Verfügung gestellten Schritte basieren auf der Annahme, dass Sie die Informatica-Dienste ohne die Aktivierung der Kerberos-Authentifizierung installiert haben. Wenn Sie die Kerberos-Authentifizierung während der Installation aktiviert haben, führen Sie die Schritte in den Informatica-Installationshandbüchern aus.

Schritt 1. Erstellen Sie eine LDAP-Benutzerdomäne mit Benutzern aus Microsoft Active Directory

Bevor Sie die Informatica-Domäne für die Verwendung der Kerberos-Authentifizierung konfigurieren, überprüfen Sie die Domänen-Benutzerkonten. Stellen Sie sicher, dass sich diese in LDAP-Sicherheitsdomänen befinden und dass die Konten vom Microsoft Active Directory-Dienst importiert werden.

Wenn die Domäne über Benutzerkonten in einer LDAP-Sicherheitsdomäne verfügt, die Microsoft Active Directory nicht verwendet, migrieren Sie die Benutzer auf eine LDAP-Sicherheitsdomäne, die Microsoft Active Directory verwendet. Weitere Informationen zur Migration von Benutzerkonten auf Microsoft Active Directory finden Sie in Ihrer LDAP-Implementierung.

Wenn die Domäne über Benutzerkonten in der nativen Sicherheitsdomäne verfügt, migrieren Sie die Benutzer auf eine LDAP-Sicherheitsdomäne, die Microsoft Active Directory verwendet.

Richten Sie eine LDAP-Sicherheitsdomäne ein und konfigurieren Sie die Verbindung zum Microsoft Active Directory-Dienst. Richten Sie dann die Filter für die Benutzer und Gruppen ein und synchronisieren Sie die Domänen-Benutzerkonten.

Weitere Informationen zum Einrichten einer LDAP-Domäne und zum Synchronisieren der Benutzerkonten finden Sie unter “Einrichten einer LDAP-Sicherheitsdomäne” auf Seite 22.

Schritt 2. Migrieren von nativen Benutzerrechten und -berechtigungen auf eine LDAP-Sicherheitsdomäne

Nachdem Sie die Domäne für die Verwendung der Kerberos-Authentifizierung konfiguriert haben, können Sie Benutzerkonten in der systemeigenen Sicherheitsdomäne nicht bearbeiten. Migrieren Sie die nativen Benutzer, Gruppen, Rollen und Berechtigungen auf eine LDAP-Sicherheitsdomäne, bevor Sie die Kerberos-Authentifizierung konfigurieren.

Wenn die Domäne über Benutzerkonten in der nativen Sicherheitsdomäne verfügt, müssen die entsprechenden Benutzerkonten in der LDAP-Sicherheitsdomäne über dieselben Gruppen, Rollen und Berechtigungen verfügen. Migrieren Sie die Gruppen, Rollen und Berechtigungen für die nativen Benutzer auf die Active Directory-Benutzer in der LDAP-Sicherheitsdomäne. Stellen Sie anschließend sicher, dass die migrierten Gruppen, Rollen und Berechtigungen ordnungsgemäß funktionieren.

Wenn die Domäne keine Benutzerkonten in der systemeigenen Sicherheitsdomäne enthält, können Sie mit “Schritt 3. Einrichten der Kerberos-Konfigurationsdatei” auf Seite 34 fortfahren.

Um die Gruppen, Rollen, Rechte und Berechtigungen von nativen Benutzer auf Benutzer in der LDAP-Sicherheitsdomäne zu migrieren, führen Sie die folgenden Schritte aus:

1. Überprüfen Sie die Benutzerkonten für die Kerberos-Authentifizierung.
2. Erstellen Sie die Benutzermigrationsdatei.
3. Führen Sie den infacmd isp migrateusers-Befehl aus.
4. Überprüfen Sie die Gruppen, Rollen, Rechte und Berechtigungen für die Benutzerkonten.

Hinweis: Um Probleme beim Migrieren von Benutzergruppen, Rollen, Rechten und Berechtigungen zu vermeiden, führen Sie während der Migration keine Arbeitsabläufe aus bzw. ändern Sie keine Benutzergruppen, Rollen, Rechte oder Berechtigungen.

Überprüfen der Benutzerkonten für Kerberos-Authentifizierung

Zeigen Sie die Liste der nativen Benutzerkonten an und legen Sie die Konten fest, die Sie auf eine LDAP-Sicherheitsdomäne für Kerberos-Authentifizierung migrieren möchten.

Führen Sie zum Auflisten der Benutzerkonten in der Informatica-Domäne den folgenden Befehl aus:

```
infacmd isp ListAllUsers
```

Jedes native Benutzerkonto, das Sie auf die LDAP-Sicherheitsdomäne migrieren möchten, muss über ein entsprechendes Konto im Microsoft Active Directory-Dienst verfügen, den Sie für Kerberos-Authentifizierung verwenden.

Wenn sich die Konten nicht im Microsoft Active Directory-Dienst befinden, fügen Sie die Benutzerkonten zum Verzeichnisdienst hinzu. Weitere Informationen zum Hinzufügen von Benutzerkonten zum Microsoft Active Directory-Dienst finden Sie in der Dokumentation zu Microsoft Active Directory.

Hinweis: Der Benutzername für Benutzerkonten in der LDAP-Sicherheitsdomäne darf maximal 20 Zeichen enthalten. Wenn Sie die Benutzerkonten zum Microsoft Active Directory-Dienst hinzufügen, achten Sie darauf, dass die Länge des Benutzernamens 20 Zeichen nicht überschreitet.

Erstellen der Benutzermigrationsdatei

Der infacmd isp migrateUsers-Befehl verwendet eine Benutzermigrationsdatei, um festzulegen, welche Gruppen, Rollen, Rechte und Berechtigungen LDAP-Benutzern zugeordnet werden sollen. Die Benutzermigrationsdatei ist eine Nur-Text-Datei mit einer Liste von nativen Benutzern und entsprechenden LDAP-Benutzern, die dieselben Gruppen, Rollen, Rechte und Berechtigungen benötigen.

Wenn Sie die Benutzermigrationsdatei erstellen, müssen Sie die Sicherheitsdomäne für das Benutzerkonto angeben. Ein Schrägstrich (/) trennt die Sicherheitsdomäne vom Benutzernamen. Ein Komma (,) trennt den nativen Benutzer vom entsprechenden LDAP-Benutzer. Sicherheitsdomänen unterscheiden zwischen Groß- und Kleinschreibung. Benutzernamen unterscheiden nicht zwischen Groß- und Kleinschreibung.

Verwenden Sie das folgende Format, um Einträge in der Benutzermigrationsdatei aufzulisten.

```
Native/<SourceUserName>,LDAP/<TargetUserName>
```

Sie können die Gruppen, Rollen, Rechte und Berechtigungen der nativen Benutzer auf Benutzer in verschiedenen LDAP-Sicherheitsdomänen migrieren. Die Benutzermigrationsdatei enthält zum Beispiel die folgende Benutzerliste:

```
Native/User1,LDAPSecurityDomain/User1
Native/User2,LDAPSecurityDomain/User2
Native/User3,newLDAPSecDomain/User3
```

Der migrateUser-Befehl ordnet User1 und User2 in LDAPSecurityDomain denselben Gruppen, Rollen, Rechten und Berechtigungen wie User1 und User2 in der nativen Sicherheitsdomäne zu. Der Befehl ordnet User3 in newLDAPSecDomain denselben Gruppen, Rollen, Rechten und Berechtigungen wie User3 in der nativen Sicherheitsdomäne zu.

Der migrateUsers-Befehl überspringt alle Einträge mit einem doppelten Quellbenutzernamen oder Zielbenutzernamen.

Ausführen des infacmd isp-Befehls migrateUsers

Um Gruppen, Rollen, Rechte und Berechtigungen von den nativen Sicherheitsdomänenbenutzern auf LDAP-Sicherheitsdomänenbenutzer zu migrieren, führen Sie den infacmd migrateUsers-Befehl aus und geben Sie die zu verwendende Benutzermigrationsdatei an.

Stellen Sie vor der Ausführung des infacmd isp-Befehls migrateUsers sicher, dass alle Instanzen des folgenden Befehls auf der Domäne ausgeführt werden:

- Analyst-Dienst
- Content-Managementdienst
- Modellrepository-Dienst
- Metadata Manager-Dienst
- PowerCenter-Repository-Dienst
- Berichterstellungsdienst

Stellen Sie sicher, dass der PowerCenter-Repository-Dienst im normalen Modus ausgeführt wird.

Um die Gruppen, Rollen, Rechte und Berechtigungen für Benutzer zu migrieren, führen Sie den folgenden Befehl aus:

```
infacmd isp migrateUsers -dn <DomainName> -un <AdministratorUserName> -pd
<AdministratorPassword> -umf <UserMigrationFile>
```

Der folgende Befehl migriert zum Beispiel die Gruppen, Rollen, Rechte und Berechtigungen für Benutzer basierend auf der `um_s.txt`-Benutzermigrationsdatei:

```
infacmd isp migrateUsers -dn UMT_Domain -un Administrator -pd Admnistrator -umf C:\UMT
\um_s.txt
```

Der Befehl überschreibt die Berechtigungen für das Verbindungsobjekt, das dem LDAP-Benutzer mit den Berechtigungen für das Verbindungsobjekt für den nativen Benutzer zugeordnet ist. Der Befehl führt die Gruppen, Rollen, Berechtigungen und Domänenobjektberechtigungen für native Benutzer und entsprechende LDAP-Benutzer zusammen.

Der Befehl migrateUsers erstellt eine detaillierte Protokolldatei namens `infacmd_umt_<Datum>_<Uhrzeit>.txt` in dem Verzeichnis, in dem Sie den Befehl ausführen.

Weitere Informationen zu dem Befehl finden Sie in der *Informatica-Befehlsreferenz*.

Fehlerbehebung beim Befehl migrateUsers

Wie kann die Migrationsleistung verbessert werden?

Um die Migrationsleistung zu verbessern, führen Sie die folgenden Schritte aus:

1. Erstellen Sie mehrere eindeutige Benutzermigrationsdateien mit einer begrenzten Anzahl von Benutzern in jeder Datei.
2. Führen Sie mehrere Instanzen des migrateUsers-Befehls gleichzeitig aus.

Beispiel: Um die Gruppen, Rollen, Rechte und Berechtigungen für 150 Benutzer zu migrieren, erstellen Sie drei Benutzermigrationsdateien mit jeweils 50 Benutzern. Führen Sie dann drei Instanzen des migrateUsers-Befehls gleichzeitig aus. Geben Sie eine eindeutige Benutzermigrationsdatei für jede Instanz des Befehls an.

Der Befehl migrateUsers ist fehlgeschlagen.

Wenn der Befehl migrateUsers fehlschlägt, stehen folgende Wiederherstellungspfade zur Verfügung:

- Führen Sie den Befehl migrateUsers erneut aus.

- Ändern Sie die Benutzermigrationsdatei. Führen Sie anschließend den Befehl migrateUsers aus.

Wenn Sie den Befehl erneut ausführen, geben Sie dieselbe Benutzermigrationsdatei an. Der Befehl überschreibt die Berechtigungen für das Verbindungsobjekt, das dem LDAP-Benutzer mit den Berechtigungen für das Verbindungsobjekt für den nativen Benutzer zugeordnet ist. Der Befehl führt die Gruppen, Rollen, Berechtigungen und Domänenobjektberechtigungen für native Benutzer und entsprechende LDAP-Benutzer zusammen.

Führen Sie zum Ändern der Benutzermigrationsdatei die folgenden Schritte durch:

1. Zeigen Sie die detaillierte Protokolldatei an, die während der Ausführung des Befehls migrateUsers erstellt wurde.
2. Löschen Sie Benutzer, die vom Befehl erfolgreich aus der Benutzermigrationsdatei migriert wurden.
3. Führen Sie den Befehl migrateUsers aus.

Überprüfen von Rechten und Berechtigungen für Benutzerkonten

Bevor Sie Kerberos-Authentifizierung aktivieren, stellen Sie sicher, dass die Benutzer in der LDAP-Sicherheitsdomäne über die richtigen Gruppen, Rollen, Rechte und Berechtigungen verfügen. Sie können infacmd verwenden, um Gruppen, Rollen, Rechte und Berechtigungen für Benutzerkonten in der LDAP-Sicherheitsdomäne zu überprüfen.

Überprüfen Sie, ob die folgenden Objekte erfolgreich migriert wurden:

Benutzer und Gruppen

Um die Gruppen zu ermitteln, zu denen Benutzerkonten gehören, rufen Sie eine Liste der Benutzer und zugeordneten Gruppen ab. Führen Sie den folgenden Befehl aus:

```
infacmd aud getUserGroupAssociation
```

Rollen

Führen Sie zum Abrufen der Liste der den Domänenbenutzern und Gruppen zugeordneten Rollen den folgenden Befehl aus:

```
infacmd aud getUserGroupAssociationForRoles
```

Berechtigungen

Führen Sie zum Abrufen einer Liste der Berechtigungen, die den Benutzern und Gruppen in der Domäne zugewiesen wurden, den folgenden Befehl aus:

```
infacmd aud getPrivilegeAssociation
```

Berechtigungen

Führen Sie zum Abrufen einer Liste der Berechtigungen, die den Benutzern und Gruppen in der Domäne zugewiesen wurden, den folgenden Befehl aus:

```
infacmd aud getDomainObjectPermissions
```

Berechtigungen für Ordner und globale Objekte

Wenn die Domäne einen PowerCenter-Repository-Dienst enthält, überprüfen Sie die Berechtigungen für PowerCenter-Ordner und globale Repository-Objekte, die den Benutzerkonten zugewiesen sind. Das PowerCenter-Repository kann die folgenden Objekte umfassen:

- Ordner
- Bereitstellungsgruppen
- Beschriftungen

- Abfragen
- Verbindungen

Nachdem Sie die Domäne für die Verwendung der Kerberos-Authentifizierung konfiguriert haben, können Sie die nativen Benutzerkonten nicht ändern.

Wenn Sie bestätigt haben, dass die Gruppen, Rollen, Rechte und Berechtigungen für die nativen Benutzerkonten erfolgreich in die LDAP-Benutzerkonten verschoben wurden, löschen Sie die nativen Benutzerkonten. Löschen Sie die Benutzerkonten mit dem Administrator-Tool. Weitere Informationen hierzu finden Sie unter "Native Benutzer löschen" auf Seite 96.

Schritt 3. Einrichten der Kerberos-Konfigurationsdatei

Kerberos speichert Konfigurationsinformationen in einer Datei mit dem Namen *krb5.conf*. Informatica benötigt bestimmte Eigenschaften in der Kerberos-Konfigurationsdatei, die so festgelegt werden sollten, dass die Informatica-Domäne die Kerberos-Authentifizierung korrekt verwenden kann. Sie müssen die Eigenschaften in der Konfigurationsdatei „krb5.conf" festlegen und die Datei anschließend in das Informatica-Verzeichnis kopieren.

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 krb5.conf-Datei.
3. Legen Sie im Abschnitt *libdefaults* die von Informatica benötigten Eigenschaften fest oder fügen Sie sie hinzu.

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

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

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

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

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

5. Speichern Sie die krb5.conf-Datei.
6. Kopieren Sie die Konfigurationsdatei in das Informatica-Verzeichnis.

   Sie müssen die Datei „krb5.conf“ in folgendes Verzeichnis kopieren: `<INFA_HOME>/services/shared/security`.
   Wenn die Domäne mehrere Knoten umfasst, kopieren Sie die Datei „krb5.conf“ auf allen Knoten in der Domäne in dasselbe Verzeichnis.

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

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

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

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

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

Schritt 4. Generieren des Prinzipalnamens- und Keytab-Formats

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

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.

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 der Prozessebene

Wenn die Informatica-Domäne eine hohe Sicherheitsstufe erfordert, erstellen Sie einen separaten SPN und eine separate Keytab-Datei für jeden Knoten und jeden Dienst im 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 Authentifizierungsaufrufe initiiert oder annimmt.

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 Anwendungsdienst, der auf einem Knoten in der Informatica-Domäne ausgeführt wird. Jeder Anwendungsdienst erfordert einen eindeutigen Dienstprinzipal- und Keytab-Dateinamen.

Ausführen des Informatica Kerberos SPN-Formatgenerators unter Windows

Sie können den Informatica Kerberos SPN-Formatgenerator ausführen, um eine Datei zu generieren, die das korrekte Format für die in der Informatica-Domäne erforderlichen SPNs und Keytab-Dateinamen anzeigt.

1. Rufen Sie auf einem Rechner, auf dem sich der Informatica-Knoten befindet, das folgende Informatica-Verzeichnis auf: `<InformaticaDirectory>/Tools/Kerberos`
2. Führen Sie die Datei „SPNFormatGenerator.bat“ aus.

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

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

   Die folgende Tabelle beschreibt die Ebenen, 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.

5. Klicken Sie auf **Weiter**.

   Die Seite **Authentifizierungsparameter – Kerberos-Authentifizierung** wird angezeigt.
6. Geben Sie die Domänen- und Knotenparameter ein, um das SPN-Format zu generieren.

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

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

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

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

7. Klicken Sie zum Generieren des SPN-Formats für einen weiteren Knoten auf **+Knoten** und geben Sie den Knotennamen und den Hostnamen an.

   Sie können mehrere Knoten für eine Domäne eingeben.
8. Klicken Sie zum Generieren des SPN-Formats für einen Dienst auf **+Dienst** und geben Sie den Dienstnamen in das Feld **Dienst auf Knoten** ein.

   Das Feld **Dienst auf Knoten** wird nur angezeigt, wenn Sie die Prozessebene für den Dienstprinzipal festlegen und auf **+Dienst** klicken. Sie können mehrere Dienste für einen Knoten eingeben. Die Dienste werden unmittelbar unter dem Knoten angezeigt, auf dem sie ausgeführt werden.
9. Klicken Sie zum Entfernen eines Knotens aus der Liste auf **-Knoten**.

   Der Informatica SPN-Formatgenerator löscht den Knoten. Wenn Sie Dienste zu dem Knoten hinzugefügt haben, werden die Dienste mit dem Knoten gelöscht.
10. Löschen Sie das Feld „Dienstname“, um einen Dienst von einem Knoten zu entfernen.
11. Klicken Sie auf **Weiter**.

    Der SPN-Formatgenerator zeigt den Pfad und den Dateinamen der Datei an, die die Liste der Dienstprinzipal- und Keytab-Dateinamen enthält.
12. Klicken Sie auf **Fertig**, um den SPN-Formatgenerator zu beenden.

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

Ausführen des Informatica Kerberos SPN-Formatgenerators unter UNIX

Sie können den Informatica Kerberos SPN-Formatgenerator ausführen, um eine Datei zu generieren, die das korrekte Format für die in der Informatica-Domäne erforderlichen SPNs und Keytab-Dateinamen anzeigt.

1. Rufen Sie auf einem Rechner, auf dem sich der Informatica-Knoten befindet, das folgende Informatica-Verzeichnis auf: `<InformaticaDirectory>/Tools/Kerberos`
2. Führen Sie in einer Shell-Befehlszeile die Datei „SPNFormatGenerator.sh“ aus.
3. Drücken Sie zur Fortsetzung die **Eingabetaste**.
4. Wählen Sie im Abschnitt **Dienstprinzipalebene** die Ebene aus, auf der die Kerberos-Dienstprinzipale für die Domäne festgelegt werden sollen.

Die folgende Tabelle beschreibt die Ebenen, die Sie auswählen können:

Ebene	Beschreibung
1->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.
2->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 ein, die zum Generieren des SPN-Formats erforderlich sind.

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

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

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

6. Geben Sie an der Eingabeaufforderung **Knoten hinzufügen?** den Wert „1“ ein, um das SPN-Format für einen weiteren Knoten zu generieren. Geben Sie dann den Knotennamen und Knoten-Hostnamen ein.

   Geben Sie zum Generieren der SPN- Formate für mehrere Knoten bei jeder Eingabeaufforderung **Knoten hinzufügen?** den Wert „1“ ein und geben Sie einen Knotennamen und einen Knoten-Hostnamen ein.

7. Geben Sie bei der Eingabeaufforderung **Dienst hinzufügen?** den Wert „1“ ein, um das SPN-Format für einen Dienst zu generieren, der auf dem zuvor angegebenen Knoten ausgeführt werden soll. Geben Sie dann den Dienstnamen ein.

Geben Sie zum Generieren der der SPN-Formate für mehrere Dienste bei jeder Eingabeaufforderung **Dienst hinzufügen?** den Wert „1“ ein und geben Sie einen Dienstnamen ein.

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

   Der SPN-Formatgenerator zeigt den Pfad und den Dateinamen der Datei an, die die Liste der Dienstprinzipal- und Keytab-Dateinamen 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.

Schritt 5. Überprüfen der Textdatei mit SPN- und Keytab-Formaten

Der Kerberos SPN-Formatgenerator generiert eine Textdatei mit dem Namen „SPNKeytabFormat.txt“. Darin sind die Dienstprinzipal- und Keytab-Dateinamen in dem Format aufgelistet, das für die Informatica-Domäne erforderlich ist. Die Liste enthält die SPNs und Keytab-Dateinamen auf Basis der gewählten Dienstprinzipalebene.

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

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
```

Schritt 6. Erstellen der Dienstprinzipalnamen und Keytab-Dateien

Senden Sie nach dem Generieren der Liste der SPN- und Keytab-Dateinamen in dem für Informatica erforderlichen Format eine Anfrage an den Kerberos-Administrator, damit dieser die SPNs zu der Kerberos-Prinzipaldatenbank hinzufügt und die Keytab-Dateien erstellt.

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

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

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

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

Aktivieren Sie die Delegierung in Microsoft Active Directory.

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

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

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

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

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

Die Keytab-Dateien für einen Knoten müssen auf dem Rechner verfügbar sein, auf dem sich der Knoten befindet. Standardmäßig werden Keytab-Dateien im folgenden Verzeichnis gespeichert: `<INFA_HOME>/isp/config/keys`.

Nachdem Sie die Keytab-Dateien vom Kerberos-Administrator erhalten haben, kopieren Sie die Keytab-Dateien in das Verzeichnis, das für die in der Informatica-Domäne verwendeten Keytab-Dateien angegeben wurde.

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.

Schritt 7. Konfigurieren der Kerberos-Authentifizierung für die Domäne

Führen Sie den infasetup-Befehl aus, um von der Authentifizierung für die Informatica-Domäne zur Kerberos-Netzwerkauthentifizierung zu wechseln.

Hinweis: Stellen Sie sicher, dass alle Repository-Objekte eingecheckt werden, bevor Sie die Domäne für die Kerberos-Authentifizierung konfigurieren.

Beim Ausführen des infasetup-Befehls zum Ändern der Domänenauthentifizierung erstellt der Befehl die folgenden LDAP-Sicherheitsdomänen:

- Interne Sicherheitsdomäne. Die interne Sicherheitsdomäne ist eine LDAP-Sicherheitsdomäne mit dem Namen *_infaInternalNamespace*. Die Sicherheitsdomäne „_infaInternalNamespace“ enthält das Standardadministrator-Benutzerkonto, das beim Konfigurieren der Kerberos-Authentifizierung erstellt wurde. Nachdem Sie die Kerberos-Authentifizierung konfiguriert haben, können Sie keine Benutzer mehr zu der Sicherheitsdomäne „_infaInternalNamespace“ hinzufügen, und Sie können die Sicherheitsdomäne nicht mehr löschen.
- Sicherheitsdomäne des Benutzerbereichs. Die Sicherheitsdomäne des Benutzerbereichs ist eine leere LDAP-Sicherheitsdomäne mit dem gleichen Namen wie der Kerberos-Benutzerbereich. Nach der Konfiguration der Kerberos-Authentifizierung können Sie Benutzer aus der Kerberos-Prinzipaldatenbank in die Sicherheitsdomäne des Benutzerbereichs importieren.

Der Befehl „infasetup“ erstellt auch ein Administrator-Benutzerkonto. Geben Sie den Benutzernamen für den Administratorbenutzer an. Nachdem Sie die Kerberos-Authentifizierung konfiguriert haben, enthält die Sicherheitsdomäne „_infaInternalNamespace“ das Administrator-Benutzerkonto.

Führen Sie zum Konfigurieren der Domäne für die Verwendung der Kerberos-Authentifizierung den folgenden Befehl aus:

```
infasetup switchToKerberosMode
```

1. Führen Sie auf einem Gateway-Knoten den infasetup-Befehl aus, um die Authentifizierung für die Domäne zu ändern.

   Wechseln Sie an der Eingabeaufforderung in das Verzeichnis, in dem sich die Informatica-Befehlszeilenprogramme befinden. Standardmäßig werden die Befehlszeilenprogramme in folgendem Verzeichnis installiert: `<InformaticaInstallationDir>/isp/bin`
2. Führen Sie den Befehl „infasetup“ mit den erforderlichen Optionen und Argumenten aus.

   Geben Sie die folgenden Befehle ein:

   - Windows: `infasetup switchToKerberosMode`
   - UNIX: `infasetup.sh switchToKerberosMode`

   In der folgenden Tabelle werden die Optionen für den Befehl „switchToKerberosMode“ beschrieben:

Option	Argument	Beschreibung
-administratorName -ad	administrator_name	Benutzername für das Domänenadministrator-Konto, das beim Konfigurieren der Kerberos-Authentifizierung erstellt wird. Das Benutzerkonto muss sich in der Kerberos-Prinzipaldatenbank befinden. Nachdem Sie die Kerberos-Authentifizierung konfiguriert haben, wird dieser Benutzer in die Sicherheitsdomäne *_infaInternalNamespace* aufgenommen.
-ServiceRealmName -srn	realm _name_of_node_spn	Name des Kerberos-Bereichs, zu dem die Informatica-Domänendienste gehören. Der Bereichsname muss in Großbuchstaben angegeben werden und unterliegt der Groß-/Kleinschreibung. Der Dienstbereichsname und der Benutzerbereichsname müssen identisch sein.

Option	Argument	Beschreibung
-UserRealmName -urn	realm _name_of_user_spn	Name des Kerberos-Bereichs, zu dem die Informatica-Domänenbenutzer gehören. Der Bereichsname muss in Großbuchstaben angegeben werden und unterliegt der Groß-/Kleinschreibung. Der Dienstbereichsname und der Benutzerbereichsname müssen identisch sein.
-SPNShareLevel -spnSL	PROCESS |NODE	Dienstprinzipalebene für die Domäne. Legen Sie eine der folgenden Ebenen für die Eigenschaft fest: - Prozess Die Domäne erfordert einen eindeutigen Dienst-Prinzipalnamen (SPN) und eine Keytab-Datei für jeden Knoten und für jeden Dienst auf einem Knoten. Die Anzahl der für jeden Knoten erforderlichen SPNs und Keytab-Dateien hängt von der Anzahl der Dienstprozesse ab, die auf dem Knoten ausgeführt werden. Verwenden Sie die Option „Prozessebene“, wenn die Domäne eine hohe Sicherheitsstufe erfordert, z. B. wenn es sich um eine Produktionsdomäne handelt. - Knoten. Die Domäne verwendet einen SPN und eine Keytab-Datei für den Knoten und für alle Dienste, die auf dem Knoten ausgeführt werden. Sie erfordert außerdem einen separaten SPN und eine separate Keytab-Datei für alle HTTP-Prozesse auf dem Knoten. Verwenden Sie die Option „Knotenebene“, wenn die Domäne keine hohe Sicherheitsstufe erfordert, z. B. bei einer Test- oder Entwicklungsdomäne. Standardwert ist „Prozess“.

Der Befehl „switchToKerberosMode“ ändert den Authentifizierungsmodus für die Domäne von der nativen bzw. LDAP-Benutzerauthentifizierung in die Kerberos-Netzwerk-Authentifizierung.

Schritt 8. Aktualisieren der Knoten in der Domäne

Führen Sie den infasetup-Befehl aus, um alle Knoten in der Domäne mit den Informationen zum Kerberos-Authentifizierungsserver zu aktualisieren.

Aktualisieren Sie alle Gateway- und Worker-Knoten mit den Informationen des Kerberos-Authentifizierungsservers, außer den Gateway-Knoten, auf dem Sie den Befehl switchToKerberosMode ausführen.

Um die Gateway- und Arbeitsknoten zu aktualisieren, verwenden Sie die folgenden Befehle:

infasetup UpdateGatewayNode

Verwenden Sie den Befehl „UpdateGatewayNode“, um die Kerberos-Authentifizierungs-Parameter auf einem Gateway-Knoten in der Domäne festzulegen. Wenn die Domäne mehrere Gateway-Knoten enthält, führen Sie den Befehl „UpdateGatewayNode“ für jeden Gateway-Knoten aus.

infasetup UpdateWorkerNode

Verwenden Sie den Befehl „UpdateWorkerNode“, um die Kerberos-Authentifizierungs-Parameter auf einem Arbeitsknoten in der Domäne festzulegen. Wenn die Domäne mehrere Arbeitsknoten enthält, führen Sie den Befehl „UpdateWorkerNode“ für jeden Arbeitsknoten aus.

1. Führen Sie auf einem Rechner, auf dem sich ein Informatica-Knoten befindet, den Befehl „infasetup“ aus, um den Knoten zu aktualisieren.

   Wechseln Sie an der Eingabeaufforderung in das Verzeichnis, in dem sich die Informatica-Befehlszeilenprogramme befinden. Standardmäßig werden die Befehlszeilenprogramme in folgendem Verzeichnis installiert: `<InformaticaInstallationDir>/isp/bin`

2. Führen Sie „infasetup“ mit der erforderlichen Optionen und Argumenten aus.

   Geben Sie den folgenden Befehl ein:

   - Windows: `infasetup UpdateGatewayNode` oder `infasetup UpdateWorkerNode`
   - UNIX: `infasetup.sh UpdateGatewayNode` oder `infasetup.sh UpdateWorkerNode`

   Die folgende Tabelle enthält eine Beschreibung der Optionen zum Aktualisieren der Kerberos-Authentifizierungsinformationen für einen Knoten:

Option	Argument	Beschreibung
-EnableKerberos -krb	enable_kerberos	Konfiguriert die Informatica-Domäne zur Verwendung der Kerberos-Authentifizierung.
-ServiceRealmName -srn	realm _name_of_node_spn	Name des Kerberos-Bereichs, zu dem die Informatica-Domänendienste gehören. Der Bereichsname muss in Großbuchstaben angegeben werden und unterliegt der Groß-/Kleinschreibung. Der Dienstbereichsname und der Benutzerbereichsname müssen identisch sein.
-UserRealmName -urn	realm _name_of_user_spn	Name des Kerberos-Bereichs, zu dem die Informatica-Domänenbenutzer gehören. Der Bereichsname muss in Großbuchstaben angegeben werden und unterliegt der Groß-/Kleinschreibung. Der Dienstbereichsname und der Benutzerbereichsname müssen identisch sein.

Schritt 9. Aktualisieren der Client-Computer

Kopieren Sie die Kerberos-Konfigurationsdatei und legen Sie die Umgebungsvariable auf den Rechnern, auf denen sich die Informatica-Clients befinden, fest. Außerdem müssen Sie den Browser für den Zugriff auf Informatica-Webanwendungen konfigurieren.

Nachdem Sie die Informatica-Domäne für die Ausführung mit der Kerberos-Authentifizierung konfiguriert haben, führen Sie die folgenden Aufgaben in den Informatica-Clienttools durch:

Kopieren Sie die Kerberos-Konfigurationsdatei auf die Client-Computer.

Kopieren Sie die Konfigurationsdatei auf jeden Computer, der einen Informatica-Client hostet. Sie müssen die Datei `krb5.conf` in das folgende Verzeichnis kopieren: `<Informatica-Client-Verzeichnis>/shared/security`

Legen Sie die KRB5_CONFIG-Umgebungsvariablen mit die Kerberos-Konfigurationsdatei fest.

Verwenden Sie die Umgebungsvariable KRB5_CONFIG, um den Pfad und Dateinamen der Kerberos-Konfigurationsdatei `krb5.conf` zu speichern. Sie müssen die Umgebungsvariable KRB5_CONFIG auf jedem Computer einrichten, auf dem ein Informatica-Client gehostet wird.

Konfigurieren des Webbrowsers.

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

Erstellen Sie unter UNIX eine Anmeldedaten-Cache-Datei für Single-Sign-On.

Für die Ausführung der Informatica-Befehlszeilenprogramme unter UNIX mit Single-Sign-On müssen Sie eine Anmeldedaten-Cache-Datei generieren, um das Benutzerkonto zu authentifizieren, das die Befehle auf dem Kerberos-Netzwerk ausführt. Verwenden Sie das Dienstprogramm *kinit* von MIT Kerberos zum Generieren der Anmeldedaten-Cache-Datei. Die Anmeldedaten Cache-Datei ermöglicht einem Benutzer die Ausführung der Befehle ohne Benutzernamen und Passwortoptionen.

Wenn Sie eine Anmeldedaten-Cache-Datei verwenden, müssen Sie den Standardpfad und -dateinamen für den Anmeldedaten-Cache in der KRB5CCNAME-Umgebungsvariablen festlegen.

Weitere Informationen über die Informatica-Befehlszeilenprogramme unter UNIX mit Single-Sign-On finden Sie in der *Informatica Befehlsreferenz*.

Schritt 10. Starten der Informatica-Domäne

Nachdem Sie die Informatica-Domäne zwecks Kerberos-Authentifizierung konfiguriert haben, starten Sie die Domäne und das Administrator-Tool.

1. Sie können den Informatica-Dienst unter Windows über die Systemsteuerung oder das Startmenü starten.

   Klicken Sie zum Starten von Informatica über das Windows-Startmenü auf **Programme** > **Informatica [Version]** > **Server** . Klicken Sie mit der rechten Maustaste auf **Informatica-Dienste starten** und wählen Sie **Als Administrator ausführen** aus.

   Führen Sie den folgenden Befehl unter UNIX aus, um den Informatica-Dämon zu starten:

   ```
   infaservice.sh startup
   ```

   infaservice.sh ist standardmäßig im folgenden Verzeichnis installiert: `<INFA_HOME>/tomcat/bin`

2. Starten Sie den Informatica Administrator.

   Starten Sie das Administrator-Tool mit der folgenden URL: `http://<fully qualified hostname>:<http port>`. Wenn Sie das Administrator-Tool für die Verwendung einer sicheren Verbindung konfiguriert haben, verwenden Sie das HTTPS-Protokoll: `https://<fully qualified hostname>:<http port>`

   Beim Starten des Administrator-Tools müssen Sie die URL zur Liste der vertrauenswürdigen Sites für den Browser hinzufügen.

3. Wählen Sie die Sicherheitsdomäne für Ihr Benutzerkonto aus.

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

Nach der Konfiguration der Kerberos-Authentifizierung

Wenn sich die Dienstprinzipalebene für die Domäne auf der Prozessebene befindet, erfordert die Domäne einen SPN und eine Keytab-Datei für jeden Dienst, den Sie in der Domäne erstellen. Bevor Sie einen Dienst aktivieren, überprüfen Sie, ob ein SPN und eine Keytab-Datei für den Dienst verfügbar sind. Kerberos kann den Anwendungsdienst nicht authentifizieren, wenn der Dienst nicht über eine Keytab-Datei im Informatica-Verzeichnis verfügt.

Wenn SPNs und Keytab-Dateien für die Anwendungsdienste, die Sie in der Domäne erstellen möchten, nicht verfügbar sind, müssen Sie den SPN und die Keytab-Datei vor dem Aktivieren des Diensts erstellen. Sie können das Format für den SPN und den Keytab-Dateinamen für den Dienst mit dem Kerberos SPN-Formatgenerator von Informatica generieren. Um Zeit zu sparen, entscheiden Sie über die Namen der Dienste, die Sie erstellen möchten, und über die Knoten, auf denen sie ausgeführt werden. Führen Sie dann das Dienstprogramm aus, um das Format für den SPN und den Keytab-Dateinamen für alle Dienste auf einmal zu erstellen.

Weitere Informationen zum Ausführen des Kerberos SPN-Formatgenerators von Informatica finden Sie unter “Schritt 4. Generieren des Prinzipalnamens- und Keytab-Formats” auf Seite 35.

Senden Sie eine Anfrage an den Kerberos-Administrator, um die SPNs zur Prinzipal-Datenbank hinzuzufügen und die entsprechende Keytab-Datei zu erstellen.

Nachdem Sie die Keytab-Dateien vom Kerberos-Administrator erhalten haben, kopieren Sie die Dateien in das für die Keytab-Datei angegebene Verzeichnis. Standardmäßig werden Keytab-Dateien im folgenden Verzeichnis gespeichert: `<INFA_HOME>/isp/config/keys`.

Wenn sich der Dienstprinzipalname für die Domäne auf der Knotenebene befindet, können Sie Anwendungsdienste erstellen und aktivieren, ohne zusätzliche SPNs und Keytab-Dateien zu erstellen.

KAPITEL 5

Domänensicherheit

Dieses Kapitel umfasst die folgenden Themen:

Domänensicherheit - Übersicht

Sie können Optionen in der Informatica-Domäne aktivieren, um eine sichere Kommunikation zwischen den Komponenten in der Domäne und zwischen der Domäne und Client-Komponenten zu konfigurieren.

Sie können verschiedene Optionen aktivieren, um bestimmte Komponenten in der Domäne zu sichern. Sie müssen nicht alle Komponenten in der Domäne sichern. Beispielsweise können Sie die Kommunikation zwischen den Diensten in der Domäne sichern, jedoch nicht die Verbindung zwischen dem Modellrepository-Dienst und der Repository-Datenbank sichern.

Informatica verwendet die TCP/IP- und HTTP-Protokolle, um zwischen Komponenten in der Domäne zu kommunizieren. Die Domäne verwendet SSL-Zertifikate für die sichere Kommunikation zwischen Komponenten.

Wenn Sie die Informatica-Dienste installieren, können Sie die sichere Kommunikation für die Dienste in der Domäne und für das Administrator-Tool aktivieren. Nach der Installation können Sie sichere Kommunikation in der Domäne über das Administrator-Tool oder die Befehlszeile konfigurieren.

Das Installationsprogramm generiert während der Installation einen Verschlüsselungsschlüssel, um vertrauliche Daten wie Passwörter, die in der Domäne gespeichert werden, zu verschlüsseln. Sie können das Schlüsselwort bereitstellen, den das Installationsprogramm zum Generieren des Verschlüsselungsschlüssels verwendet. Nach der Installation können Sie den Verschlüsselungsschlüssel für vertrauliche Daten ändern. Sie müssen den Inhalt der Repositorys aktualisieren, um die verschlüsselten Daten zu aktualisieren.

Sie können eine sichere Kommunikation in den folgenden Bereichen aktivieren:

Domäne

Sie können innerhalb der Domäne Optionen auswählen, um sichere Kommunikation für die folgenden Komponenten zu aktivieren:

- Zwischen dem Dienstmanager, den Diensten in der Domäne und den Informatica-Client-Tools
- Zwischen der Domäne und dem Domänenkonfigurations-Repository
- Zwischen den Repository-Diensten und Repository-Datenbanken
- Zwischen dem PowerCenter-Integrationsdienst und DTM-Prozessen

Webanwendungsdienste

Sie können die Verbindung zwischen einem Webanwendungsdienst, wie z. B. dem Analyst-Dienst, und dem Browser sichern

Quellen und Ziele

Sie können sichere Kommunikation zwischen dem Datenintegrationsdienst und dem PowerCenter-Integrationsdienst sowie den Quell- und Zieldatenbanken aktivieren.

Datenspeicher

Informatica verschlüsselt vertrauliche Daten, wie z. B. Passwörter, wenn Daten in der Domäne gespeichert werden. Informatica erzeugt einen Verschlüsselungsschlüssel basierend auf einem Schlüsselwort, das Sie während der Installation bereitstellen. Informatica verwendet den Verschlüsselungsschlüssel, um vertrauliche Daten zu ver- und entschlüsseln, die in der Domäne gespeichert sind.

Sichere Kommunikation innerhalb der Domäne

Sie können die Option „Sichere Kommunikation“ verwenden, um die Verbindung zwischen Diensten und zwischen Diensten und den Dienstmanagern in der Domäne zu sichern. Außerdem können Sie die Sicherheit für Arbeitsabläufe aktivieren und sichere Datenbanken für die Repositorys verwenden, die Sie in der Domäne erstellen.

Konfigurieren Sie nach dem Sichern der Domäne die Informatica-Client-Anwendungen zur Zusammenarbeit mit einer sicheren Domäne.

Sichere Kommunikation für Dienste und den Dienstmanager

Sie können sichere Kommunikation innerhalb der Domäne während der Installation konfigurieren. Nach der Installation können Sie eine sichere Kommunikation für die Domäne im Administrator-Tool oder über die Befehlszeile konfigurieren.

Informatica stellt ein SSL-Zertifikat zur Verfügung, das Sie zum Sichern der Domäne verwenden können. Dennoch sollten Sie ein benutzerdefiniertes Zertifikat für Domänen bereitstellen, die eine höhere Sicherheitsstufe benötigen, wie z. B. eine Domäne in einer Produktionsumgebung. Geben Sie die Schlüsselspeicher- und Truststore-Dateien an, die die zu verwendenden SSL-Zertifikate enthalten.

Hinweis: Informatica stellt SSL-Zertifikate zu Bewertungszwecken bereit. Wenn Sie kein SSL-Zertifikat zur Verfügung stellen, verwendet Informatica den gleichen standardmäßigen privaten Schlüssel für alle Informatica-Installationen. Die Sicherheit Ihrer Domäne könnte gefährdet sein. Stellen Sie ein SSL-Zertifikat zur Verfügung, um einen hohen Grad an Sicherheit für die Domäne sicherzustellen. Das von Ihnen zur Verfügung gestellte Zertifikat kann selbstsigniert werden oder von einer Zertifizierungsbehörde signiert werden.

Wenn Sie eine sichere Kommunikation für die Domäne konfigurieren, sichern Sie die Verbindungen zwischen den folgenden Komponenten:

- Zwischen dem Dienstmanager und allen in der Domäne ausgeführten Diensten
- Zwischen dem Datenintegrationsdienst und dem Modellrepository-Dienst
- Zwischen dem Datenintegrationsdienst und den Arbeitsablaufprozessen
- Zwischen dem PowerCenter-Integrationsdienst und dem PowerCenter-Repository-Dienst
- Zwischen den Domänendiensten und den Informatica-Client-Tools sowie Befehlszeilenprogrammen

Anforderungen für sichere Kommunikation innerhalb der Domäne

Stellen Sie vor dem Aktivieren sicherer Kommunikation innerhalb der Domäne sicher, dass 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 Schlüsselspeicher importiert.

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

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

Sie haben das Zertifikat in Truststores importiert.

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

Die Schlüsselspeicher und Truststores befinden sich im richtigen Verzeichnis.

Wenn Sie während der Installation sichere Kommunikation aktivieren, müssen sich der Schlüsselspeicher und der Truststore in einem Verzeichnis befinden, auf das das Installationsprogramm zugreifen kann.

Wenn Sie nach der Installation sichere Kommunikation aktivieren, müssen sich der Schlüsselspeicher und der Truststore in einem Verzeichnis befinden, auf das die Befehlszeilenprogramme zugreifen können.

Weitere Informationen zum Erstellen eines benutzerdefinierten Schlüsselspeichers und Truststores finden Sie im Artikel „How to Create Keystore and Truststore Files for Secure Communication in the Informatica Domain“ in der Informatica How-To Library: https://mysupport.informatica.com/docs/DOC-12984

Konfigurieren Sie nach dem Sichern der Domäne die Informatica-Client-Anwendungen zur Zusammenarbeit mit einer sicheren Domäne.

Aktivieren sicherer Kommunikation für die Domäne über die Befehlszeile

Verwenden Sie die infacmd- und infasetup-Befehle, um eine sichere Kommunikation für die Domäne zu aktivieren. Nachdem Sie die sichere Kommunikation aktiviert haben, müssen Sie die Domäne neu starten, damit die Änderungen wirksam werden.

Um Ihre SSL-Zertifikatsdateien zu verwenden, geben Sie die Schlüsselspeicher- und Truststore-Dateien an, wenn Sie den infasetup-Befehl ausführen.

Um eine sichere Domänenkommunikation über die Befehlszeile zu konfigurieren, verwenden Sie die folgenden Befehle:

infacmd isp UpdateDomainOptions

Verwenden Sie den Befehl UpdateDomainOptions, um den sicheren Kommunikationsmodus für die Domäne einzurichten.

infasetup UpdateGatewayNode

Verwenden Sie den UpdateGatewayNode-Befehl, um sichere Kommunikation für den Dienstmanager auf einem Gateway-Knoten in einer Domäne zu aktivieren. Wenn die Domäne über mehrere Gateway-Knoten verfügt, führen Sie den UpdateGatewayNode-Befehl auf jedem Gateway-Knoten aus.

infasetup UpdateWorkerNode

Verwenden Sie den UpdateWorkerNode-Befehl, um sichere Kommunikation für den Dienstmanager auf einem Worker-Knoten in einer Domäne zu aktivieren. Wenn die Domäne mehrere Worker-Knoten aufweist, führen Sie den UpdateWorkerNode-Befehl auf jedem Worker-Knoten aus.

1. Stellen Sie sicher, dass die zu sichernde Domäne ausgeführt wird.
2. Führen Sie den Befehl zum Aktualisieren der Domäne aus.

   Wechseln Sie an der Eingabeaufforderung in das Verzeichnis, in dem sich die Informatica-Befehlszeilenprogramme befinden. Standardmäßig werden die Befehlszeilenprogramme in folgendem Verzeichnis installiert: `<InformaticaInstallationDir>/isp/bin`
3. Führen Sie „infacmd“ mit den erforderlichen Optionen und Argumenten aus.

   Geben Sie den folgenden Befehl ein:

   - Windows: `infacmd isp UpdateDomainOptions`
   - UNIX: `infacmd.sh isp UpdateDomainOptions`

   Um eine sichere Kommunikation für die Domäne zu konfigurieren, fügen Sie beim Ausführen des infacmd-Befehls die folgenden Optionen hinzu:

Option	Argument	Beschreibung
-DomainOptions -do	option_name=value	Legen Sie die folgende Option fest, um eine sichere Kommunikation für die Domäne zu konfigurieren: TLSMode=True

4. Fahren Sie die Domäne herunter.

   Die Domäne muss heruntergefahren werden, bevor Sie die infasetup-Befehle ausführen.
5. Führen Sie „infasetup“ mit der erforderlichen Optionen und Argumenten aus.

   Geben Sie den folgenden Befehl ein:

   - Windows: `infasetup UpdateGatewayNode` oder `infasetup UpdateWorkerNode`

- UNIX: `infasetup.sh UpdateGatewayNode` oder `infasetup.sh UpdateWorkerNode`

Um die sichere Kommunikation auf den Knoten zu konfigurieren, führen Sie die Befehle mit den folgenden Optionen aus:

Option	Argument	Beschreibung
-EnableTLS -tls	enable_tls	Konfiguriert die sichere Kommunikation für die Dienste in der Informatica-Domäne.
-NodeKeystore -nk	node_keystore_directory	Optional, wenn Sie das Standard-SSL-Zertifikat von Informatica verwenden. Erforderlich, wenn Sie Ihr SSL-Zertifikat verwenden. Verzeichnis, das die Schlüsselspeicherdateien enthält. Für die Informatica-Domäne muss das SSL-Zertifikat im PEM-Format und in JKS (Java Keystore)-Dateien vorliegen. Das Verzeichnis muss Schlüsselspeicherdateien in den Formaten PEM und JKS enthalten. Die Schlüsselspeicherdateien müssen „infa_keystore.jks“ und „infa_keystore.pem“ lauten. Sie können dieselbe Schlüsselspeicherdatei für mehrere Knoten verwenden.
-NodeKeystorePass -nkp	node_keystore_password	Optional, wenn Sie das Standard-SSL-Zertifikat von Informatica verwenden. Erforderlich, wenn Sie Ihr SSL-Zertifikat verwenden. Das Passwort für die infa_keystore.jks-Datei.
-NodeTruststore -nt	node_truststore_directory	Optional, wenn Sie das Standard-SSL-Zertifikat von Informatica verwenden. Erforderlich, wenn Sie Ihr SSL-Zertifikat verwenden. Verzeichnis, das die Truststore-Dateien enthält. Für die Informatica-Domäne muss das SSL-Zertifikat im PEM-Format und in JKS (Java Keystore)-Dateien vorliegen. Das Verzeichnis muss Truststore-Dateien in den Formaten PEM und JKS enthalten. Die Truststore-Dateien müssen die Namen infa_truststore.jks und infa_truststore.pem aufweisen. Sie können dieselbe Truststore-Datei für mehrere Knoten verwenden.
-NodeTruststorePass -ntp	node_truststore_password	Optional, wenn Sie das Standard-SSL-Zertifikat von Informatica verwenden. Erforderlich, wenn Sie Ihr SSL-Zertifikat verwenden. Passwort für die infa_truststore.jks-Datei.

6. Führen Sie den infasetup-Befehl auf jedem Knoten in der Domäne aus.

   Wenn Sie über mehrere Gateway-Knoten in der Domäne verfügen, führen Sie infasetup UpdateGatewayNode auf jedem Gateway-Knoten aus. Wenn Sie über mehrere Worker-Knoten verfügen, führen Sie infasetup UpdateWorkerNode auf jedem Worker-Knoten aus. Sie müssen für alle Knoten in der Domäne dieselben Schlüsselspeicher- und Truststore-Dateien verwenden.

7. Starten Sie die Domäne neu.

Nachdem Sie alle Knoten in der Domäne aktualisiert haben, müssen Sie die Rechner aktualisieren, auf denen sich die Informatica-Clienttools befinden. Legen Sie den Speicherort der SSL-Zertifikate in den Informatica-Truststore-Umgebungsvariablen fest.

Aktivieren einer sicheren Kommunikation für die Domäne im Administrator-Tool

Sie können das Administrator-Tool verwenden, um sichere Kommunikation für die Domäne zu aktivieren. Wenn Sie die sichere Kommunikation im Administrator-Tool aktiveren, müssen Sie auch infasetup-Befehle zum Aktualisieren der Knoten ausführen.

Wenn Sie die Option „Sichere Kommunikation“ im Administrator-Tool aktivieren, müssen Sie den infasetup-Befehl auch zum Aktualisieren der Informatica-Konfigurationsdateien auf jedem Knoten ausführen. Um Ihre zu verwendenden SSL-Zertifikatsdateien anzugeben, geben Sie die Schlüsselspeicher- und Truststore-Dateien an, wenn Sie den infasetup-Befehl ausführen.

Verwenden Sie zum Aktualisieren der Informatica-Konfigurationsdateien auf jedem Knoten die folgenden Befehle:

infasetup UpdateGatewayNode

Verwenden Sie den UpdateGatewayNode-Befehl, um sichere Kommunikation für den Dienstmanager auf einem Gateway-Knoten in einer Domäne zu aktivieren. Wenn die Domäne über mehrere Gateway-Knoten verfügt, führen Sie den UpdateGatewayNode-Befehl auf jedem Gateway-Knoten aus.

infasetup UpdateWorkerNode

Verwenden Sie den UpdateWorkerNode-Befehl, um sichere Kommunikation für den Dienstmanager auf einem Worker-Knoten in einer Domäne zu aktivieren. Wenn die Domäne mehrere Worker-Knoten aufweist, führen Sie den UpdateWorkerNode-Befehl auf jedem Worker-Knoten aus.

Führen Sie im Administrator-Tool die folgenden Schritte aus, um die sichere Kommunikation in der Domäne zu aktivieren:

1. Wählen Sie die Domäne im Administrator-Tool aus.
2. Klicken Sie im Inhaltsbereich auf die Ansicht **Eigenschaften**.
3. Gehen Sie zum Bereich **Allgemeine Eigenschaften** und klicken Sie auf **Bearbeiten**.
4. Wählen Sie im Fenster **Allgemeine Eigenschaften bearbeiten Sichere Kommunikation aktivieren** aus.
5. Klicken Sie auf **OK**.
6. Fahren Sie die Domäne herunter.

   Die Domäne muss heruntergefahren werden, bevor Sie die infasetup-Befehle ausführen.
7. Führen Sie den infasetup-Befehl aus, um die Informatica-Konfigurationsdateien zu aktualisieren und die SSL-Zertifikatsdateien anzugeben.

   Wechseln Sie an der Eingabeaufforderung in das Verzeichnis, in dem sich die Informatica-Befehlszeilenprogramme befinden. Standardmäßig werden die Befehlszeilenprogramme in folgendem Verzeichnis installiert: `<InformaticaInstallationDir>/isp/bin`
8. Führen Sie „infasetup“ mit der erforderlichen Optionen und Argumenten aus.

   Geben Sie den folgenden Befehl ein:

   - Windows: `infasetup UpdateGatewayNode` oder `infasetup UpdateWorkerNode`
   - UNIX: `infasetup.sh UpdateGatewayNode` oder `infasetup.sh UpdateWorkerNode`

Um die sichere Kommunikation auf den Knoten zu konfigurieren, führen Sie die Befehle mit den folgenden Optionen aus:

Option	Argument	Beschreibung
-EnableTLS -tls	enable_tls	Konfiguriert die sichere Kommunikation für die Dienste in der Informatica-Domäne.
-NodeKeystore -nk	node_keystore_directory	Optional, wenn Sie das Standard-SSL-Zertifikat von Informatica verwenden. Erforderlich, wenn Sie Ihr SSL-Zertifikat verwenden. Verzeichnis, das die Schlüsselspeicherdateien enthält. Für die Informatica-Domäne muss das SSL-Zertifikat im PEM-Format und in JKS (Java Keystore)-Dateien vorliegen. Das Verzeichnis muss Schlüsselspeicherdateien in den Formaten PEM und JKS enthalten. Die Schlüsselspeicherdateien müssen „infa_keystore.jks“ und „infa_keystore.pem“ lauten. Sie können dieselbe Schlüsselspeicherdatei für mehrere Knoten verwenden.
-NodeKeystorePass -nkp	node_keystore_password	Optional, wenn Sie das Standard-SSL-Zertifikat von Informatica verwenden. Erforderlich, wenn Sie Ihr SSL-Zertifikat verwenden. Das Passwort für die infa_keystore.jks-Datei.
-NodeTruststore -nt	node_truststore_directory	Optional, wenn Sie das Standard-SSL-Zertifikat von Informatica verwenden. Erforderlich, wenn Sie Ihr SSL-Zertifikat verwenden. Verzeichnis, das die Truststore-Dateien enthält. Für die Informatica-Domäne muss das SSL-Zertifikat im PEM-Format und in JKS (Java Keystore)-Dateien vorliegen. Das Verzeichnis muss Truststore-Dateien in den Formaten PEM und JKS enthalten. Die Truststore-Dateien müssen die Namen infa_truststore.jks und infa_truststore.pem aufweisen. Sie können dieselbe Truststore-Datei für mehrere Knoten verwenden.
-NodeTruststorePass -ntp	node_truststore_password	Optional, wenn Sie das Standard-SSL-Zertifikat von Informatica verwenden. Erforderlich, wenn Sie Ihr SSL-Zertifikat verwenden. Passwort für die infa_truststore.jks-Datei.

9. Führen Sie den infasetup-Befehl auf jedem Knoten in der Domäne aus.

   Wenn Sie über mehrere Gateway-Knoten in der Domäne verfügen, führen Sie infasetup UpdateGatewayNode auf jedem Gateway-Knoten aus. Wenn Sie über mehrere Worker-Knoten verfügen, führen Sie infasetup UpdateWorkerNode auf jedem Worker-Knoten aus. Sie müssen für alle Knoten in der Domäne dieselben Schlüsselspeicher- und Truststore-Dateien verwenden.

10. Starten Sie die Domäne neu.

Nachdem Sie alle Knoten in der Domäne aktualisiert haben, müssen Sie die Rechner aktualisieren, auf denen sich die Informatica-Clienttools befinden. Legen Sie den Speicherort der SSL-Zertifikate in den Informatica-Truststore-Umgebungsvariablen fest.

Konfigurieren der Informatica-Client-Anwendungen zum Arbeiten mit einer sicheren Domäne

Wenn Sie sichere Kommunikation innerhalb der Domäne aktivieren, sichern Sie ebenfalls Verbindungen zwischen der Domäne und Informatica-Client-Anwendungen, wie z. B. dem Developer Tool. Geben Sie den Speicherort und das Passwort der Truststore-Dateien an, die zum Sichern der Domäne mit Umgebungsvariablen verwendet werden.

Wenn Sie die Informatica-SSL-Zertifikat verwenden, müssen Sie die INFA_TRUSTSTORE oder INFA_TRUSTSTORE_PASSWORD-Umgebungsvariable nicht festzulegen. Wenn Sie die Informatica-Clients installieren, legt das Installationsprogramm die Umgebungsvariablen fest und installiert die standardmäßigen Truststore-Dateien im folgenden Verzeichnis: `<Informatica-Installationsverzeichnis>\clients\shared\security`

Wenn Sie die zu verwendenden SSL-Zertifikate bereitstellen, kopieren Sie die Truststore-Dateien auf den Computer, der den Client hostet, und legen Sie die Variable INFA_TRUSTSTORE auf das Verzeichnis fest, das die Truststore-Dateien enthält. Truststore-Dateien müssen im JKS- und PEM-Format mit der Bezeichnung „infa_truststore.jks“ und „infa_truststore.pem“ vorliegen. Sie müssen außerdem die Variable INFA_TRUSTSTORE_PASSWORD mit dem Passwort für die Datei „infa_truststore.jks“ festlegen.

Legen Sie die folgenden Umgebungsvariablen für die Truststore-Informationen fest:

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.

Sichere Domänenkonfigurations-Repository-Datenbank

Das Informatica-Domänenkonfigurations-Repository speichert die Konfigurationsinformationen und Benutzerkonto-Berechtigungen. Beim Erstellen einer Informatica-Domäne müssen Sie ein Domänenkonfigurations-Repository erstellen.

Sie können ein Domänenkonfigurations-Repository in einer Datenbank erstellen, die mit dem SSL-Protokoll gesichert ist. Das SSL-Protokoll verwendet in einer Truststore-Datei gespeicherte SSL-Zertifikate. Der Zugriff auf die sichere Datenbank erfordert ein Truststore, der die Zertifikate für die Datenbank enthält.

Sie können eine sichere Domänenkonfigurations-Repository-Datenbank erstellen, wenn Sie die Informatica-Dienste installieren und eine Domäne erstellen. Weitere Informationen zum Konfigurieren eines sicheren Domänenkonfigurations-Repository während der Installation finden Sie in den Informatica-Installationshandbüchern.

Nach der Installation können Sie eine sichere Domänenkonfigurations-Repository-Datenbank über die Befehlszeile konfigurieren.

Hinweis: Bevor Sie eine sichere Domänenkonfigurations-Repository-Datenbank nach der Installation konfigurieren, müssen Sie eine sichere Kommunikation für die Domäne aktivieren.

Sie können ein sicheres Domänenkonfigurations-Repository in den folgenden Datenbanken erstellen:

- Oracle
- Microsoft SQL Server

- IBM DB2

Konfigurieren einer sicheren Domänenkonfigurations-Repository-Datenbank

Nach der Installation können Sie das Domänenkonfigurations-Repository in eine sichere Datenbank ändern. Sie können eine sichere Domänenkonfigurations-Repository-Datenbank nur verwenden, wenn Sie eine sichere Kommunikation für die Domäne aktivieren.

Sie müssen die Domäne herunterfahren, bevor Sie die Domänenkonfigurations-Repository-Datenbank ändern. Verwenden Sie den infasetup-Befehl, um die Domänenkonfigurations-Repository-Datenbank zu sichern und sie in einer sicheren Datenbank wiederherzustellen. Geben Sie beim Wiederherstellen des Domänenkonfigurations-Repositorys in der sicheren Datenbank die Sicherheitsparameter für die sichere Datenbank an. Aktualisieren Sie anschließend den Gateway-Knoten mit den Domänenkonfigurations-Repository-Informationen.

Um die Repository-Datenbank zu sichern sowie wiederherzustellen und den Gateway-Knoten zu aktualisieren, verwenden Sie die folgenden Befehle:

infasetup BackupDomain

Verwenden Sie die BackupDomain-Option, um Daten aus der Domänenkonfigurations-Repository-Datenbank zu sichern.

infasetup RestoreDomain

Verwenden Sie die RestoreDomain-Option, um Domänenkonfigurations-Repository-Daten in einer sicheren Datenbank wiederherzustellen.

infasetup UpdateGatewayNode

Verwenden Sie die UpdateGatewayNode-Option, um die Domänenkonfigurations-Repository-Einstellungen in den Gateway-Knoten der Domäne zu aktualisieren.

Um das Domänenkonfigurations-Repository in eine sichere Datenbank zu ändern, führen Sie die folgenden Schritte durch:

1. Stellen Sie sicher, dass eine sichere Kommunikation für die Domäne aktiviert ist.

   Die Domäne muss sicher sein, bevor Sie eine sichere Datenbank für das Domänenkonfigurations-Repository verwenden können.
2. Fahren Sie die Domäne herunter.
3. Führen Sie den infasetup-Befehl BackupDomain aus und geben Sie die Datenbankverbindungsinformationen an.

   Beim Ausführen des BackupDomain-Befehls sichert infasetup die meisten Datenbanktabellen für die Domänenkonfiguration in der Datei, deren Namen Sie angeben.

   Hinweis: Wenn der infasetup-Backup- oder infasetup-Wiederherstellungsbefehl mit einem Java-Speicherfehler fehlschlägt, stellen Sie für infasetup mehr Systemspeicher zur Verfügung. Um den Systemspeicher zu vergrößern, legen Sie den Wert -Xmx in der Umgebungsvariable INFA_JAVA_CMD_OPTS fest.
4. Verwenden Sie das Dienstprogramm zur Datenbanksicherung, um zusätzliche Repository-Tabellen manuell zu sichern, die vom infasetup-Befehl nicht gesichert werden.

   Sichern Sie die Inhalte der folgenden Tabelle:

   - ISP_RUN_LOG
5. Um das Domänenkonfigurations-Repository in der sicheren Datenbank wiederherzustellen, führen Sie den infasetup-Befehl RestoreDomain aus und geben Sie die Datenbankverbindungsinformationen an.

Geben Sie zusätzlich zu den Verbindungsinformationen die folgenden für die sichere Datenbank erforderlichen Optionen an:

Option	Argument	Beschreibung
-DatabaseTlsEnabled -dbtls	database_tls_enabled	Erforderlich. Gibt an, ob die Datenbank, in der das Domänenkonfigurations-Repository wiederhergestellt wird, eine sichere Datenbank ist. Legen Sie diese Option auf TRUE fest.
-DatabaseTruststoreLocation -dbtl	database_truststore_location	Erforderlich. Pfad und Dateiname der Truststore-Datei, die das SSL-Zertifikat für die Datenbank enthält.
-DatabaseTruststorePassword -dbtp	database_truststore_password	Erforderlich. Passwort für die Datenbank-Truststore-Datei für die sichere Datenbank.

Fügen Sie die folgenden Sicherheitsparameter zum Verbindungsstring hinzu:

EncryptionMethod

Erforderlich. Gibt an, ob Daten bei der Übertragung über das Netzwerk verschlüsselt sind. 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 festgelegt wurde, validiert Informatica das vom Datenbankserver gesendete Zertifikat. Wenn Sie einen HostNameInCertificate-Parameter eingeben, validiert Informatica ebenfalls den Hostnamen im Zertifikat.

Wenn dieser Parameter auf FALSE gesetzt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat nicht. Informatica ignoriert alle von Ihnen angegebenen Truststore-Informationen.

Der Standardwert lautet „True“.

HostNameInCertificate

Optional. Hostname des Computers, auf dem die sichere Datenbank gehostet wird. Wenn Sie einen Hostnamen angeben, validiert Informatica den Hostnamen im Verbindungsstring mit dem Hostnamen im SSL-Zertifikat.

cryptoProtocolVersion

Erforderlich für Oracle, wenn die Informatica-Domäne auf AIX ausgeführt wird und als Verschlüsselungsebene für Oracle-Datenbanken TLS festgelegt wurde. Legen Sie den Parameter auf `cryptoProtocolVersion=TLSv1,TLSv1.1,TLSv1.2` fest.

6. Verwenden Sie das Datenbank-Wiederherstellungs-Dienstprogramm, um die Repository-Tabellen wiederherzustellen, die Sie manuell gesichert haben.

   Stellen Sie die folgende Tabelle wieder her:

   - ISP_RUN_LOG

7. Führen Sie zum Aktualisieren der Knoten in der Domäne mit Informationen über das sichere Domänenkonfigurations-Repository den Befehl „infasetup UpdateGatewayNode“ aus und geben Sie die sicheren Datenbankverbindungsinformationen an.

Geben Sie zusätzlich zu den Knotenoptionen die folgenden für die sichere Datenbank erforderlichen Optionen an:

Option	Argument	Beschreibung
-DatabaseTlsEnabled -dbtls	database_tls_enabled	Erforderlich. Gibt an, ob die Datenbank, die für das Domänenkonfigurations-Repository verwendet wird, eine sichere Datenbank ist. Legen Sie diese Option auf TRUE fest.
-DatabaseConnectionString -cs	database_connection_string	Erforderlich. Verbindungsstring zum Herstellen der Verbindung mit der sicheren Datenbank. Der Verbindungsstring muss die Sicherheitsparameter enthalten, die Sie im Verbindungsstring hinzugefügt haben, als Sie den Befehl „infasetup RestoreDomain“ in Schritt 5 ausgeführt haben.
-DatabaseTruststorePassword -dbtp	database_truststore_password	Erforderlich. Passwort für die Datenbank-Truststore-Datei für die sichere Datenbank.

Wenn Sie über mehrere Gateway-Knoten in der Domäne verfügen, führen Sie infasetup UpdateGatewayNode auf jedem Gateway-Knoten aus.

8. Starten Sie die Domäne neu.

Sichere PowerCenter-Repository-Datenbank

Wenn Sie einen PowerCenter-Repository-Dienst erstellen, können Sie das zugehörige PowerCenter-Repository in einer mit dem SSL-Protokoll gesicherten Datenbank erstellen.

Der PowerCenter-Repository-Dienst stellt eine Verbindung zur PowerCenter-Repository-Datenbank über die native Konnektivität her.

Überprüfen Sie beim Erstellen eines PowerCenter-Repositorys auf einer sicheren Datenbank, dass die Datenbank-Client-Dateien die sicheren Verbindungsinformationen für die Datenbank enthalten. Wenn Sie beispielsweise einen PowerCenter-Repository auf einer sicheren Oracle-Datenbank erstellen, konfigurieren Sie die Client-Dateien tnsnames.ora und sqlnet.ora der Oracle-Datenbank mit den sicheren Verbindungsinformationen.

Sichere Modellrepository-Datenbank

Wenn Sie einen Modellrepository-Dienst erstellen, können Sie das zugehörige Modellrepository in einer mit dem SSL-Protokoll gesicherten Datenbank erstellen.

Der Modellrepository-Dienst stellt mithilfe von JDBC-Treibern eine Verbindung zur Modellrepository-Datenbank her.

1. Richten Sie eine mit dem SSL-Protokoll gesicherte Datenbank ein.
2. Erstellen Sie im Administrator-Tool einen Modellrepository-Dienst.
3. Geben Sie im Dialogfeld **Neuer Modellrepository-Dienst** die allgemeinen Eigenschaften für den Modellrepository-Dienst ein und klicken Sie auf **Weiter**.
4. Geben Sie die Datenbankeigenschaften und den JDBC-Verbindungsstring für den Modellrepository-Dienst ein.

Um eine Verbindung zu einer sicheren Datenbank herzustellen, geben Sie die sicheren Datenbankparameter im Feld **Sichere JDBC-Parameter** ein. Informatica behandelt den Wert des Felds **Sichere JDBC-Parameter** als vertrauliche Daten und speichert die verschlüsselte Parameterzeichenfolge.

Die folgende Liste beschreibt die Parameter für sichere Datenbanken:

EncryptionMethod

Erforderlich. Gibt an, ob Daten bei der Übertragung über das Netzwerk verschlüsselt sind. 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 festgelegt wurde, validiert Informatica das vom Datenbankserver gesendete Zertifikat. Wenn Sie einen HostNameInCertificate-Parameter eingeben, validiert Informatica ebenfalls den Hostnamen im Zertifikat.

Wenn dieser Parameter auf FALSE gesetzt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat nicht. Informatica ignoriert alle von Ihnen angegebenen Truststore-Informationen.

Der Standardwert lautet „True“.

HostNameInCertificate

Optional. Hostname des Computers, auf dem die sichere Datenbank gehostet wird. Wenn Sie einen Hostnamen angeben, validiert Informatica den Hostnamen im Verbindungsstring mit dem Hostnamen im SSL-Zertifikat.

cryptoProtocolVersion

Erforderlich für Oracle, wenn die Informatica-Domäne auf AIX ausgeführt wird und als Verschlüsselungsebene für Oracle-Datenbanken TLS festgelegt wurde. Legen Sie den Parameter auf `cryptoProtocolVersion=TLSv1,TLSv1.1,TLSv1.2` fest.

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: `<InformaticaInstallationDirectory>/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 zum Verbindungsstring hinzufügen, geben Sie im Feld **Sichere JDBC-Parameter** keinen Parameter ein.

5. Testen Sie die Verbindung, um sicherzustellen, dass die Verbindung zur sicheren Repository-Datenbank gültig ist.
6. Stellen Sie den Vorgang zum Erstellen eines Modellrepository-Diensts fertig.

Sichere Kommunikation für Arbeitsabläufe und Sitzungen

Wenn Sie die Option der sicheren Kommunikation für die Domäne aktivieren, sichert Informatica die Verbindung zwischen dem Datenintegrationsdienst und PowerCenter-Integrationsdienst sowie den DTM-Prozessen.

Wenn Sie zudem PowerCenter-Sitzungen auf einem Gitter ausführen, können Sie eine Option zum Sichern der Datenkommunikation zwischen den DTM-Prozessen aktivieren.

Wählen Sie zum Aktivieren der sicheren Datenkommunikation zwischen DTM-Prozessen in PowerCenter-Sitzungen die Option **Datenverschlüsselung aktivieren** für den PowerCenter-Integrationsdienst aus.

Hinweis: PowerCenter-Sitzungen benötigen mehr CPU und Speicher, wenn die DTM-Prozesse im sicheren Modus ausgeführt werden. Bevor Sie die sichere Datenkommunikation zwischen DTM-Prozessen für PowerCenter-Sitzungen aktivieren, bestimmen Sie, ob die Domänenressourcen für zusätzliches Laden ausreichend sind.

Aktivieren einer sicheren Kommunikation für PowerCenter-DTM-Prozesse

Um die Verbindung zwischen den DTM-Prozessen in PowerCenter-Sitzungen zu sichern, die auf einem Gitter ausgeführt werden, konfigurieren Sie den PowerCenter-Integrationsdienst für die Aktivierung der Datenverschlüsselung für DTM-Prozesse.

1. Wählen Sie im Navigator des Administrator-Tools den PowerCenter-Integrationsdienst aus.
2. Klicken Sie im Inhaltsbereich auf die Ansicht „Eigenschaften“.
3. Wechseln Sie zum Abschnitt der PowerCenter-Integrationsdienst-Eigenschaften und klicken Sie auf „Bearbeiten“.
4. Wählen Sie im Fenster **PowerCenter-Integrationsdienst-Eigenschaften bearbeiten** **Datenverschlüsselung aktivieren** aus.
5. Klicken Sie auf **OK**.

Beim Ausführen einer PowerCenter-Sitzung auf einem Gitter senden die DTM-Prozesse verschlüsselte Daten, wenn sie mit anderen DTM-Prozessen kommunizieren.

Sichere Verbindungen zu einem Webanwendungsdienst

Sichern Sie die Verbindung zwischen dem Webanwendungsdienst und dem Browser, um Daten zu schützen, die zwischen einem Webanwendungsdienst und dem Browser übermittelt werden.

Sie können die folgenden Verbindungen sichern:

Verbindungen zum Administrator-Tool

Sie können die Verbindung zwischen dem Administrator-Tool und dem Browser sichern.

Verbindungen zu Webanwendungsdiensten

Sie können die Verbindung zwischen den folgenden Webanwendungsdiensten und dem Browser sichern:

- Analyst-Dienst
- Hub-Konsolendienst für Webdienste
- Metadata Manager-Dienst

- Data Analyzer-Dienst

Anforderungen für sichere Verbindungen zu Webanwendungsdiensten

Stellen Sie vor dem Sichern der Verbindung zu einem Webanwendungsdienst sicher, dass 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 in einem Verzeichnis, auf das zugegriffen werden kann.

Der Schlüsselspeicher muss sich in einen Verzeichnis befinden, auf das das Administrator-Tool und die Befehlszeilenprogramme Zugriff haben.

Aktivieren sicherer Verbindungen zum Administrator-Tool

Nach der Installation können Sie über die Befehlszeile sichere Verbindungen mit dem Administrator-Tool konfigurieren.

Sie müssen die Gateway-Knoten in der Domäne mit den Eigenschaften für eine sichere Verbindung zwischen dem Browser und dem Informatica Administrator-Dienst aktualisieren.

Zum Aktualisieren des Gateway-Knotens mit den Eigenschaften der sicheren Verbindung führen Sie den folgenden Befehl aus: `infasetup UpdateGatewayNode`

Fügen Sie die folgenden Optionen hinzu:

Option	Argument	Beschreibung
-HttpsPort -hs	AdminConsole_https_port	Zu verwendende Portnummer für eine sichere Verbindung mit dem Informatica Administrator-Dienst.
-KeystoreFile -kf	AdminConsole_Keystore_File	Pfad und Dateiname der Schlüsselspeicherdatei zur Verwendung für die HTTPS-Verbindung mit dem Informatica Administrator-Dienst.
-KeystorePass -kp	AdminConsole_Keystore_Password	Passwort für die Schlüsselspeicherdatei.

Wenn Sie in der Domäne über mehrere Gateway-Knoten verfügen, führen Sie den Befehl auf jedem Gateway-Knoten aus.

Informatica-Webanwendungsdienste

Konfigurieren Sie eine sichere Verbindung für einen Webanwendungsdienst, wenn Sie diesen erstellen oder konfigurieren. Jeder Anwendungsdienst hat bestimmte Eigenschaften für die sichere HTTPS-Verbindung.

Sicherheit für das Analyst Tool

Beim Erstellen des Analyst-Dienstes können Sie die sicheren HTTPS-Eigenschaften für das Analyst Tool konfigurieren.

Um die Verbindung zwischen dem Browser und dem Analyst-Dienst zu sichern, konfigurieren Sie die folgenden Analyst-Dienst-Eigenschaften:

Eigenschaft	Beschreibung
Sichere Kommunikation aktivieren	Wählen Sie diese Option aus, um eine sichere Verbindung zwischen dem Analyst Tool und dem Analyst-Dienst zu aktivieren.
HTTPS-Port	Portnummer, auf der die Informatica Analyst-Web-Anwendung bei Aktivierung des TLS (Transport Layer Security)-Protokolls 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	Informatica empfiehlt, dieses Feld leer zu lassen. Welche TLS-Version aktiviert wird, hängt vom eingegebenen Wert ab. Bei einem leeren Feld wird die höchste der verfügbaren TLS-Versionen aktiviert. Durch Eingabe eines Werts könnten hingegen frühere TLS-Versionen aktiviert werden. Das Verhalten basiert auf der Java-Version für Ihre Umgebung. Weitere Informationen können Sie der Dokumentation für Ihre Java-Version entnehmen.

Sicherheit für die Webdienst-Hub-Konsole

Beim Erstellen des Webdienst-Hub-Dienstes können Sie die sicheren HTTPS-Eigenschaften für die Webdienst-Hub-Konsole konfigurieren.

Konfigurieren Sie zum Sichern der Verbindung zwischen dem Browser und dem Webdienst-Hub-Dienst die folgenden Webdienst-Hub-Dienst-Eigenschaften:

Eigenschaft	Beschreibung
URLScheme	Gibt das von Ihnen für den Webdienst-Hub konfigurierte Sicherheitsprotokoll an: - HTTP. Webdienst-Hub nur unter HTTP ausführen. - HTTPS. Webdienst-Hub nur unter HTTPS ausführen. - HTTP und HTTPS. Webdienst-Hub im HTTP- und HTTPS-Modus ausführen.
Hub-Portnummer (https)	Portnummer für den Webdienst-Hub, der unter HTTPS ausgeführt wird. Wird angezeigt, wenn das ausgewählte URL-Schema HTTPS enthält. Erforderlich, wenn Sie den Webdienst-Hub unter HTTPS ausführen möchten. Der Standardwert ist 7343.
Schlüsselspeicherdatei	Pfad und Dateiname der Schlüsselspeicherdatei mit den Schlüsseln und Zertifikaten, die für eine HTTPS-Verbindung erforderlich sind.
Schlüsselspeicher-Passwort	Passwort für die Schlüsselspeicherdatei. Wenn diese Eigenschaft nicht festgelegt ist, verwendet der Webdienst-Hub das Standardpasswort *changeit*.

Sicherheit für Metadata Manager

Beim Erstellen des Metadata Manager-Diensts können Sie die sicheren HTTPS-Eigenschaften für die Metadata Manager-Web-Anwendung konfigurieren.

Um die Verbindung zwischen dem Browser und dem Metadata Manager-Dienst zu sichern, konfigurieren Sie die folgenden Metadata Manager-Dienst-Eigenschaften:

Eigenschaft	Beschreibung
SSL (Secure Sockets Layer) aktivieren	Gibt an, dass Sie eine sichere Verbindung für die Metadata Manager-Webanwendung konfigurieren möchten. **Hinweis:** Diese Eigenschaft wird angezeigt, wenn Sie einen Metadata Manager-Dienst erstellen. Setzen Sie zum Sichern der Verbindung für einen vorhandenen Metadata Manager-Dienst die Konfigurationseigenschaft **URL-Schema** auf HTTPS.
Portnummer	Nummer des Ports, auf dem die Metadata Manager-Anwendung ausgeführt wird. Standardwert ist 10250.
Schlüsselspeicherdatei	Die Schlüsselspeicherdatei mit den Schlüsseln und Zertifikaten, die bei Konfiguration einer sicheren Verbindung für die Metadata Manager-Webanwendung erforderlich sind. **Hinweis:** Der Metadata Manager-Dienst verwendet RSA-Verschlüsselung. Aus diesem Grund empfiehlt Informatica die Verwendung eines Sicherheitszertifikats, das mit dem RSA-Algorithmus erzeugt wurde.
Schlüsselspeicherpasswort	Passwort für die Schlüsselspeicherdatei.

Sicherheit für Data Analyzer

Beim Erstellen des Berichterstellungsdiensts können Sie die sicheren HTTPS-Eigenschaften für Data Analyzer konfigurieren.

Um die Verbindung zwischen dem Browser und dem Berichterstellungsdienst zu sichern, konfigurieren Sie die folgende Berichterstellungsdienst-Eigenschaft:

Eigenschaft	Beschreibung
HTTPS auf Port aktivieren	Der vom Berichterstellungsdienst verwendete SSL-Port für sichere Verbindungen. Sie können den Wert bearbeiten, wenn Sie den HTTP-Port für den Knoten konfiguriert haben, auf dem Sie den Berichterstellungsdienst erstellen. Geben Sie einen Wert zwischen 1 und 65535 ein und stellen Sie sicher, dass sich der Wert von dem des HTTP-Ports unterscheidet. Falls der Knoten, auf dem Sie den Berichterstellungsdienst erstellen, nicht für den HTTPS-Port konfiguriert ist, dürfen Sie HTTPS nicht für den Berichterstellungsdienst konfigurieren. Standardwert ist 16443.

Chiffre-Suites für die Informatica-Domäne

Sie können die Chiffre-Suites konfigurieren, die von der Informatica-Domäne beim Verschlüsseln von Verbindungen innerhalb der Informatica-Domäne verwendet werden. Verbindungen der Informatica-Domäne mit Ressourcen außerhalb der Domäne sind von der Konfiguration der Chiffre-Suites nicht betroffen.

Wenn Sie sichere Kommunikation für die Informatica-Domäne oder sichere Verbindungen mit Webanwendungsdiensten aktivieren, verwendet die Informatica-Domäne Chiffre-Suites zum Verschlüsseln des Verkehrs.

Informatica erstellt die Gültigkeitsliste mit Chiffre-Suites basierend auf den folgenden Listen:

Blacklist

Liste mit Chiffre-Suites, die von der Informatica-Domäne blockiert werden sollen. Wenn Sie eine Chiffre-Suite auf die Blacklist setzen, entfernt die Informatica-Domäne die Chiffre-Suite aus der Gültigkeitsliste. Sie können Chiffre-Suites, die sich in der Standardliste befinden, zur Blacklist hinzufügen.

Standardliste

Liste mit Chiffre-Suites, die von der Informatica-Domäne standardmäßig unterstützt werden. Wenn Sie keine Whitelist oder Blacklist konfigurieren, verwendet die Informatica-Domäne die Standardliste als Gültigkeitsliste.

Weitere Informationen finden Sie unter Anhang B, “Standardliste der Chiffre-Suites” auf Seite 216

Whitelist

Liste mit Chiffre-Suites, die von der Informatica-Domäne unterstützt werden sollen. Wenn Sie der Whitelist eine Chiffre-Suite hinzufügen, fügt die Informatica-Domäne die Chiffre-Suite zur Gültigkeitsliste hinzu. Chiffre-Suites, die sich in der Standardliste befinden, müssen nicht zur Whitelist hinzugefügt werden.

Informatica erstellt die Gültigkeitsliste, indem Chiffre-Suites in der Whitelist zur Standardliste hinzugefügt und Chiffre-Suites in der Blacklist aus der Standardliste entfernt werden.

Beachten Sie die folgenden Richtlinien für Gültigkeitsliste:

- Zur Verwendung einer benutzerdefinierten Gültigkeitsliste für sichere Verbindungen mit Webclients muss die Informatica-Domäne sichere Kommunikation innerhalb der Domäne einsetzen. Wenn in der Domäne keine sichere Kommunikation eingesetzt wird, verwendet Informatica die Standardliste als Gültigkeitsliste.
- Die Gültigkeitsliste steuert ausschließlich Verbindungen innerhalb der Informatica-Domäne. Verbindungen mit Datenquellen verwenden die Gültigkeitsliste nicht.
- Die Gültigkeitsliste muss mindestens eine Chiffre-Suite enthalten, die von TLS v1.1 oder 1.2 unterstützt wird.
- Bei der Gültigkeitsliste muss es sich um eine gültige Chiffre-Suite für Windows, die Java-Laufzeitumgebung und OpenSSL handeln.

Installieren Sie zum Erreichen einer höheren Sicherheitsstufe die JCE (Java Cryptography Extension), um Unterstützung für Chiffre-Suites zu aktivieren, die AES-256 verwenden.

Erstellen von Listen mit Chiffre-Suites

Bevor Sie die Informatica-Domäne zur Verwendung bestimmter Chiffre-Suites konfigurieren können, erstellen Sie eine Whitelist zur Angabe von Chiffre-Suites, die zusätzlich zur Standardliste unterstützt werden sollen, oder eine Blacklist zur Angabe der zu blockierenden Chiffre-Suites.

Arbeiten Sie mit dem für die Netzwerksicherheit zuständigen Administrator zusammen, um die für die Informatica-Domäne geeigneten Chiffre-Suites festzulegen.

Bei der Liste mit Chiffre-Suites muss es sich um eine kommagetrennte Liste handeln. Verwenden Sie die IANA-Namen (Internet Assigned Numbers Authority) für die Chiffre-Suites in der Liste. Alternativ können Sie einen regulären Java-Ausdruck verwenden.

Sie können die Whitelist und Blacklist mit den Befehlszeilenprogrammen konfigurieren. Sie können die Listen direkt in Befehlsparametern bereitstellen oder Klartextdateien angeben, die kommagetrennte Listen enthalten.

Der folgende Beispieltext zeigt eine Liste mit zwei Chiffre-Suites:

```
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

Sie können die Whitelist und Blacklist mit Chiffre-Suites für die Informatica-Domäne konfigurieren, wenn Sie die Domäne erstellen. Sie müssen die Befehlszeilenprogramme verwenden, um die Informatica-Domäne sowie die Gateway- und Arbeitsknoten zu erstellen. Weitere Informationen finden Sie in den Einträgen für die folgenden Befehle in der *Informatica-Befehlsreferenz*: DefineDomain, DefineGatewayNode und DefineWorkerNode.

Alternativ können Sie die Whitelist und Blacklist für eine vorhandene Informatica-Domäne konfigurieren.

Konfigurieren der Informatica-Domäne anhand einer neuen Gültigkeitsliste mit Chiffre-Suites

Zum Konfigurieren der von der Informatica-Domäne verwendeten Chiffre-Suites müssen Sie die Informatica-Domäne, alle Gateway- sowie Arbeitsknoten mit der gleichen Whitelist und Blacklist aktualisieren.

Hinweis: Änderungen an der Blacklist, Whitelist und der Gültigkeitsliste sind nicht kumulativ. Informatica erstellt eine neue Gültigkeitsliste basierend auf der Blacklist, der Whitelist und der Standardliste, wenn Sie den Befehl ausführen. Die neue Gültigkeitsliste überschreibt die vorherige Liste.

Führen Sie die folgenden Schritte durch, um eine vorhandene Informatica-Domäne anhand einer neuen Gültigkeitsliste mit Chiffre-Suites zu konfigurieren:

1. Fahren Sie die Informatica-Domäne herunter.

2. Führen Sie optional den infasetup listDomainCiphers-Befehl aus, um die Listen mit Chiffre-Suites anzuzeigen, die von einer Domäne oder einem Knoten unterstützt oder blockiert werden.

   Führen Sie beispielsweise den folgenden Befehl aus, um alle Listen mit Chiffre-Suites anzuzeigen:

   ```
   infasetup listDomainCiphers -l ALL -dc true
   ```

3. Führen Sie den infasetup updateDomainCiphers-Befehl auf einem Gateway-Knoten aus und geben Sie eine Whitelist, eine Blacklist oder beide an.

   Führen Sie beispielsweise den folgenden Befehl aus, um der Gültigkeitsliste eine Chiffre-Suite hinzuzufügen und zwei Chiffre-Suites aus der Gültigkeitsliste zu entfernen:

   ```
   infasetup updateDomainCiphers -cwl TLS_DHE_DSS_WITH_AES_128_CBC_SHA -cbl
   TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_3DES_EDE_CBC_SHA
   ```

4. Führen Sie den infasetup updateGatewayNode-Befehl auf allen Gateway-Knoten aus und geben Sie eine Whitelist, eine Blacklist oder beide an.

   Verwenden Sie dieselbe Whitelist und Blacklist wie die Domäne.

   Führen Sie beispielsweise folgenden Befehl aus:

   ```
   infasetup updateGatewayNode -cwl TLS_DHE_DSS_WITH_AES_128_CBC_SHA -cbl
   TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_3DES_EDE_CBC_SHA
   ```

5. Aktualisieren Sie alle Arbeitsknoten mit dem gleichen Satz an Chiffre-Suites wie die Informatica-Domäne.

   Verwenden Sie dieselbe Whitelist und Blacklist wie die Domäne.

   Führen Sie beispielsweise folgenden Befehl aus:

   ```
   infasetup updateWorkerNode -cwl TLS_DHE_DSS_WITH_AES_128_CBC_SHA -cbl
   TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_3DES_EDE_CBC_SHA
   ```

6. Starten Sie die Informatica-Domäne.

7. Führen Sie optional den infacmd isp listDomainCiphers-Befehl aus, um die Listen mit Chiffre-Suites anzuzeigen, die von einer Domäne oder einem Knoten verwendet werden.

   Führen Sie beispielsweise den folgenden Befehl aus, um die Gültigkeitsliste mit Chiffre-Suites anzuzeigen, die von der Domäne verwendet wird:

   ```
   infacmd isp listCiphers -l EFFECTIVE -dc true
   ```

Sichere Quellen und Ziele

Informatica verwendet Verbindungsobjekte, um eine Verbindung zu relationalen Datenbanken als Quelle oder Ziel herzustellen. Sie können ein Verbindungsobjekt für eine relationale Datenbank erstellen, die mit einem SSL-Zertifikat gesichert ist.

Sie können PowerCenter-Verbindungsobjekte im Arbeitsablauf-Manager erstellen. Sie erstellen die Datendienst-, Datenqualitäts- oder Profilerstellungsverbindung im Developer-Tool oder im Administrator-Tool.

Sie können eine Verbindung zu einer sicheren Quelle bzw. zu einem sicheren Ziel auf den folgenden Datenbanken erstellen:

- Oracle
- Microsoft SQL Server
- IBM DB2

Datenintegrationsdienst-Quellen und -Ziele

Wenn Sie ein Verbindungsobjekt für den Datenintegrationsdienst zum Verarbeiten von Mappings, Datenprofilen, Scorecards bzw. SQL-Datendiensten erstellen, können Sie eine Verbindung zu einer mit dem SSL-Protokoll gesicherten Datenbank definieren.

Der Datenintegrationsdienst stellt eine Verbindung zur Quell- bzw. Zieldatenbank über JDBC-Treiber her. Wenn Sie die Verbindung zu einer sicheren Repository-Datenbank konfigurieren, müssen Sie die sicheren Verbindungsparameter zum JDBC-Verbindungsstring hinzufügen.

1. Richten Sie eine mit dem SSL-Protokoll gesicherte Datenbank ein, um sie als Quelle oder Ziel zu verwenden.
2. Erstellen Sie eine Verbindung im Administrator-Tool.
3. Wählen Sie im Dialogfeld **Neue Verbindung** den Verbindungstyp aus und klicken Sie auf **OK**.

   Sie können eine Verbindung zu einer sicheren DB2-, Microsoft SQL Server- oder Oracle-Datenbank herstellen.
4. Geben Sie im Dialogfeld **Neue Verbindung - Schritt 1 von 3** die Eigenschaften für die Verbindung ein und klicken Sie auf **Weiter**.
5. Geben Sie auf der Seite **Neue Verbindung - Schritt 2 von 3** den Verbindungsstring zur Datenbank ein.

   Um eine Verbindung zu einer sicheren Datenbank herzustellen, geben Sie die sicheren Datenbankparameter im Feld **Erweiterte JDBC-Sicherheitsoptionen** ein. Informatica behandelt den Wert des Felds **Erweiterte JDBC-Sicherheitsoptionen** als vertrauliche Daten und speichert die verschlüsselte Parameterzeichenfolge.

   Die folgende Liste beschreibt die Parameter für sichere Datenbanken:

   EncryptionMethod

   Erforderlich. Gibt an, ob Daten bei der Übertragung über das Netzwerk verschlüsselt sind. 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 festgelegt wurde, validiert Informatica das vom Datenbankserver gesendete Zertifikat. Wenn Sie einen HostNameInCertificate-Parameter eingeben, validiert Informatica ebenfalls den Hostnamen im Zertifikat.

   Wenn dieser Parameter auf FALSE gesetzt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat nicht. Informatica ignoriert alle von Ihnen angegebenen Truststore-Informationen.

   Der Standardwert lautet „True“.

   HostNameInCertificate

   Optional. Hostname des Computers, auf dem die sichere Datenbank gehostet wird. Wenn Sie einen Hostnamen angeben, validiert Informatica den Hostnamen im Verbindungsstring mit dem Hostnamen im SSL-Zertifikat.

   TrustStore

   Erforderlich. Pfad und Dateiname der Truststore-Datei, die das SSL-Zertifikat für die Datenbank enthält.

   TrustStorePassword

   Erforderlich. Passwort der Truststore-Datei für die sichere Datenbank.

Hinweis: Informatica hängt die sicheren JDBC-Parameter an den Verbindungsstring an. Wenn Sie die sicheren JDBC-Parameter direkt zum Verbindungsstring hinzufügen, geben Sie im Feld **Erweiterte JDBC-Sicherheitsoptionen** keine Parameter ein.

6. Testen Sie die Verbindung, um sicherzustellen, dass die Verbindung zur sicheren Datenbank gültig ist.
7. Stellen Sie den Prozess zum Erstellen der relationalen Verbindung fertig.

PowerCenter-Quellen und -Ziele

Wenn Sie ein Verbindungsobjekt für eine PowerCenter-Sitzung erstellen, können Sie eine Verbindung zu einer mit dem SSL-Protokoll gesicherten Datenbank definieren.

Sie können eine Verbindung zu relationalen PowerCenter-Quellen und -Zielen über die native Konnektivität oder ODBC-Treiber herstellen.

Wenn Sie eine Verbindung zu einer sicheren relationalen Quelle bzw. zu einem sicheren relationalen Ziel über die native Konnektivität herstellen, stellen Sie sicher, dass der Datenbank-Client die Verbindungsinformationen für die sichere Datenbank enthält. Wenn Sie beispielsweise eine Verbindung zu einem PowerCenter-Ziel auf einer sicheren Oracle-Datenbank erstellen, konfigurieren Sie die Oracle-Datenbank-Client-Datei *tnsnames.ora* mit den Verbindungsinformationen für die sichere Datenbank.

Wenn Sie eine Verbindung zu einer sicheren relationalen Quelle bzw. zu einem sicheren relationalen Ziel über ODBC-Treiber herstellen, stellen Sie sicher, dass der Datenbank-Client die Verbindungsinformationen für die sichere Datenbank enthält und dass die ODBC-Datenquelle die Verbindung zur sicheren Datenbank korrekt definiert.

Sicherer Datenspeicher

Informatica verschlüsselt vertrauliche Daten wie Passwörter und sichere Verbindungsparameter, bevor die Daten im Domänenkonfigurations-Repository gespeichert werden. Informatica verwendet ein Schlüsselwort, das Sie zum Erstellen eines Verschlüsselungsschlüssels bereitstellen, mit dem vertrauliche Daten verschlüsselt werden sollen.

Während der Installation müssen Sie ein Schlüsselwort für das Installationsprogramm bereitstellen, um den Verschlüsselungsschlüssel für die Domäne zu generieren. Alle Knoten in einer Domäne müssen denselben Verschlüsselungsschlüssel verwenden. Bei einer Installation auf mehreren Knoten verwendet das Installationsprogramm denselben Verschlüsselungsschlüssel für alle Knoten in der Domäne. Weitere Informationen zum Generieren eines Verschlüsselungsschlüssels für die Domäne während der Installation finden Sie in den Informatica-Installationshandbüchern.

Nach der Installation können Sie den Verschlüsselungsschlüssel für die Domäne ändern. Führen Sie den infasetup-Befehl aus, um einen Verschlüsselungsschlüssel zu generieren und den Verschlüsselungsschlüssel für die Domäne zu ändern. Nachdem Sie den Verschlüsselungsschlüssel für die Domäne geändert haben, müssen Sie den Inhalt der Repositorys in der Domäne aktualisieren, um die verschlüsselten Daten zu aktualisieren.

Hinweis: Sie müssen den Namen der Domäne, das Schlüsselwort für den Verschlüsselungsschlüssel und die Verschlüsselungsschlüssel-Datei an einem sicheren Speicherort aufbewahren. Der Domänenname, das Schlüsselwort und der Verschlüsselungsschlüssel werden benötigt, wenn Sie den Verschlüsselungsschlüssel für die Domäne ändern oder ein Repository in eine andere Domäne verschieben. Wenn Sie die Verschlüsselungsschlüssel-Datei verlieren, benötigen Sie das Schlüsselwort, um den Verschlüsselungsschlüssel erneut zu generieren. Wenn Sie das Schlüsselwort und den

Verschlüsselungsschlüssel verlieren, können Sie den Verschlüsselungsschlüssel für die Domäne nicht ändern bzw. ein Repository nicht in eine andere Domäne verschieben.

Sicheres Verzeichnis unter UNIX

Wenn Sie Informatica installieren, erstellt das Installationsprogramm ein Verzeichnis zum Speichern von Informatica-Dateien, die eingeschränkten Zugriff benötigen, wie die Verschlüsselungsschlüsseldatei der Domäne. Das Installationsprogramm weist unter UNIX unterschiedliche Berechtigungen für das Verzeichnis und die Dateien im Verzeichnis zu.

Standardmäßig erstellt das Installationsprogramm das folgende Verzeichnis im Informatica-Installationsverzeichnis, um den Verschlüsselungsschlüssel zu speichern: `<INFA_HOME>/isp/config/keys`.

Das Verzeichnis „/keys“ enthält die Verschlüsselungsschlüsseldatei für den Knoten. Wenn Sie die Domäne konfigurieren, um die Kerberos-Authentifizierung zu verwenden, enthält das Verzeichnis auch die Kerberos-Keytab-Dateien.

Während der Installation können Sie ein anderes Verzeichnis festlegen, in dem die Verschlüsselungsdatei gespeichert werden soll. Das Installationsprogramm weist dieselben Berechtigungen zum angegebenen Verzeichnis wie das Standardverzeichnis zu.

Das Verzeichnis „/keys“ und die Dateien im Verzeichnis enthalten die folgenden Berechtigungen:

Verzeichnisberechtigungen

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

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

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

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

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

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

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

Dateiberechtigungen

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

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

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

Ändern des Verschlüsselungsschlüssels über die Befehlszeile

Nach der Installation können Sie den Verschlüsselungsschlüssel für die Domäne über die Befehlszeile ändern. Sie müssen die Domäne herunterfahren, bevor Sie den Verschlüsselungsschlüssel ändern.

Verwenden Sie den infasetup-Befehl zum Generieren eines Verschlüsselungsschlüssels und konfigurieren Sie die Domäne, um den neuen Verschlüsselungsschlüssel zu verwenden.

Die folgenden infasetup-Befehle generieren und ändern den Verschlüsselungsschlüssel:

generateEncryptionKey

Generiert einen Verschlüsselungsschlüssel in einer Datei mit dem Namen *sitekey*. Wenn das für den Verschlüsselungsschlüssel angegebene Verzeichnis eine Datei mit dem Namen „sitekey“ enthält, benennt Informatica die Datei in *siteKey_old* um.

migrateEncryptionKey

Ändert den Verschlüsselungsschlüssel, der zum Speichern von vertraulichen Daten in der Informatica-Domäne verwendet wird.

Hinweis: Wenn die Domäne enthält einen Berichterstellungsdienst enthält, ändern Sie den Verschlüsselungsschlüssel nicht. Der Befehl „migrateEncryptionKey“ schlägt fehl, wenn die Domäne einen Berichterstellungsdienst enthält.

Führen Sie zum Ändern des Verschlüsselungsschlüssels für eine Domäne die folgenden Schritte durch:

1. Fahren Sie die Domäne herunter.
2. Sichern Sie die Domäne, bevor Sie den Verschlüsselungsschlüssel ändern.

   Um sicherzustellen, dass Sie die Domäne wiederherstellen können, wenn Probleme beim Ändern des Verschlüsselungsschlüssels auftreten, sichern Sie die Domäne vor dem Ausführen der infasetup-Befehle.
3. Führen Sie zum Generieren eines Verschlüsselungsschlüssels für die Domäne den infasetup-Befehl „generateEncryptionKey“ aus.

Geben Sie die folgenden Optionen zum Generieren eines Verschlüsselungsschlüssels an:

Option	Argument	Beschreibung
-keyword -kw	keyword	Die Textzeichenfolge, die als Basiswort verwendet wird, aus dem ein Verschlüsselungsschlüssel generiert werden soll. Das Schlüsselwort muss die folgenden Kriterien erfüllen: - Hat eine Länge von 8 bis 20 Zeichen - Enthält mindestens einen Großbuchstaben - Enthält mindestens einen Kleinbuchstaben - Enthält mindestens eine Zahl - Enthält keine Leerzeichen
-domainName -dn	domain_name	Name der Informatica-Domäne.
-encryptionKeyLocation -kl	encryption_key_location	Verzeichnis, das den aktuellen Verschlüsselungsschlüssel enthält. Der Name der Verschlüsselungsdatei lautet *sitekey*. Informatica benennt die aktuelle *sitekey*-Datei in *sitekey_old* um und generiert einen Verschlüsselungsschlüssel in einer neuen Datei mit dem Namen *sitekey* im selben Verzeichnis.

4. Führen Sie zum Ändern des Verschlüsselungsschlüssels für die Domäne den Befehl „infasetup migrateEncryptionKey“ aus und geben Sie den Speicherort des alten und neuen Verschlüsselungsschlüssels an.

Geben Sie die folgenden Optionen an, die zum Ändern des Verschlüsselungsschlüssels für die Domäne erforderlich sind:

Option	Argument	Beschreibung
-LocationOfEncryptionKeys -loc	location_of_encryption_keys	Verzeichnis, in dem die alte Verschlüsselungsschlüsseldatei mit dem Namen *siteKey_old* und die neue Verschlüsselungsschlüsseldatei mit dem Namen *siteKey* gespeichert sind. Das Verzeichnis muss die alten und neuen Verschlüsselungsschlüsseldateien enthalten. Wenn die alten und neuen Verschlüsselungsschlüsseldateien in verschiedenen Verzeichnissen gespeichert werden, kopieren Sie die Verschlüsselungsschlüsseldateien in dasselbe Verzeichnis. Wenn die Domäne mehrere Knoten enthält, muss dieses Verzeichnis allen Knoten in der Domäne zugänglich sein, in der Sie den Befehl „migrateEncryptionKey“ ausführen. **Hinweis:** Unter UNIX wird beim Dateinamen *siteKey_old* die Groß- und Kleinschreibung berücksichtigt. Wenn Sie die vorherige Verschlüsselungsschlüsseldatei manuell umbenennen, überprüfen Sie die Groß- und Kleinschreibung beim Dateinamen auf ihre Richtigkeit.
-IsDomainMigrated -mig	is_domain_migrated	Gibt an, ob die Domäne für die Verwendung des neuesten Verschlüsselungsschlüssels aktualisiert wurde. Beim erstmaligen Ausführen des Befehls „migrateEncryptionKey“ legen Sie diese Option auf FALSE fest, um anzugeben, dass die Domäne den alten Verschlüsselungsschlüssel verwendet. Nach dem erstmaligen Ausführen des Befehls „migrateEncryptionKey“ zum Aktualisieren anderer Knoten in der Domäne setzen Sie diese Option auf TRUE fest, um anzugeben, dass die Domäne für die Verwendung des neuesten Verschlüsselungsschlüssels aktualisiert wurde. Sie können den Befehl „migrateEncryptionKey“ auch ohne diese Option ausführen. Standardwert ist „true“.

5. Führen Sie den infasetup-Befehl auf jedem Knoten in der Domäne aus.

   Wenn die Domäne mehrere Knoten enthält, führen Sie „infasetup migrateEncryptionKey“ auf jedem Knoten aus. Führen Sie den Befehl auf den Gateway-Knoten aus, bevor Sie den Befehl auf den Arbeitsknoten ausführen. Sie können die IsDomainMigrated-Option nach dem erstmaligen Ausführen des Befehls ausführen.

6. Starten Sie die Domäne neu.

   Sie müssen ein Upgrade für alle Repository-Dienste in der Domäne ausführen, um vertrauliche Daten in den Repositorys mit dem neuen Verschlüsselungsschlüssel zu aktualisieren und zu verschlüsseln.

7. Aktualisieren Sie alle Modellrepository-Dienste, PowerCenter-Repository-Dienste und Metadata Manager-Dienste.

   Upgrades für Modellrepository-Dienste und PowerCenter-Repository-Dienste können Sie im Administrator-Tool oder an der Eingabeaufforderung durchführen. Upgrades für Metadata Manager-Dienste können Sie im Administrator-Tool ausführen.

   Hinweis: Der Metadata Manager-Dienst muss deaktiviert werden, bevor Sie das Upgrade des Diensts durchführen können.

   Wählen Sie im Kopfzeilenbereich des Administrator-Tool **Verwalten** > **Upgrade**, um ein Upgrade für einen Dienst durchzuführen. Wenn Sie mehrere Dienste wählen, führt das Administrator-Tool die Upgrades für die Dienste in der richtigen Reihenfolge durch.

   Verwenden Sie einen der folgenden Befehle, um ein Upgrade für einen Dienst an der Eingabeaufforderung durchzuführen:

Repository-Diensttyp	Befehl
Modellrepository-Dienst	`infacmd mrs UpgradeContents`
PowerCenter-Repository-Dienst	`pmrep Upgrade`

Anwendungsdienste und Ports

Informatica-Domänendienste und Anwendungsdienste in der Informatica-Domäne haben eindeutige Ports.

Informatica-Domäne

Die folgende Tabelle listet den mit der Informatica-Domäne verbundenen Standardport auf:

Typ	Standardport
Domänenkonfiguration	Standardwert ist 6005. Sie können den Standardport während der Installation ändern. Sie können den Port nach der Installation mit dem Befehl „infasetup updateGatewayNode” ändern.
Dienstmanager	6006
Zum Herunterfahren des Dienstmanagers	6007
Informatica Administrator (HTTP)	6008
Informatica Administrator (HTTPS)	8443
Zum Herunterfahren von Informatica Administrator	6009
Dienstprozess (Minimum)	6013
Dienstprozess (Maximum)	6113

Analyst-Dienst

Die folgende Tabelle listet den mit dem Analyst-Dienst verbundenen Standardport auf:

Typ	Standardport
Analyst-Dienst (HTTP)	8085
Analyst-Dienst (HTTPS)	Kein Standardport. Geben Sie die erforderliche Portnummer beim Erstellen des Dienstes ein.
Analyst-Dienst (Staging-Datenbank)	Kein Standardport. Geben Sie die Portnummer der Datenbank ein.

Content-Managementdienst

Die folgende Tabelle listet den mit dem Content-Managementdienst verbundenen Standardport auf:

Typ	Standardport
Content-Managementdienst (HTTP)	8105
Content-Managementdienst (HTTPS)	Kein Standardport. Geben Sie die erforderliche Portnummer beim Erstellen des Dienstes ein.

Data Director-Dienst

Die folgende Tabelle listet den mit dem Data Director-Dienst verbundenen Standardport auf:

Typ	Standardport
Data Director-Dienst (HTTP)	Kein Standardport. Geben Sie die erforderliche Portnummer beim Erstellen des Dienstes ein.
Data Director-Dienst (HTTPS)	Kein Standardport. Geben Sie die erforderliche Portnummer beim Erstellen des Dienstes ein.

Datenintegrationsdienst

Die folgende Tabelle listet den mit dem Datenintegrationsdienst verbundenen Standardport auf:

Typ	Standardport
Datenintegrationsdienst (HTTP-Proxy)	8085
Datenintegrationsdienst (HTTP)	8095
Datenintegrationsdienst (HTTPS)	Kein Standardport. Geben Sie die erforderliche Portnummer beim Erstellen des Dienstes ein.
Profiling-Warehouse-Datenbank	Kein Standardport. Geben Sie die Portnummer der Datenbank ein.
Human-Task-Datenbank	Kein Standardport. Geben Sie die Portnummer der Datenbank ein.

Metadata Manager-Dienst

Die folgende Tabelle listet den mit dem Metadata Manager-Dienst verbundenen Standardport auf:

Typ	Standardport
Metadata Manager-Dienst (HTTP)	Standardwert ist 10250.
Metadata Manager-Dienst (HTTPS)	Kein Standardport. Geben Sie die erforderliche Portnummer beim Erstellen des Dienstes ein.

PowerExchange-Listenerdienst

Verwenden Sie dieselbe Portnummer, die Sie in der SVCNODE-Anweisung in der DBMOVER-Datei angegeben haben.

Wenn Sie mehr als einen Listener Service für die Ausführung auf einem Knoten definieren, müssen Sie für jeden Dienst eine eindeutige SVCNODE-Portnummer definieren.

PowerExchange-Protokollierungsdienst

Verwenden Sie dieselbe Portnummer, die Sie in der SVCNODE-Anweisung in der DBMOVER-Datei angegeben haben.

Wenn Sie mehr als einen Listener Service für die Ausführung auf einem Knoten definieren, müssen Sie für jeden Dienst eine eindeutige SVCNODE-Portnummer definieren.

Berichterstellungsdienst

Die folgende Tabelle listet den mit dem Berichterstellungsdienst verbundenen Standardport auf:

Typ	Standardport
Berichterstellungsdienst (HTTP)	16080
Berichterstellungsdienst (HTTPS)	16443

Berichterstellungs- und Dashboard-Dienst (veraltet)

Die folgende Tabelle listet den mit dem Berichterstellungs- und Dashboard-Dienst verbundenen Standardport auf:

Typ	Standardport
Berichterstellungs- und Dashboard-Dienst (HTTP)	Kein Standardport. Geben Sie die erforderliche Portnummer beim Erstellen des Dienstes ein.
Berichterstellungs- und Dashboard-Dienst (HTTPS)	Kein Standardport. Geben Sie die erforderliche Portnummer beim Erstellen des Dienstes ein.

Webdienst-Hub-Dienst

Die folgende Tabelle listet den mit dem Webdienst-Hub-Dienst verbundenen Standardport auf:

Typ	Standardport
Webdienst-Hub-Dienst (HTTP)	7333
Webdienst-Hub-Dienst (HTTPS)	7343

KAPITEL 6

Sicherheitsverwaltung in Informatica Administrator

Dieses Kapitel umfasst die folgenden Themen:

Informatica Administrator verwenden - Übersicht

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

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

Administrative Domänenaufgaben

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

Administrative Domänenaufgaben

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

Administrative Domänenaufgaben

Verwalten von Protokollen, Domänenobjekten und Benutzerberechtigungen.

Administrative Sicherheitsaufgaben:

Verwalten von Benutzern, Gruppen, Rollen und Berechtigungen.

Im Administrator-Tool gibt es folgende Registerkarten:

Domäne

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

Protokolle

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

Überwachung

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

Überwachung

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

Überwachung

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

Überwachung

Ansicht und Überwachen von Ultra Messaging-Bereitstellungen.

Berichte

Ausführen eines Webdienstberichts oder eines Lizenzverwaltungsberichts.

Sicherheit

Verwalten von Benutzern, Gruppen, Rollen und Berechtigungen.

Sicherheit

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

Sicherheit

Verwalten von Benutzern, Gruppen, Rollen und Berechtigungen.

Das Administrator-Tool besitzt die folgenden Kopfzeileneinträge:

Abmelden

Abmelden vom Administrator-Tool.

Verwalten

Verwalten Ihres Kontos.

Hilfe

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

Hilfe

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

Hilfe

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

Benutzersicherheit

Der Dienstmanager und einige Anwendungsdienste steuern die Benutzersicherheit in den Anwendungs-Clients. Zu den Anwendungs-Clients gehören der Data Analyzer, Informatica Administrator, Informatica Analyst, Informatica Developer, Metadata Manager und der PowerCenter Client. Der Dienstmanager und einige Anwendungsdienste steuern die Benutzersicherheit in den Anwendungs-Clients. Zu den Anwendungs-Clients gehören Informatica Administrator und Informatica Developer. Der Dienstmanager und einige Anwendungsdienste steuern die Benutzersicherheit in den Anwendungs-Clients. Der Anwendungs-Client enthält Informatica Administrator.

Der Dienstmanager und die Anwendungsdienste steuern die Benutzersicherheit durch die Ausführung folgender Funktionen:

Verschlüsselung

Wenn Sie sich bei einer Client-Anwendung anmelden, verschlüsselt der Dienstmanager das Passwort.

Authentifizierung

Wenn Sie sich bei einer Client-Anwendung anmelden, authentifiziert der Dienstmanager Ihr Benutzerkonto auf der Basis Ihres Benutzernamens und Passworts oder anhand Ihres Benutzer-Authentifizierungs-Tokens.

Autorisierung

Wenn Sie ein Objekt in einem Anwendungs-Client anfordern, autorisieren der Dienstmanager und einige andere Anwendungsdienste die Anforderung anhand Ihrer Berechtigungen und Rollen.

Sie können HTTPS ebenfalls für die sichere Verbindung zur Domäne und zu den Anwendungsdiensten verwenden. Die folgenden Anwendungsdienste stellen eine HTTPS-Verbindung zusammen mit der Informatica-Domäne bereit:

- Datenintegrationsdienst
- Analyst-Dienst
- Content-Managementdienst
- Metadata Manager-Dienst
- Berichterstellungsdienst
- Berichterstellungs- und Dashboard-Dienst
- Webdienst-Hub-Dienst

Sie können HTTPS ebenfalls für die sichere Verbindung zur Domäne und zu den Anwendungsdiensten verwenden. Die folgenden Anwendungsdienste unterstützen die HTTPS-Verbindung zusammen mit der Informatica-Domäne:

- Datenintegrationsdienst
- Analyst-Dienst

Sie können HTTPS ebenfalls für die sichere Verbindung zur Domäne und zu den Anwendungsdiensten verwenden.

Verschlüsselung

Informatica verschlüsselt Passworte, die von Anwendungs-Clients an den Service Manager geschickt werden. Informatica verwendet die AES-Verschlüsselung mit mehrfachen 128-Bit-Schlüsseln, um Passwörter in der Domänenkonfigurationsdatenbank zu verschlüsseln. Konfigurieren Sie HTTPS, um Passwörter zu verschlüsseln, die von Anwendungs-Clients an den Service Manager geschickt werden.

Authentifizierung

Der Service Manager authentifiziert Benutzer, die sich bei Anwendungs-Clients anmelden.

Wenn Sie sich erstmals bei einem Client anmelden, geben Sie einen Benutzernamen, ein Passwort und die Sicherheitsdomäne ein. Eine Sicherheitsdomäne ist eine Ansammlung von Benutzerkonten und Gruppen in einer Informatica-Domäne.

Die von Ihnen gewählte Sicherheitsdomäne bestimmt die Authentifizierungsmethode, die der Service Manager zum Authentifizieren Ihres Benutzerkontos verwendet:

- Nativ. Wenn Sie sich als nativer Benutzer bei einem Anwendungs-Client anmelden, authentifiziert der Service Manager Ihren Benutzernamen und Ihr Passwort gegen die Benutzerkonten in der Datenbank für die Domänenkonfiguration.
- Lightweight Directory Access Protocol (LDAP) Melden Sie sich bei einem Anwendungs-Client als LDAP-Benutzer an, übergibt der Service Manager Ihren Benutzernamen und Ihr Passwort an den externen LDAP-Verzeichnisdienst für die Authentifizierung.

Wenn Sie sich als nativer Benutzer bei einem Anwendungs-Client anmelden, authentifiziert der Service Manager Ihren Benutzernamen und Ihr Passwort gegen die Benutzerkonten in der Datenbank für die Domänenkonfiguration.

Wenn Sie sich als nativer Benutzer bei einem Anwendungs-Client anmelden, authentifiziert der Service Manager Ihren Benutzernamen und Ihr Passwort gegen die Benutzerkonten in der Datenbank für die Domänenkonfiguration.

Single Sign-On

Nach der Anmeldung bei einem Anwendungs-Client ermöglicht der Service Manager es Ihnen, einen anderen Anwendungs-Client zu starten, um auf mehrere Repositorys innerhalb des Anwendungs-Client zugreifen. Sie müssen sich bei der zusätzlichen Anwendung dem oder Client-Repository nicht anmelden.

Beim ersten Start authentifiziert der Service Manager Ihr Benutzerkonto, erstellt einen verschlüsselten Authentifizierungs-Token für Ihr Konto und gibt den Authentifizierungs-Token an die Client-Anwendung zurück. Der Authentifizierungs-Token enthält Benutzernamen, Sicherheits-Domäne und eine Ablaufzeit. Der Service Manager erneuert in regelmäßigen Abständen, vor Ablauf der Gültigkeit, den Authentifizierungs-Token.

Wenn Sie einen Anwendungs-Client von einem anderen aus starten, übergibt der Anwendungs-Client den Authentifizierungs-Token an den nächsten Anwendungs-Client. Der nächste Anwendungs-Client sendet den Authentifizierungs-Token an den Service Manager, um den Benutzer zu authentifizieren.

Wenn Sie innerhalb eines Anwendungs-Client auf mehrere Repositorys zugreifen, sendet der Anwendungs-Client den Authentifizierungs-Token an den Service Manager, um den Benutzer zu authentifizieren.

Autorisierung

Der Service Manager autorisiert Benutzeranfragen für Domänenobjekte. Anfragen können vom Administrator-Tool ausgehen. Folgende Anwendungsdienste autorisieren Benutzeranfragen für andere Objekte:

- Datenintegrationsdienst
- Metadata Manager Service
- Modellrepository-Dienst
- PowerCenter Repository Service
- Reporting Service

Der Service Manager autorisiert Benutzeranfragen für Domänenobjekte. Anfragen können vom Administrator-Tool ausgehen. Folgende Anwendungsdienste autorisieren Benutzeranfragen für andere Objekte:

- Datenintegrationsdienst
- Modellrepository-Dienst

Beim Erstellen nativer Benutzer und Gruppen oder Importieren von LDAP-Benutzern und Gruppen speichert der Service Manager die Informationen in der Domänenkonfigurationsdatenbank in folgenden Repositorys:

- Data Analyzer Repository
- Modellrepository
- PowerCenter Repository
- PowerCenter Repository für Metadata Manager

Der Service Manager synchronisiert die Benutzer- und Gruppeninformationen zwischen den Repositorys und der Datenbank für die Domänenkonfiguration, wenn folgende Ereignisse eintreten:

- Neustart des Metadata Manager Service, des Modellrepository-Diensts, des PowerCenter Repository Service oder des Reporting Service.
- Hinzufügen oder Entfernen nativer Benutzer oder Gruppen.
- Der Service Manager synchronisiert die Liste der LDAP-Benutzer und Gruppen in der Domänenkonfigurations-Datenbank mit der Liste der Benutzer und Gruppen im LDAP-Verzeichnisdienst.

Der Service Manager synchronisiert die Benutzer- und Gruppeninformationen zwischen den Repositorys und der Datenbank für die Domänenkonfiguration, wenn folgende Ereignisse eintreten:

- Neustarten des Modellrepository-Diensts.
- Hinzufügen oder Entfernen nativer Benutzer oder Gruppen.

Beim Zuordnen von Berechtigungen zu Benutzern und Gruppen in einem Anwendungs-Client speichert der Anwendungsdienst die Berechtigungszuordnungen zusammen mit den Benutzer- und Gruppeninformationen im entsprechenden Repository.

Wenn Sie ein Objekt in einem Anwendungs-Client anfordern, autorisiert der entsprechende Anwendungsdienst Ihre Anfrage. Beispiel: Bei dem Versuch, ein Projekt im Informatica Developer zu bearbeiten, autorisiert der Modellrepository-Dienst Ihre Anfrage basierend auf Ihren Rechten, Ihrer Rolle und den Ihnen zugeordneten Berechtigungen.

Registerkarte Sicherheit

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

Die Registerkarte Sicherheit besteht aus folgenden Komponenten:

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

- Menü "Sicherheitsaktionen". Enthält Optionen zum Erstellen oder Löschen einer Gruppe, eines Benutzers oder einer Rolle.
- Menü "Sicherheitsaktionen". Enthält Optionen zum Erstellen oder Löschen einer Gruppe, eines Benutzers oder einer Rolle.

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

Der Suchbereich

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

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

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

   Im Abschnitt Suchergebnis können maximal 100 Objekte angezeigt werden. Wenn die Suche mehr als 100 Objekte ergibt, schränken Sie die Suchergebnisse durch weitere Suchkriterien ein.
4. Wählen Sie ein Objekt im Abschnitt Suchergebnisse aus, um weitere Informationen zu diesem Objekt im Inhaltsfenster anzuzeigen.

Der Sicherheits-Navigator

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

Der Navigator auf der Registerkarte Sicherheit enthält folgende Abschnitte:

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

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

- Klicken Sie auf das Menü Aktionen. Jeder Abschnitt des Navigators enthält das Menü Aktionen zur Verwaltung von Gruppen, Benutzern oder Rollen. Wählen Sie im Navigator ein Objekt aus und klicken Sie auf das Menü Aktionen, um Gruppen, Benutzer oder Rollen zu erstellen bzw. zu löschen.
- Rechter Mausklick auf Objekt. Wenn Sie ein Objekt im Navigator mit der rechten Maustaste anklicken, erscheinen die Optionen aus dem Menü Aktionen zum Erstellen, Löschen und Verschieben des Objekts.
- Ziehen Sie ein Objekt von einem Abschnitt in einen anderen. Wenn Sie ein Objekt einem anderen Objekt zuweisen möchten, ziehen Sie es einfach auf den anderen Bereich des Navigators. Zum Beispiel: Um einen Benutzer einer nativen Gruppe zuzuordnen, können Sie den Benutzer im Abschnitt Benutzer des Navigators auswählen und dann zu der nativen Gruppe im Abschnitt Gruppen ziehen.

- Mehrere Benutzer oder Rollen aus dem Inhaltsbereich in den Navigator ziehen. Wählen Sie mehrere Benutzer oder Rollen im Inhaltsbereich aus und ziehen Sie diese in den Navigator, um die ausgewählten Objekte einem anderen Objekt zuzuordnen. Zum Beispiel: Um mehrere Benutzer einer nativen Gruppe zuzuordnen, wählen Sie im Navigatorabschnitt Benutzer den Ordner Native Benutzer aus. Mit den Tasten Strg und Umsch markieren Sie mehrere Benutzer und ziehen diese Benutzerauswahl in die native Gruppe des Abschnitts Gruppen im Navigator.
- Tastenkombinationen verwenden. Mit Hilfe von Tastenkombinationen können Sie die verschiedenen Abschnitte des Navigators ansteuern.

Gruppen

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

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

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

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

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

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

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

Benutzer

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

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

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

- Informatica Administrator
- Informatica Developer

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

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

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

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

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

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

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

Rollen

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

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

- Systemdefinierte Rollen Enthält Rollen, die Sie nicht ändern oder löschen können. Die Administrator-Rolle ist eine vom System definierte Rolle.
- Benutzerdefinierte Rollen Enthält Rollen, die Sie erstellen, bearbeiten und löschen können. Das Administrator Tool enthält einige benutzerdefinierte Rollen, die Sie bearbeiten und an Benutzer und Gruppen zuweisen können.

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

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

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

Passwortverwaltung

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

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

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

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

Ändern Ihres Passwortes.

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

1. Klicken Sie im Überschriftsbereich des Administrator Tools auf **Verwalten** > **Passwort ändern**.

   Die Anwendung "Passwort ändern" öffnet ein neues Browserfenster.
2. Geben Sie das aktuelle Passwort in das Feld **Passwort** ein und das neue Passwort in die Felder **Neues Passwort** und **Passwort bestätigen**.
3. Klicken Sie auf **Aktualisieren**.

Domänensicherheitsmanagement

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

Eine sichere Kommunikation lässt sich wie folgt konfigurieren:

Zwischen den Diensten innerhalb der Domäne

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

Zwischen Domäne und externen Komponenten

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

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

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

Sicherheitsverwaltung für Benutzer

Sie verwalten die Benutzersicherheit innerhalb der Domäne anhand von Berechtigungen.

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

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

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

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

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

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

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

KAPITEL 7

Benutzer und Gruppen

Dieses Kapitel umfasst die folgenden Themen:

Benutzer und Gruppen - ÜbersichtBenutzer und Gruppen

Um auf die Anwendungsdienste und Objekte in der Informatica-Domäne zugreifen und die Anwendungs-Clients nutzen zu können, müssen Sie ein Benutzerkonto haben. Die von Ihnen durchführbaren Aufgaben richten sich nach dem Benutzerkontentyp und dem PowerCenter Express-Lizenztyp.

Um auf die Anwendungsdienste und Objekte in der Informatica-Domäne zugreifen und die Anwendungs-Clients nutzen zu können, müssen Sie ein Benutzerkonto haben.

Während der Installation wird ein Standard-Administrator-Benutzerkonto erstellt. Verwenden Sie das standardmäßige Administratorkonto, um sich an der Informatica-Domäne anzumelden und Anwendungsdienste, Domänenobjekte und andere Benutzerkonten zu verwalten. Wenn Sie sich nach der Installation bei der Informatica-Domäne anmelden, ändern Sie Passwort, um die Sicherheit für die Informatica-Domäne und die Anwendungen zu gewährleisten.

Hinweis: Wenn Sie PowerCenter Express Personal Edition installieren, müssen Sie das standardmäßige Administratorkonto für alle Operationen verwenden. Sie können weder Benutzer oder Gruppen erstellen noch Berechtigungen verwalten.

Die Benutzerkontenverwaltung umfasst in Informatica die folgenden Hauptkomponenten:

- Benutzer. Sie können verschiedene Arten von Benutzerkonten in der Informatica-Domäne einrichten. Die Benutzer können Aufgaben auf der Grundlage der ihnen zugewiesenen Rollen, Berechtigungen und den ihnen zugewiesenen Befugnisse durchführen.
- Authentifizierung. Wenn sich ein Benutzer an einem Anwendungs-Client anmeldet, authentifiziert der Service Manager das Benutzerkonto in der Informatica-Domäne und stellt sicher, dass der Benutzer den Anwendungs-Client verwenden kann. Die Informatica-Domäne kann zur Authentifizierung von Benutzern

eine native oder LDAP-Authentifizierung verwenden. Der Service Manager organisiert Benutzerkonten und Gruppen nach Sicherheitsdomäne. Er authentifiziert Benutzer auf der Basis der Sicherheitsdomäne, der der Benutzer angehört.

- Authentifizierung. Wenn sich ein Benutzer an einem Anwendungs-Client anmeldet, authentifiziert der Service Manager das Benutzerkonto in der Informatica-Domäne und stellt sicher, dass der Benutzer den Anwendungs-Client verwenden kann.
- Authentifizierung. Wenn sich ein Benutzer an einem Anwendungs-Client anmeldet, authentifiziert der Service Manager das Benutzerkonto in der Informatica-Domäne und stellt sicher, dass der Benutzer den Anwendungs-Client verwenden kann.
- Gruppen. Sie können Benutzergruppen einrichten und jeder Gruppe verschiedene Rollen und Berechtigungen zuweisen. Die einer Gruppe zugewiesenen Rollen und Berechtigungen legen die Aufgaben fest, die die Benutzer in der Gruppe innerhalb der Informatica-Domäne durchführen können.
- Berechtigungen und Rollen. Berechtigungen bestimmen die Aktionen, die Benutzer in Anwendungs-Clients ausführen können. Eine Rolle ist eine Zusammenstellung von Berechtigungen, die Sie Benutzern und Gruppen zuordnen können. Sie ordnen Benutzern und Gruppen für die Domäne und für Anwendungsdienste in der Domäne Rollen der Berechtigungen zu.
- Betriebssystemprofile. Wenn Sie den PowerCenter Integration Service unter UNIX ausführen, können Sie den PowerCenter Integration Service so konfigurieren, dass bei der Ausführung von Arbeitsabläufen Betriebssystemprofile verwendet werden. Auf der Registerkarte "Sicherheit" des Administrator-Tools können Sie Betriebssystemprofile erstellen und verwalten.
- Kontosperre. Sie können eine Kontosperre konfigurieren, um ein Benutzerkonto zu sperren, wenn der Benutzer falsche Anmeldedaten im Administrator-Tool oder beliebigen Anwendungs-Clients wie dem Developer-Tool oder Analyst-Tool eingibt. Sie können ein Benutzerkonto auch entsperren.
- Kontosperre. Sie können Kontosperren konfigurieren, um ein Benutzerkonto zu sperren, wenn der Benutzer fehlerhafte Anmeldedaten im Administrator-Tool oder Developer-Tool angibt. Sie können ein Benutzerkonto auch entsperren.
- Kontosperre. Sie können Kontosperren konfigurieren, um ein Benutzerkonto zu sperren, wenn der Benutzer fehlerhafte Anmeldedaten im Administrator-Tool angibt. Sie können ein Benutzerkonto auch entsperren.

Standardgruppen

Die Informatica-Domäne enthält einen Satz von Benutzergruppen, die während der Installation erstellt werden.

Standardmäßig enthält die Informatica-Domäne die folgenden Benutzergruppen nach der Installation:

- Jeder
- Administrator

Administratorgruppe

Die Informatica-Domäne enthält die Standardgruppe „Administrator“. Das während der Installation erstellte Standard-Administratorkonto gehört zu dieser Gruppe.

Die Administratorgruppe verfügt über Administrator-Berechtigungen für die Domäne und alle Anwendungsdienste. Sie können Benutzer zur Administratorgruppe hinzufügen oder daraus entfernen. Alle Benutzer in der Administratorgruppe verfügen über dieselben Berechtigungen, die der Standardadministrator während der Installation erstellt hat.

Sie können weder das standardmäßige Administratorkonto aus der Administratorgruppe noch die Administratorgruppe löschen.

Gruppe „Jeder“

Die Informatica-Domäne enthält die Standardgruppe „Jeder“. Alle Benutzer in der Domäne gehören zu dieser Gruppe.

Standardmäßig verfügt die Gruppe „Jeder“ über keine Berechtigungen. Sie können der Gruppe „Jeder“ Berechtigungen und Rollen zuweisen, um allen Benutzern denselben Zugang zu ermöglichen.

Sie können die folgenden Aufgaben nicht in der Gruppe „Jeder“ ausführen:

- Bearbeiten oder Löschen der Gruppe "Jeder".
- Benutzer in die Gruppe "Jeder" hinzufügen oder daraus entfernen.
- Eine Gruppe in die Gruppe "Jeder" verschieben.

Das Konzept der Benutzerkonten

Eine Informatica-Domäne kann folgende Arten von Benutzerkonten haben:

- Standardadministrator
- Domänenadministrator
- Anwendungs-Client-Administrator
- Benutzer

Eine Informatica-Domäne kann folgende Arten von Benutzerkonten haben:

- Standardadministrator
- Domänenadministrator
- Anwendungs-Client-Administrator
- Benutzer

Die Informatica-Domäne hat ein Standardadministratorkonto.

Standardadministrator

Beim Installieren von Informatica Services erstellt das Installationsprogramm den Standardadministrator mit einem von Ihnen vergebenen Benutzernamen und Passwort. Für die Erstanmeldung beim Administrator-Tool können Sie das Standardadministratorkonto verwenden.

Der Standardadministrator verfügt über Administratorberechtigungen für die Domäne und alle Anwendungsdienste.

Der Standardadministrator kann folgende Aufgaben übernehmen:

- Erstellen, Konfigurieren und Verwalten aller Objekte in der Domäne, einschließlich Knoten, Anwendungsdiensten sowie Administrator- und Benutzerkonten.
- Konfigurieren und Verwalten aller Objekte und Benutzerkonten, die von anderen Domänenadministratoren und Anwendungs-Client-Administratoren erstellt wurden.
- Anmelden bei einem beliebigen Anwendungs-Client.

Der Standardadministrator ist ein Benutzerkonto in der nativen Sicherheitsdomäne. Sie können keinen Standardadministrator erstellen. Auch den Benutzernamen oder die Berechtigungen des Standardadministrators können Sie nicht deaktivieren oder ändern. . Das Passwort des Standardadministrators können Sie jedoch ändern.

Domänenadministrator

Ein Domänenadministrator kann Objekte in der Domäne erstellen und verwalten.

Der Domänenadministrator kann sich im Administrator-Tool anmelden und Anwendungsdienste in der Domäne erstellen und konfigurieren. Dennoch kann sich der Domänenadministrator standardmäßig nicht an den Anwendungs-Clients anmelden. Der Standardadministrator muss einem Domänenadministrator explizit sämtliche Berechtigungen für die Anwendungsdienste übergeben, damit sich dieser anmelden und Verwaltungsaufgaben in den Anwendungs-Clients durchführen kann.

Der Domänenadministrator kann sich am Administrator-Tool anmelden und Anwendungsdienste in der Domäne konfigurieren. Dennoch kann sich der Domänenadministrator standardmäßig nicht an den Anwendungs-Clients anmelden. Der Standardadministrator muss einem Domänenadministrator explizit sämtliche Berechtigungen für die Anwendungsdienste übergeben, damit sich dieser anmelden und Verwaltungsaufgaben in den Anwendungs-Clients durchführen kann.

Um einen Domänenadministrator zu erstellen, weisen Sie einem Benutzer die Administratorrolle für die Domäne zu.

Anwendungs-Client-Administrator

Ein Anwendungs-Client-Administrator kann Objekte in einem Anwendungs-Client erstellen und verwalten. Für die Anwendungs-Clients müssen Sie Administratorkonten erstellen. Um die Administratorberechtigungen zu begrenzen und die Sicherheit der Anwendungs-Clients zu gewährleisten, sollten Sie für jeden Anwendungs-Client ein separates Administratorkonto einrichten.

Standardmäßig verfügt der Anwendungs-Client nicht über Rechte oder Berechtigungen für die Domäne. Ohne Berechtigungen oder Rechte für die Domäne kann sich der Anwendungs-Client-Administrator nicht beim Administrator-Tool anmelden, um den Anwendungsdienst zu verwalten.

Sie können die folgenden Anwendungs-Client-Administratoren einrichten:

Data Analyzer-Administrator

Verfügt über umfassende Berechtigungen und Rechte in Data Analyzer. Der Data Analyzer-Administrator kann sich bei Data Analyzer anmelden, um Data Analyzer-Objekte zu erstellen und zu verwalten und alle Aufgaben im Anwendungs-Client auszuführen.

Um einen Data Analyzer-Administrator zu erstellen, müssen Sie einem Benutzer die Administratorrolle für einen Berichterstellungsdienst zuweisen.

Informatica Analyst-Administrator

Verfügt über umfassende Berechtigungen und Rechte in Informatica Analyst. Der Informatica Analyst-Administrator kann sich bei Informatica Analyst anmelden, um Projekte und Objekte in Projekten zu erstellen und zu verwalten und alle Aufgaben im Anwendungs-Client auszuführen.

Um einen Informatica Analyst-Administrator zu erstellen, weisen Sie einem Benutzer die Administratorrolle für einen Analyst-Dienst und für den zugeordneten Modellrepository-Dienst zu.

Informatica Developer-Administrator

Verfügt über umfassende Berechtigungen und Rechte in Informatica Developer. Der Informatica Developer-Administrator kann sich bei Informatica Developer anmelden, um Projekte und Objekte in Projekten zu erstellen und zu verwalten und alle Aufgaben im Anwendungs-Client auszuführen.

Um einen Informatica Developer-Administrator zu erstellen, weisen Sie einem Benutzer die Administratorrolle für einen Modellrepository-Dienst zu.

Metadata Manager-Administrator

Verfügt über umfassende Berechtigungen und Rechte in Metadata Manager. Der Metadata Manager-Administrator kann sich bei Metadata Manager anmelden, um Metadata Manager-Objekte zu erstellen und zu verwalten und alle Aufgaben im Anwendungs-Client auszuführen.

Um einen Metadata Manager-Administrator zu erstellen, weisen Sie einem Benutzer die Administratorrolle für einen Metadata Manager-Dienst zu.

Jaspersoft-Administrator

Administratorberechtigungen sind bei Jaspersoft in der Rolle ROLE_ADMINISTRATOR abgebildet.

Test Data Manager-Administrator

Verfügt über umfassende Berechtigungen und Rechte in Test Data Manager. Der Test Data Manager-Administrator kann sich bei Test Data Manager anmelden, um Test Data Manager-Objekte zu erstellen sowie zu verwalten und alle Aufgaben im Anwendungs-Client auszuführen.

Um einen Test Data Manager-Administrator zu erstellen, weisen Sie einem Benutzer die Administratorrolle für einen Test Data Manager-Dienst zu.

PowerCenter Client-Administrator

Verfügt über umfassende Berechtigungen und Rechte für alle Objekte im PowerCenter Client. Der PowerCenter Client-Administrator kann sich beim PowerCenter Client anmelden, um die PowerCenter-Repository-Objekte zu verwalten und alle Aufgaben im PowerCenter-Client auszuführen. Außerdem kann der PowerCenter Client-Administrator alle Aufgaben in den Befehlszeilenprogrammen pmrep und pmcmd ausführen.

Um einen PowerCenter Client-Administrator zu erstellen, weisen Sie einem Benutzer die Administratorrolle für einen PowerCenter-Repository-Dienst zu.

Benutzer

Ein Benutzer mit einem Konto in der Informatica-Domäne kann Tasks in Anwendungs-Clients ausführen.

Üblicherweise erstellt der Standard- oder Domänenadministrator die Benutzerkonten und verwaltet diese bzw. weist ihnen Rollen und Berechtigungen in der Informatica-Domäne zu. Jedoch kann jeder Benutzer mit der erforderlichen Domänenberechtigung ein Benutzerkonto erstellen und diesem Rollen und Berechtigungen zuweisen.

Benutzer können Ausgaben in Anwendungs-Clients ausführen, die ihren Berechtigungen entsprechen.

Benutzer verwalten

Sie können Benutzer in der nativen Sicherheitsdomäne erstellen, bearbeiten und löschen. Die Eigenschaften von Benutzerkonten in der LDAP-Sicherheitsdomäne können Sie jedoch nicht löschen oder bearbeiten. Sie können auch die Benutzerzuweisungen für LDAP-Gruppen nicht ändern.

Sie können Benutzer je nach Typ der PowerCenter Express-Lizenz erstellen, bearbeiten und löschen. Sie können einem Benutzerkonto Rollen und Berechtigungen zuweisen. Die einem Benutzer zugewiesenen Rollen und Berechtigungen legen die Aufgaben fest, die der Benutzer innerhalb der Informatica-Domäne durchführen kann. Wenn Sie die PowerCenter Express Personal Edition verwenden, können Sie keine Benutzer oder Gruppen erstellen. Sie müssen den standardmäßigen Administratorbenutzer verwenden, um alle Aufgaben durchzuführen.

Sie können Benutzer je nach Lizenztyp erstellen, bearbeiten und löschen. Sie können einem Benutzerkonto Rollen und Berechtigungen zuweisen. Die einem Benutzer zugewiesenen Rollen und Berechtigungen legen die Aufgaben fest, die der Benutzer innerhalb der Informatica-Domäne durchführen kann.

Sie können Rollen und Berechtigungen zu einem Benutzerkonto in der nativen oder in einer LDAP-Sicherheitsdomäne zuweisen. Die einem Benutzer zugewiesenen Rollen und Berechtigungen legen die Aufgaben fest, die der Benutzer innerhalb der Informatica-Domäne durchführen kann.

Sie können ein Benutzerkonto auch entsperren.

Erstellen nativer Benutzer Erstellen von BenutzernErstellen von Benutzern

Auf der Registerkarte Sicherheit können Sie native Benutzer hinzufügen, bearbeiten oder löschen.

1. Klicken Sie im Administrator-Tool auf die Registerkarte "Sicherheit".
2. Klicken Sie im Menü "Sicherheitsaktionen" auf "Benutzer erstellen".
3. Geben Sie folgende Details für den Benutzer ein:

Eigenschaft	Beschreibung
Anmeldename	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, und 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. **Hinweis:** Der Data Analyzer verwendet den Benutzerkontonamen und die Sicherheitsdomäne im Format *UserName@SecurityDomain* zur Festlegung der Länge des Benutzer-Anmeldenamens. Die Kombination aus Benutzernamen, @-Symbol und Sicherheitsdomäne darf nicht mehr als 128 Zeichen lang sein.
Passwort	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	Vollständiger Name für das Benutzerkonto. Der vollständige Name darf folgende Sonderzeichen nicht enthalten: < > “ **Hinweis:** Im Data Analyzer ist die Eigenschaft des vollständigen Namens das Äquivalent dreier separater Eigenschaften namens Erster Vorname, Zweiter Vorname und Nachname.

Eigenschaft	Beschreibung
Beschreibung	Beschreibung des Benutzerkontos. Die Beschreibung darf nicht länger als 765 Zeichen sein und keines der folgenden Sonderzeichen enthalten: < > “
E-Mail	E-Mail-Adresse des Benutzers. Die E-Mail-Adresse darf keines der folgenden Sonderzeichen enthalten: < > “ Geben Sie die E-Mail-Adresse im Format UserName@Domäne ein.
Telefon	Telefonnummer des Benutzers. Die Telefonnummer darf keines der folgenden Sonderzeichen enthalten: < > “

4. Klicken Sie auf "OK", um das Benutzerkonto zu speichern.

   Nachdem Sie ein Benutzerkonto erstellt haben, werden in der Detailübersicht die Eigenschaften des Benutzerkontos und die Gruppen, denen der Benutzer zugeordnet ist, angezeigt.

Allgemeine Eigenschaften der nativen Benutzer bearbeiten

Sie können den Anmeldename eines nativen Benutzers nicht ändern. Sie können das Passwort und andere Details eines nativen Benutzerkontos ändern.

1. Klicken Sie im Administrator Tool auf die Registerkarte Sicherheit.
2. Im Abschnitt Benutzer des Navigators wählen Sie ein natives Benutzerkonto aus und klicken auf Bearbeiten.
3. Um ein anderes Passwort festzulegen, wählen Sie Passwort ändern.

   Auf der Registerkarte Sicherheit werden die Einträge in den Feldern Passwort und Passwort bestätigen gelöscht.
4. Geben Sie ein neues Passwort ein und bestätigen Sie dieses.
5. Ändern Sie den kompletten Namen, die Beschreibung, E-Mail und Telefon wie erforderlich.
6. Klicken Sie auf OK, um die Änderungen zu speichern.

Zuweisen von nativen Benutzern zu nativen Gruppen

Weisen Sie native Benutzer einer nativen Gruppe in der Registerkarte Sicherheit zu.

1. Klicken Sie im Administrator Tool auf die Registerkarte Sicherheit.
2. Wählen Sie im Abschnitt „Benutzer“ des Navigators ein natives Benutzerkonto aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf die Registerkarte Gruppen.
4. Um einen nativen Benutzer einer Gruppe zuzuweisen, wählen Sie einen Gruppennamen in der Spalte „Alle Gruppen“ aus und klicken auf **Hinzufügen**.

   Wenn in der Spalte Alle Gruppen keine verschachtelten Gruppen angezeigt werden, erweitern Sie jede Gruppe. Dann werden alle verschachtelten Gruppen angezeigt.

   Sie können einen nativen Benutzer mehreren Gruppen zuweisen. Mit der Strg- oder der Umschalttaste können Sie mehrere Gruppen auf einmal auswählen.

5. Um einen nativen Benutzer aus einer Gruppe zu entfernen, wählen Sie eine Gruppe in der Spalte „Zugewiesene Gruppen“ aus und klicken auf **Entfernen**.
6. Klicken Sie auf **OK**, um die Gruppenzuordnungen zu speichern.

Zuweisen von LDAP-Benutzern zu nativen Gruppen

Sie können LDAP-Benutzerkonten nativen Gruppen zuweisen. Die Zuweisung von LDAP-Benutzerkonten zu LDAP-Gruppen kann nicht geändert werden.

1. Klicken Sie im Administrator Tool auf die Registerkarte Sicherheit.
2. Wählen Sie im Gruppenabschnitt des Navigators eine native Gruppe aus und klicken Sie auf "Bearbeiten".
3. Klicken Sie auf die Registerkarte "Benutzer".
4. Um einen LDAP-Benutzer einer Gruppe zuzuweisen, wählen Sie einen LDAP-Benutzer in der Spalte "Alle Benutzer" aus und klicken Sie auf "Hinzufügen".
5. Um einen LDAP-Benutzer aus einer Gruppe zu entfernen, wählen Sie einen LDAP-Benutzer in der Spalte "Zugewiesene Benutzer" aus und klicken Sie auf "Entfernen".
6. Klicken Sie auf "OK", um die Benutzerzuweisungen zu speichern.

Aktivieren und Deaktivieren von Benutzerkonten

Benutzer mit aktiven Konten können sich bei Anwendungs-Clients anmelden und Aufgaben basierend auf ihren Berechtigungen ausführen. Wenn Sie Benutzer vorübergehend vom Zugriff auf Anwendungs-Clients ausschließen möchten, können Sie deren Konten deaktivieren. Sie können Benutzerkonten in der nativen oder einer LDAP-Sicherheitsdomäne aktivieren und deaktivieren. Bei deaktiviertem Benutzerkonto kann sich der Benutzer nicht bei den Anwendungs-Clients anmelden.

Benutzer mit aktiven Konten können sich bei Anwendungs-Clients anmelden und Aufgaben basierend auf ihren Berechtigungen ausführen. Wenn Sie Benutzer vorübergehend vom Zugriff auf Anwendungs-Clients ausschließen möchten, können Sie deren Konten deaktivieren. Bei deaktiviertem Benutzerkonto kann sich der Benutzer nicht bei den Anwendungs-Clients anmelden.

Um ein Benutzerkonto zu deaktivieren, wählen Sie ein Benutzerkonto im Abschnitt Benutzer des Navigators und klicken Sie auf Deaktivieren. Wählen Sie ein deaktiviertes Benutzerkonto aus, wird auf der Registerkarte Sicherheit eine Meldung eingeblendet, die anzeigt, dass das Benutzerkonto deaktiviert ist. Ist ein Benutzerkonto deaktiviert, ist die Schaltfläche Aktivieren verfügbar. Klicken Sie auf Aktivieren, um das Benutzerkonto zu aktivieren.

Das Standard-Administratorkonto können Sie nicht deaktivieren.

Hinweis: Wenn der Service Manager ein Benutzerkonto aus dem LDAP-Verzeichnisdienst importiert, wird das LDAP-Attribut, das besagt, dass ein Benutzerkonto aktiviert oder deaktiviert ist, nicht mit importiert. Der Service Manager importiert alle Benutzerkonten als aktivierte Benutzerkonten. Falls Sie nicht möchten, dass der Benutzer auf Anwendungs-Clients zugreift, müssen Sie das LDAP-Benutzerkonto im Administrator-Tool deaktivieren. Bei der späteren Synchronisierung mit dem LDAP-Server behält das Benutzerkonto den aktivierten oder deaktivierten Statussatz im Administrator-Tool bei.

Native Benutzer löschen

Um ein natives Benutzerkonto zu löschen, klicken Sie das Benutzerkonto im Abschnitt Benutzer des Navigators an und wählen Sie Benutzer löschen. Bestätigen Sie, dass Sie das Benutzerkonto löschen möchten.

Das Standardadministratorkonto können Sie nicht löschen. Wenn Sie sich am Administrator Tool anmelden, können Sie Ihr Benutzerkonto nicht löschen.

Benutzer des PowerCenters löschen

Wenn Sie einen Benutzer löschen, der Objekte im PowerCenter Repository besitzt, entfernen Sie die Eigentumsrechte, die der Benutzer in Bezug auf Ordner, Verbindungsobjekte, Bereitstellungsgruppen, Beschriftungen oder Abfragen hat. Nach dem Löschen des Benutzers, wird der Standardadministrator zum Eigentümer aller Objekte, die dem entfernten Benutzer gehört haben.

Wenn Sie die Historie eines versionierten Objekts anzeigen, das zuvor von einem gelöschten Benutzer besessen wurde, erscheint der Name des gelöschten Benutzers vor dem Wort "gelöscht".

Benutzer aus Data Analyzer löschen

Wenn Sie einen Benutzer löschen, löscht der Data Analyzer die dem Benutzer zugeordneten Meldungen, Meldungs-E-Mail-Konten und persönlichen Ordner sowie Dashboards.

Der Data Analyzer löscht alle Berichte, die der Benutzer basierend auf dem Sicherheitsprofil des Berichts abonniert hat. Der Data Analyzer unterhält ein Sicherheitsprofil für jeden Benutzer, der den Bericht abonniert. Ein Bericht, der mit benutzerbasierter Sicherheit arbeitet, nutzt das Sicherheitsprofil des Benutzers, der auf den Bericht zugreift. Ein Bericht, der mit providerbasierter Sicherheit arbeitet, nutzt das Sicherheitsprofil des Benutzers, dem der Bericht gehört.

Wenn Sie einen Benutzer löschen, löscht der Data Analyzer keinen Bericht im öffentlichen Ordner des Benutzers. Der Data Analyzer kann auch dann einen Bericht mit benutzerbasierter Sicherheit ausführen, wenn der Berichtseigentümer nicht existiert. Der Data Analyzer kann jedoch das Sicherheitsprofil für einen Bericht mit providerbasierter Sicherheit nicht bestimmen, wenn der Berichtseigentümer nicht existiert. Bevor Sie einen Benutzer löschen, überprüfen Sie, ob die Berichte mit providerbasierter Sicherheit einen neuen Eigentümer haben.

Beispiel: Sie möchten den Benutzer A löschen, der einen Bericht im öffentlichen Ordner mit providerbasierter Sicherheit hat. Erstellen Sie einen Benutzer mit demselben Sicherheitsprofil wie der Benutzer A. Bestimmen Sie alle Berichte mit providerbasierter Sicherheit im öffentlichen Ordner des Benutzers A. Veranlassen Sie dann die Anmeldung des anderen Benutzers mit demselben Sicherheitsprofil und speichern Sie diese Berichte im öffentlichen Ordner mit providerbasierter Sicherheit und demselben Berichtsnamen. Damit ist gewährleistet, dass die Berichte nach dem Löschen des Benutzers im öffentlichen Ordner mit derselben Sicherheit bleiben.

Benutzer aus Metadata Manager löschen

Wenn Sie einen Benutzer löschen, der eigene Tastenkombinationen und Ordner besitzt, verschiebt der Metadata Manager den persönlichen Ordner des Benutzers in einen Ordner namens "Gelöschte Benutzer", die zum Standardadministrator gehören. Der persönliche Ordner eines gelöschten Benutzers enthält alle Tastenkombinationen und Ordner, die vom betreffenden Benutzer erstellt wurden. Alle gemeinsamen Ordner bleiben gemeinsam, nachdem ein Benutzer gelöscht wurde.

Wenn der Ordner "Gelöschter Benutzer" bereits einen Ordner mit demselben Benutzernamen enthält, nennt der Metadata Manager den zusätzlichen Ordner "Kopien (n) von <Benutzername>."

LDAP-Benutzer

LDAP-Benutzer lassen sich im Administrator Tool nicht hinzufügen, bearbeiten oder löschen. Sie müssen die LDAP-Benutzerkonten im LDAP-Verzeichnisdienst verwalten.

Entsperren eines Benutzerkontos

Der Domänenadministrator kann ein Benutzerkonto entsperren, das für eine Domäne gesperrt ist. Wenn der Benutzer ein nativer Benutzer ist, kann der Administrator den Benutzer auffordern, sein Passwort zurückzusetzen, bevor dieser sich erneut an der Domäne anmeldet.

Der Benutzer muss über eine in der Domäne konfigurierte gültige E-Mail-Adresse verfügen, um eine Benachrichtigung zu erhalten, wenn sein Benutzerpasswort zurückgesetzt wird.

Wenn der Benutzer für den LDAP-Authentifizierungsserver gesperrt wird, muss der LDAP-Administrator das Benutzerkonto im LDAP-Server entsperren.

1. Klicken Sie im Administrator-Tool auf die Registerkarte **Sicherheit**.
2. Klicken Sie auf **Kontoverwaltung**.

   Die Seite „Kontoverwaltung“ zeigt die folgenden Listen gesperrter Benutzer an:

   Gesperrte native Benutzer

   Enthält Benutzerkonten in der nativen Sicherheitsdomäne, die gesperrt sind.

   Gesperrte LDAP-Benutzer

   Enthält Benutzerkonten in LDAP-Sicherheitsdomänen, die gesperrt sind.
3. Wählen Sie die Benutzer aus, die entsperrt werden sollen.
4. Wählen Sie **Benutzername entsperren und Passwort zurücksetzen** aus, um ein neues Passwort für den Benutzer zu generieren, nachdem Sie das Konto entsperrt haben.

   Der Benutzer erhält das neue Passwort per E-Mail.
5. Klicken Sie auf die Schaltfläche **Ausgewählte Benutzer entsperren**.

Vergrößern des Systemspeichers für eine Vielzahl von Benutzern

Die Bearbeitungszeit für einen Neustart der Informatica-Domäne, die LDAP-Benutzersynchronisierung und einige infacmd und infasetup Befehle steigt proportional zur Anzahl der Benutzer in der Informatica-Domäne.

Die Anzahl der Benutzer wirkt sich auf die Bearbeitungszeit folgender Befehle aus:

- infasetup BackupDomain, DeleteDomain und RestoreDomain
- infacmd isp ExportDomainObjects, ExportObjects, ImportDomainObjects und ImportObjects
- infacmd oie ExportObjects und ImportObjects

Möglicherweise müssen Sie bei einer Vielzahl von Benutzern in der Domäne den von Informatica Services, infasetup und infacmd verwendeten Systemspeicher vergrößern. Konfigurieren Sie zum Vergrößern der maximalen Heap-Größe folgende Umgebungsvariablen und geben Sie den Wert in Megabyte an:

- INFA_JAVA_OPTS Bestimmt die maximale Heap-Größe, die von Informatica-Diensten verwendet wird. Auf jedem Knoten zu konfigurieren, auf dem Informatica Services installiert wird.
- ICMD_JAVA_OPTS. Bestimmt die maximale Heap-Größe, die von infacmd verwendet wird. Ist auf jedem Computer zu konfigurieren, auf dem Sie infacmd ausführen.
- INFA_JAVA_CMD_OPTS. Bestimmt die maximale Heap-Größe, die von infasetup verwendet wird. Auf jedem Computer zu konfigurieren, auf dem Sie infasetup konfigurieren.

Beispiel: Um 2048 MB Systemspeicher unter UNIX für die Umgebungsvariable INFA_JAVA_OPTS zu konfigurieren, müssen Sie folgenden Befehl verwenden:

```
setenv INFA_JAVA_OPTS "-Xmx2048m"
```

Unter Windows konfigurieren Sie die Variablen als Systemvariablen.

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.

Damit die Änderungen wirksam werden, starten Sie den Knoten bitte nach dem Konfigurieren dieser Umgebungsvariablen neu.

Anzeigen von Benutzeraktivität

Verwenden Sie den infacmd isp getUserActivityLog-Befehl oder die Registerkarte „Protokolle“ des Administrator-Tools, um Benutzeraktivitätsprotokolle anzuzeigen. Verwenden Sie die Protokollereignisse der Benutzeraktivität, um festzustellen, wann ein Benutzer Dienste, Knoten, Benutzergruppen oder Rollen erstellt, aktualisiert oder gelöscht hat.

Führen Sie den folgenden Befehl aus, um die Protokollereignisse der Benutzeraktivität für alle Benutzer anzuzeigen:

```
infacmd isp getUserActivityLog -dn domain_name -un user_name -pd password
```

Der Befehl fordert die Administratorrolle oder die Mitgliedschaft in der Administratorgruppe.

Sie können Protokollereignisse basierend auf den folgenden optionalen Filtern anzeigen:

- Benutzername
- Sicherheitsdomäne
- Datum und Uhrzeit
- Chronologische Reihenfolge
- Aktivitätscode
- Aktivitätstext

Sie können die Protokollereignisse in der Befehlszeile anzeigen oder in den folgenden Formaten in eine Datei schreiben:

- Binär
- Text
- XML

Wenn Sie ein Protokoll im binären Format drucken, können Sie den infacmd isp convertUserActivityLog-Befehl verwenden, um eine Konvertierung ins Text- oder HTML-Format durchzuführen.

Weitere Informationen zu Benutzeraktivitätsprotokollen und zur Registerkarte „Protokolle“ des Administrator-Tools finden Sie im *Informatica Administrator-Handbuch*.

Filter für Benutzeraktivitätsprotokolle

Verwenden Sie einen oder mehrere Filter, um Protokollereignisse für bestimmte Benutzer, Datumsangaben oder Ereignisse abzurufen.

Verwenden Sie einen oder mehrere der folgenden Parameter für den infacmd isp getUserActivityLog-Befehl, um Protokollereignisse zu filtern:

Benutzer und Sicherheitsdomänen

Optional. Die Liste der Benutzer, für die Sie Protokollereignisse erhalten möchten. Trennen Sie mehrere Benutzer mit einem Leerzeichen. Verwenden Sie das Platzhaltersymbol (*), um Protokolle für mehrere Benutzer in einer einzelnen Sicherheitsdomäne oder in allen Sicherheitsdomänen anzuzeigen. Beispiel: Die folgenden Zeichenfolgen sind gültige Werte für diese Option:

```
user:Native
"user:*"
"user*"
"*_users_*"
"*:Native"
```

Fügen Sie dem getUserActivityLog-Befehl den folgenden Parameter hinzu, um Protokollereignisse basierend auf dem Benutzer oder der Sicherheitsdomäne zu filtern:

```
-usrs <UserName>:<SecurityDomain>
```

Beispiel: Fügen Sie den folgenden Parameter hinzu, um Benutzeraktivität für einen Benutzer namens User1 auf allen Sicherheitsdomänen abzurufen:

```
-usrs "User1:*"
```

Datum und Uhrzeit

Optional. Der Datumsbereich, für den Sie Protokollereignisse anzeigen möchten.

Wenn Sie ein Enddatum eingeben, das vor dem Startdatum liegt, gibt der Befehl keine Protokollereignisse zurück.

Geben Sie das Datum und die Uhrzeit in einem der folgenden Formate ein:

- MM/tt/jjjj
- MM/tt/jjjj HH:mm:ss
- jjjj-MM-tt
- jjjj-MM-tt HH:mm:ss

Fügen Sie dem getUserActivityLog-Befehl den folgenden Parameter hinzu, um das Protokoll nach Start- und Enddatum zu filtern:

```
-sd <start_date> -ed <end_date>
```

Beispiel: Fügen Sie den folgenden Parameter hinzu, um Benutzeraktivität zwischen dem 1. Januar 2014 und dem 3. Februar 2014 abzurufen:

```
-sd 01/01/2014 -ed 02/03/2014
```

Aktivitätscode

Optional. Gibt Protokollereignisse auf Basis des Aktivitätscodes zurück.

Verwenden Sie das Platzhaltersymbol (*), um Protokollereignisse für mehrere Aktivitätscodes abzurufen. Gültige Aktivitätscodes:

- CCM_10437. Gibt an, dass eine Aktivität erfolgreich war.
- CCM_10438. Gibt an, dass eine Aktivität fehlgeschlagen ist.

Fügen Sie dem getUserActivityLog-Befehl den folgenden Parameter hinzu, um nach Aktivitätscode zu filtern:

```
-ac <activity_code>
```

Beispiel: Fügen Sie den folgenden Parameter hinzu, um erfolgreiche Protokollereignisse abzurufen:

```
-ac CCM_10437
```

Wenn Sie das Platzhaltersymbol verwenden, setzen Sie das Argument in Anführungszeichen.

Aktivitätstext

Optional. Gibt die Protokollereignisse auf Basis einer im Aktivitätstext gefundenen Zeichenfolge zurück.

Fügen Sie dem getUserActivityLog-Befehl den folgenden Parameter hinzu, um nach Aktivitätstext zu filtern:

```
-atxt <activity_text>
```

Verwenden Sie das Platzhaltersymbol (*), um Protokolle für mehrere Ereignisse abzurufen. Beispiel: Der folgende Parameter gibt alle Protokollereignisse zurück, die „Dienst wird aktiviert“ in ihrer Beschreibung enthalten:

```
-atxt "*Enabling service*"
```

Wenn Sie das Platzhaltersymbol verwenden, setzen Sie das Argument in Anführungszeichen.

Chronologische Reihenfolge

Optional. Druckt Protokollereignisse in umgekehrter chronologischer Reihenfolge. Wenn Sie diesen Parameter nicht angeben, zeigt der Befehl Protokollereignisse in chronologischer Reihenfolge an.

Fügen Sie dem getUserActivityLog-Befehl den folgenden Parameter hinzu, um das aktuelle Ergebnis zuerst zu drucken:

```
-ro true
```

Schreiben und Anzeigen von Protokollereignissen der Benutzeraktivität

Sie können Protokollereignisse der Benutzeraktivität in eine Datei schreiben oder in der Befehlszeile anzeigen, wenn Sie den infacmd isp getUserActivityLog-Befehl verwenden. Schreiben Sie Protokollereignisse der Benutzeraktivität in den Formaten, in denen Sie die exportierte Protokollereignisdatei verwenden möchten.

Schreiben und Anzeigen von Protokolldateien

Um die Protokollereignisse der Benutzeraktivität in einer Datei zu schreiben, führen Sie den Befehl mit dem Ausgabedateiparameter-lo aus:

```
-lo output_file_name
```

Wenn Sie kein Ausgabeformat angeben, schreibt der Befehl die Protokollereignisse in eine Textdatei. Beispiel: Führen Sie den folgenden Befehl aus, um Protokollereignisse in eine Datei namens `log.txt` zu schreiben:

```
infacmd isp getUserActivityLog -dn TestDomain -un Administrator -pd Administrator -lo
log.txt
```

Um ein Ausgabeformat anzugeben, führen Sie den Befehl mit dem Formatparameter -fm aus:

```
-fm output_format_BIN_TEXT_XML
```

Gültige Formate umfassen:

- Bin (binär). Verwenden Sie das Binärformat, um die Protokollereignisse im binären Format zu sichern. Möglicherweise müssen Sie dieses Format verwenden, um Protokollereignisse an den globalen Kundensupport von Informatica zu senden.
- Text. Verwenden Sie das Textformat, wenn Sie die Protokollereignisse in einem Texteditor analysieren möchten.
- XML. Verwenden Sie das XML-Format, wenn Sie die Protokollereignisse in einem externen Tool analysieren möchten, das XML verwendet, oder wenn Sie XML-Tools wie zum Beispiel XSLT benutzen möchten.

Wenn Sie Text oder XML als Ausgabeformat angeben, aber keine Ausgabedatei festlegen, zeigt der Befehl das Text- oder XML-Protokoll in der Befehlszeile an.

Wenn Sie „Binär“ als Ausgabeformat festlegen, müssen Sie einen Ausgabedateinamen angeben.

Beispiel: Führen Sie den folgenden Befehl aus, um Protokollereignisse in eine Datei namens `log.xml` zu schreiben:

```
infacmd isp getUserActivityLog -dn TestDomain -un Administrator -pd Administrator -fm
xml -lo log.xml
```

Konvertieren von Protokolldateien

Wenn Sie den getUserActivity-Befehl zum Schreiben von Protokollereignissen in eine Binärdatei verwenden, können Sie die Datei ins Text- oder XML-Format konvertieren.

Führen Sie den folgenden Befehl aus, um ein von Ihnen abgerufenes binäres Protokoll ins Text- oder HTML-Format zu konvertieren:

```
infacmd isp convertUserActivityLogFile -in BIN_input_file_name -fm
output_format_TEXT_XML -lo output_file_name
```

Beispiel: Führen Sie den folgenden Befehl aus, um eine binäre Eingabedatei namens `log.bin` ins XML-Format zu konvertieren und in einer Datei namens `convertedLog.xml` auszugeben:

```
infacmd isp convertUserActivityLogFile -in log.bin -fm XML -lo convertedLog.xml
```

Um das Protokoll in der Befehlszeile anzuzeigen, lassen Sie den Ausgabedateinamen weg.

Wenn Sie das Format weglassen, verwendet der Befehl das Textformat.

Gruppen verwalten

Sie können Gruppen in der nativen Sicherheitsdomäne erstellen, bearbeiten und löschen.

Sie können Rollen und Berechtigungen zu einer Gruppe in der nativen oder in einer LDAP-Sicherheitsdomäne zuweisen. Die Eigenschaften von Gruppenkonten in der LDAP-Sicherheitsdomäne können jedoch nicht gelöscht oder bearbeitet werden. Die einer Gruppe zugewiesenen Rollen und Berechtigungen legen die Aufgaben fest, die die Benutzer in der Gruppe innerhalb der Informatica-Domäne durchführen können.

Sie können einer Gruppe Rollen und Berechtigungen zuweisen. Die einer Gruppe zugewiesenen Rollen und Berechtigungen legen die Aufgaben fest, die die Benutzer in der Gruppe innerhalb der Informatica-Domäne durchführen können.

Sie können einer Gruppe Rollen und Berechtigungen zuweisen. Die einer Gruppe zugewiesenen Rollen und Berechtigungen legen die Aufgaben fest, die die Benutzer in der Gruppe innerhalb der Informatica-Domäne durchführen können.

Hinzufügen einer nativen Gruppe

Auf der Registerkarte "Sicherheit" können Sie native Gruppen hinzufügen, bearbeiten oder entfernen.

Eine native Gruppe kann native LDAP-Benutzerkonten oder andere native Gruppen enthalten. Sie können mehrere Ebenen nativer Gruppen erstellen. Zum Beispiel enthält die Gruppe "Finance" die Gruppe "AccountsPayable", die wiederum die Gruppe "OfficeSupplies" enthält. Die Gruppe "Finance" ist der Gruppe "AccountsPayable" übergeordnet und die Gruppe "AccountsPayable" fungiert als übergeordnete Gruppe der Gruppe "OfficeSupplies". Jede Gruppe kann weitere native Gruppen enthalten.

Eine native Gruppe kann Benutzerkonten oder andere native Gruppen enthalten. Sie können mehrere Ebenen nativer Gruppen erstellen. Zum Beispiel enthält die Gruppe "Finance" die Gruppe "AccountsPayable", die wiederum die Gruppe "OfficeSupplies" enthält. Die Gruppe "Finance" ist der Gruppe "AccountsPayable" übergeordnet und die Gruppe "AccountsPayable" fungiert als übergeordnete Gruppe der Gruppe "OfficeSupplies". Jede Gruppe kann weitere native Gruppen enthalten.

Eine native Gruppe kann Benutzerkonten oder andere native Gruppen enthalten. Sie können mehrere Ebenen nativer Gruppen erstellen. Zum Beispiel enthält die Gruppe "Finance" die Gruppe "AccountsPayable", die wiederum die Gruppe "OfficeSupplies" enthält. Die Gruppe "Finance" ist der Gruppe "AccountsPayable" übergeordnet und die Gruppe "AccountsPayable" fungiert als übergeordnete Gruppe der Gruppe "OfficeSupplies". Jede Gruppe kann weitere native Gruppen enthalten.

1. Klicken Sie im Administrator-Tool auf die Registerkarte „Sicherheit“.
2. Klicken Sie im Menü "Sicherheitsaktionen" auf "Gruppe erstellen".
3. Geben Sie folgende Informationen für die Gruppe ein:

Eigenschaft	Beschreibung
Name	Name der Gruppe. Beim Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden, und er darf nicht länger als 128 Zeichen sein. Er darf weder einen Tabulator oder 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.
Übergeordnete Gruppe	Die Gruppe, zu der die neue Gruppe gehört. Wählen Sie eine native Gruppe, bevor Sie auf Gruppe erstellen geklickt haben, ist die ausgewählte Gruppe die übergeordnete Gruppe. Andernfalls wird im Feld Übergeordnete Gruppe Nativ angezeigt. Dies bedeutet, dass die neue Gruppe zu keiner Gruppe gehört.
Beschreibung	Beschreibung der Gruppe. Die Gruppenbeschreibung darf nicht länger als 765 Zeichen sein und auch die folgenden Sonderzeichen nicht enthalten: < > “

4. Klicken Sie auf "Durchsuchen", um eine andere übergeordnete Gruppe auszuwählen.

   Sie haben die Möglichkeit, mehr als eine Ebene von Gruppen und Untergruppen zu erstellen.
5. Klicken Sie auf "OK", um die Gruppe zu speichern.

Eigenschaften einer nativen Gruppe bearbeiten

Nachdem Sie eine Gruppe erstellt haben, können Sie die Gruppenbeschreibung und die Benutzerliste in der Gruppe ändern. Den Namen oder das übergeordnete Element der Gruppe können Sie nicht ändern. Um das übergeordnete Element der Gruppe zu ändern, müssen Sie die Gruppe in eine andere Gruppe verschieben.

1. Klicken Sie im Administrator-Tool auf die Registerkarte „Sicherheit“.
2. Wählen Sie im Abschnitt „Gruppen“ des Navigators eine native Gruppe aus und klicken Sie auf „Bearbeiten“.
3. Ändern Sie die Gruppenbeschreibung.
4. Um die Benutzerliste der Gruppe zu ändern, klicken Sie auf die Registerkarte „Benutzer“.

   Auf der Registerkarte Benutzer steht die Liste der Benutzer in der Domäne und die Liste der Benutzer, die der Gruppe zugeordnet wurden.
5. Um einer Gruppe Benutzer zuzuordnen, wählen Sie ein Benutzerkonto in der Spalte „Alle Benutzer“ und klicken Sie auf „Hinzufügen“.
6. Wenn Sie einen Benutzer aus einer Gruppe entfernen möchten, wählen Sie ein Benutzerkonto in der Spalte „Zugeordnete Benutzer“ und klicken Sie auf „Entfernen“.
7. Klicken Sie auf „OK“, um die Änderungen zu speichern.

Eine native Gruppe in eine andere native Gruppe verschieben

Um Gruppen von Benutzern in der nativen Sicherheitsdomäne zu organisieren, können Sie verschachtelte Gruppen einrichten und Gruppen in andere Gruppen verschieben.

Um einen native Gruppe in eine andere native Gruppe zu verschieben, klicken Sie im Abschnitt "Gruppen" des Navigators den Namen der nativen Gruppe mit der rechten Maustaste an und wählen "Gruppe verschieben".

Eine native Gruppe löschen

Um eine native Gruppe zu löschen, klicken Sie den Gruppennamen im Abschnitt Gruppen des Navigators an und wählen Sie Gruppe löschen.

Wenn Sie eine Gruppe löschen, verlieren die Benutzer in dieser Gruppe ihre Mitgliedschaft in der Gruppe und alle Berechtigungen, die sie von dieser Gruppe erben.

Wenn Sie eine Gruppe löschen, entfernt der Service Manager alle Gruppen und Untergruppen, die zu dieser Gruppe gehören.

LDAP-Gruppen

Sie können im Administrator-Tool keine LDAP-Gruppen hinzufügen, bearbeiten oder löschen und auch nicht die Benutzerzuordnungen der LDAP-Gruppen ändern. Gruppen und Benutzerzuordnungen müssen im LDAP-Verzeichnisdienst verwaltet werden.

Die Betriebssystemprofile verwalten

Wenn der PowerCenter Integration Service Betriebssystemprofile verwendet, führt er Arbeitsabläufe mit den Einstellungen derjenigen Betriebssystemprofile aus, die dem Arbeitsablauf oder dem Ordner des Arbeitsablaufs zugeordnet sind.

Sie können die Betriebssystemprofile erstellen, bearbeiten, löschen und ihnen Berechtigungen zuweisen, indem Sie das Dialogfeld "Betriebssystemprofile konfigurieren" öffnen.

Zur Anzeige des Dialogfelds "Betriebssystemprofile konfigurieren" klicken Sie im Menü Sicherheitsaktionen auf Betriebssystemprofile konfigurieren.

Führen Sie die folgenden Schritte aus, um ein Betriebssystemprofil zu konfigurieren:

1. Erstellen Sie ein Betriebssystemprofil.
2. Konfigurieren Sie die Dienstprozessvariablen und die Umgebungsvariablen in den Eigenschaften des Betriebssystemprofils.
3. Weisen Sie dem Betriebssystemprofile Berechtigungen zu.

Betriebssystemprofile erstellen.

Betriebssystemprofile müssen Sie erstellen, wenn der PowerCenter Integration Service mit Betriebssystemprofilen arbeitet.

Die folgende Tabelle beschreibt die Eigenschaften, die Sie konfigurieren müssen, um ein Betriebssystemprofil zu erstellen:

Eigenschaft	Beschreibung
Name	Name des Betriebssystemprofils. Beim Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden, und er muss in der Domäne eindeutig sein. Er darf nicht länger als 128 Zeichen sein oder mit @ beginnen. Außerdem darf er keines der folgenden Sonderzeichen enthalten: % * + \ / . ? < > Der Name darf ein ASCII-Leerzeichen enthalten, jedoch nicht an erster oder letzter Stelle. Alle anderen Leerzeichen sind nicht zulässig.
Systembenutzername	Name eines Betriebssystembenutzers, der auf den Computern, auf denen der PowerCenter Integration Service ausgeführt wird, existiert. Der PowerCenter Integration Service führt die Arbeitsabläufe mit dem Systemzugriff des im Betriebssystemprofil definierten Systembenutzers aus. **Hinweis:** Beim Erstellen von Betriebssystemprofilen können Sie weder den Systembenutzernamen als Root angeben noch einen Nicht-Root-Benutzer mit uid==0 verwenden.
$PMRootDir	Root-Verzeichnis, auf das vom Knoten aus zugegriffen werden kann. Dies ist das Root-Verzeichnis für andere Dienstprozessvariablen. Es darf keines der folgenden Sonderzeichen enthalten: * ? < > " | ,

Den Namen oder den Systembenutzernamen können Sie nach dem Erstellen eines Betriebssystemprofils nicht mehr bearbeiten. Wenn Sie den im Betriebssystemprofil angegebenen Betriebssystembenutzer nicht mehr verwenden möchten, müssen Sie das Betriebssystemprofil löschen. Nach dem Löschen eines Betriebssystemprofils müssen Sie den Repository-Ordnern, denen das Betriebssystemprofil zugewiesen war, ein anderes Betriebssystemprofil zuweisen.

Eigenschaften von Betriebssystemprofilen

Nachdem Sie ein Betriebssystemprofil erstellt haben, konfigurieren Sie die Betriebssystemprofil-Eigenschaften. Um die Eigenschaften eines Betriebssystemprofils zu bearbeiten, wählen Sie das Profil im Dialogfeld "Betriebssystemprofile konfigurieren" aus und klicken dann auf "Bearbeiten".

Hinweis: Dienstprozessvariablen, die in Sitzungseigenschaften und Parameterdateien festgelegt sind, überschreiben die Einstellungen des Betriebssystemprofils.

In der folgenden Tabelle werden die Eigenschaften eines Betriebssystemprofils beschrieben:

Eigenschaft	Beschreibung
Name	Schreibgeschützter Name des Betriebssystemprofils. Der Name darf nicht länger als 128 Zeichen sein. Er darf keine Leerzeichen oder die folgenden Sonderzeichen enthalten: \ / : * ? " < > | [ ] = + ; ,
Systembenutzername	Schreibgeschützter Name eines Betriebssystembenutzers, der auf dem Computer existiert, auf dem der PowerCenter Integration Service läuft. Der PowerCenter Integration Service führt Arbeitsabläufe mit dem Systemzugriff des Betriebssystembenutzers aus, der für das Betriebssystemprofil definiert ist.
$PMRootDir	Root-Verzeichnis, auf das vom Knoten aus zugegriffen werden kann. Dabei handelt es sich um das Root-Verzeichnis für andere Dienstprozessvariablen. Es darf die folgenden Sonderzeichen nicht enthalten: * ? < > " | ,
$PMSessionLogDir	Verzeichnis für Sitzungs-Logs. Es darf die folgenden Sonderzeichen nicht enthalten: * ? < > " | , Standard ist $PMRootDir/SessLogs.
$PMBadFileDir	Verzeichnis für Ablehnungsdateien. Es darf die folgenden Sonderzeichen nicht enthalten: * ? < > " | , Standard ist $PMRootDir/BadFiles.
$PMCacheDir	Standardverzeichnis für Index- und Datencache-Dateien. Sie können die Leistung steigern, wenn das Cache-Verzeichnis für den PowerCenter Integration Service-Prozess ein lokales Laufwerk ist. Verwenden Sie kein zugeordnetes oder eingebundenes Laufwerk für die Cache-Dateien. Es darf die folgenden Sonderzeichen nicht enthalten: * ? < > " | , Standard ist $PMRootDir/Cache.
$PMTargetFileDir	Verzeichnis für Targetdateien. Es darf die folgenden Sonderzeichen nicht enthalten: * ? < > " | , Standard ist $PMRootDir/TgtFiles.
$PMSourceFileDir	Verzeichnis für Quelldateien. Es darf die folgenden Sonderzeichen nicht enthalten: * ? < > " | , Standard ist $PMRootDir/SrcFiles.
$PMExtProcDir	Verzeichnis für externe Prozeduren. Es darf die folgenden Sonderzeichen nicht enthalten: * ? < > " | , Standard ist $PMRootDir/ExtProc.
$PMTempDir	Verzeichnis für temporäre Dateien. Es darf die folgenden Sonderzeichen nicht enthalten: * ? < > " | , Standard ist $PMRootDir/Temp.

Eigenschaft	Beschreibung
$PMLookupFileDir	Verzeichnis für Lookup-Dateien. Es darf die folgenden Sonderzeichen nicht enthalten: * ? < > " | , Standard ist $PMRootDir/LkpFiles.
$PMStorageDir	Verzeichnis nach Laufzeitdateien. Arbeitsablauf-Wiederherstellungsdateien speichern im $PMStorageDir, das in den PowerCenter Integration Service-Eigenschaften konfiguriert ist. Sitzungs-Wiederherstellungsdateien speichern im $PMStorageDir, das im Betriebssystemprofil konfiguriert ist. Es darf die folgenden Sonderzeichen nicht enthalten: * ? < > " | , Standard ist $PMRootDir/Storage.
Umgebungsvariablen	Name und Wert von Umgebungsvariablen, die vom Integration Service zur Laufzeit des Arbeitsablaufs verwendet werden. Wenn Sie die Umgebungsvariable LD_LIBRARY_PATH in den Betriebssystemprofil-Eigenschaften angeben, hängt der Integration Service hängt den Wert dieser Variablen an seine Umgebungsvariable LD_LIBRARY_PATH an. Der Integration Service verwendet den Wert seiner Umgebungsvariable LD_LIBRARY_PATH, um die Umgebungsvariablen untergeordneter Prozesse festzulegen, die für das Betriebssystemprofil generiert werden. Wenn Sie die Umgebungsvariable LD_LIBRARY_PATH in den Betriebssystemprofil-Eigenschaften nicht angeben, verwendet der Integration Service seine Umgebungsvariable LD_LIBRARY_PATH.

Betriebssystemprofil erstellen

1. Klicken Sie im Administrator Tool auf die Registerkarte Sicherheit.
2. Im Menü Sicherheitsaktionen klicken Sie auf Betriebssystemprofile konfigurieren.

   Das Dialogfeld "Betriebssystemprofile konfigurieren" erscheint.
3. Klicken Sie auf Profil erstellen.
4. Geben Sie den Benutzernamen, den Systembenutzernamen und $PMRootDir ein.
5. Klicken Sie auf OK.

   Nachdem Sie das Profil erstellt haben, müssen Sie die Eigenschaften konfigurieren.
6. Klicken Sie das Betriebssystemprofil an, das Sie konfigurieren möchten.
7. Wählen Sie die Registerkarte Eigenschaften und klicken Sie auf Bearbeiten.
8. Bearbeiten Sie die Eigenschaften und klicken Sie auf OK.
9. Wählen Sie die Registerkarte Berechtigungen aus.

   Es erscheint eine Liste aller Benutzer mit Berechtigungen auf dem Betriebssystemprofil.
10. Klicken Sie auf Bearbeiten.
11. Bearbeiten Sie die Berechtigungen und klicken Sie auf OK.

Arbeiten mit Betriebssystemprofilen in einer sicheren Domäne

Sie können Betriebssystemprofile in einer Informatica-Domäne verwenden, auf der sichere Kommunikation aktiviert ist.

Beachten Sie die folgenden Regeln und Richtlinien, wenn Sie Betriebssystemprofile in einer Domäne verwenden, auf der sichere Kommunikation aktiviert ist:

- Sie müssen die folgende Umgebungsvariable für das Betriebssystemprofil festlegen:
  INFA_TRUSTSTORE

  Legen Sie den Wert für das Verzeichnis fest, das die Truststore-Dateien für die SSL-Zertifikate für die sichere Domäne festlegt. Das Verzeichnis muss eine Truststore-Datei mit dem Namen „infa_truststore.pem“ enthalten.
- Außerdem müssen Sie, wenn der PowerCenter-Integrationdienst die Option „Sitzung auf Gitter“ verwendet, die folgenden Umgebungsvariablen für das Betriebssystemprofil festlegen:
  INFA_KEYSTORE

  Legen Sie den Wert für das Verzeichnis fest, das die Schlüsselspeicherdateien für die SSL-Zertifikate für die sichere Domäne enthält. Das Verzeichnis muss eine Schlüsselspeicherdatei mit dem Namen „infa_keystore.pem“ enthalten.

  INFA_KEYSTORE_PASSWORD

  Legen Sie den Wert für das Passwort für die Datei „infa_keystore.pem“ fest, die das SSL-Zertifikat für die sichere Domäne enthält. Das Passwort muss verschlüsselt werden. Verwenden Sie das Befehlszeilenprogramm „pmpasswd“ zum Verschlüsseln des Passworts.

Sie können die Umgebungsvariablen für das Betriebssystemprofil im Administrator-Tool festlegen. Um die Umgebungsvariablen für das Betriebssystemprofil festzulegen, klicken Sie auf **Sicherheit** > **Betriebssystemprofile**. Bearbeiten Sie die Eigenschaften des Betriebssystemprofils und legen Sie die Umgebungsvariablen fest.

Arbeiten mit Betriebssystemprofilen in einer Domäne mit Kerberos-Authentifizierung

Sie können Betriebssystemprofile in einer Informatica-Domäne verwenden, die auf einem Netzwerk mit Kerberos-Authentifizierung ausgeführt wird.

Beachten Sie die folgenden Regeln und Richtlinien, wenn Sie Betriebssystemprofile in einer Domäne verwenden, die auf einem Netzwerk mit Kerberos-Authentifizierung ausgeführt wird:

- Das Benutzerkonto für das Betriebssystemprofil muss ein Prinzipal im Active Directory-Dienst sein, das für die Kerberos-Authentifizierung verwendet wird und in eine LDAP-Sicherheitsdomäne in der Informatica-Domäne importiert wurde.
- Das Benutzerkonto muss über eine Anmeldedaten-Cache-Datei von Kerberos verfügen, die für das Benutzerkonto des Betriebssystemprofils zugänglich ist. Jedes Benutzerkonto des Betriebssystemprofils muss über eine separate Anmeldedaten-Cache-Datei verfügen.
- Die Anmeldedaten-Cache-Datei für das Benutzerkonto des Betriebssystemprofils muss weiterleitbar sein. Beispiel: Wenn Sie das *kinit*-Dienstprogramm verwenden, um die Anmeldedaten-Cache-Datei zu erstellen, müssen Sie die *-f*-Option einbeziehen.
- Die Anmeldedaten-Cache-Datei für das Benutzerkonto des Betriebssystemprofils muss verfügbar sein, wenn Sie einen Arbeitsablauf ausführen, der ein Betriebssystemprofil verwendet.
- Die Anmeldedaten-Cache-Datei für das Benutzerkonto des Betriebssystemprofils muss immer die neuesten Anmeldedaten enthalten. Sie können ein Dienstprogramm für den geplanten Job wie *cron* ausführen, um die Benutzeranmeldedaten in der Anmeldedaten-Cache-Datei regelmäßig zu aktualisieren.

- Sie müssen die folgenden Umgebungsvariablen für das Betriebssystemprofil festlegen:
  INFA_OSPI_SECURITY_DOMAIN

  Legen Sie den Wert für den Namen der Sicherheitsdomäne fest, die das Benutzerkonto für das Betriebssystemprofil enthält. Wenn sich das Benutzerkonto in der Sicherheitsdomäne des Benutzerbereichs für Kerberos befindet, müssen Sie die Variable nicht festlegen. Die Sicherheitsdomäne des Benutzerbereichs für Kerberos ist die Sicherheitsdomäne, die während der Installation erstellt wird, und denselben Namen wie der Kerberos-Benutzerbereich aufweist.

  KRB5_CONFIG

  Legen Sie den Wert für den Pfad und Dateinamen der Kerberos-Konfigurationsdatei fest. Der Name der Kerberos-Konfigurationsdatei lautet *krb5.conf*.

  KRB5CCNAME

  Legen Sie den Wert für den Pfad und Dateinamen der Anmeldedaten-Cache-Datei von Kerberos für das Benutzerkonto des Betriebssystemprofils fest.

  Sie können die Umgebungsvariablen für das Betriebssystemprofil im Administrator-Tool festlegen. Um die Umgebungsvariablen für das Betriebssystemprofil festzulegen, klicken Sie auf **Sicherheit** > **Betriebssystemprofile**. Bearbeiten Sie die Eigenschaften des Betriebssystemprofils und legen Sie die Umgebungsvariablen fest.

Kontosperre

Um die Sicherheit in der Informatica-Domäne zu verbessern, kann ein Administrator die Kontosperre der Domänenbenutzerkonten, einschließlich anderer Administrator-Benutzer, nach mehreren fehlgeschlagenen Anmeldungen erzwingen.

Der Administrator kann die Anzahl fehlgeschlagener Anmeldungen festlegen, die ein Benutzer durchführen kann, bevor das Konto gesperrt wird. Wenn ein Konto gesperrt ist, kann der Administrator das Konto in der Informatica-Domäne entsperren.

Wenn der Administrator ein Benutzerkonto entsperrt, kann der Administrator die Option „Benutzername entsperren und Passwort zurücksetzen“ auswählen, um das Benutzerpasswort zurückzusetzen. Der Administrator kann eine E-Mail an den Benutzer senden, um den Benutzer aufzufordern, das Passwort vor dem erneuten Anmelden bei der Domäne zu ändern. Um zu ermöglichen, dass die Domäne E-Mails an Benutzer sendet, wenn diese ihr Passwort zurücksetzen, konfigurieren Sie die E-Mail-Servereinstellungen für die Domäne.

Wenn der Benutzer für die Informatica-Domäne und den LDAP-Server gesperrt wird, kann der Informatica Administrator das Benutzerkonto in der Informatica-Domäne entsperren. Der Benutzer kann sich erst bei der Informatica-Domäne anmelden, wenn der LDAP-Administrator auch das Benutzerkonto im LDAP-Server entsperrt.

Hinweis: Wenn die Informatica-Domäne die Kerberos-Netzwerk-Authentifizierung verwendet, können Sie die Kontosperre nicht für Benutzerkonten konfigurieren. Die Ansicht **Kontoverwaltung** ist nicht in der Registerkarte **Sicherheit** des Administrator-Tools verfügbar.

Konfigurieren der Kontosperre

Wählen Sie die Kontosperre-Optionen aus, um Benutzerkonten in der Informatica-Domäne nach mehreren fehlgeschlagenen Anmeldungen zu sperren.

1. Klicken Sie im Administrator-Tool auf **Sicherheit** > **Kontoverwaltung**.
2. Klicken Sie im Bereich **Kontosperren-Konfiguration** auf **Bearbeiten**.
3. Legen Sie die folgenden Eigenschaften fest:

Eigenschaft	Beschreibung
Kontosperre aktivieren	Erzwingt die Kontosperre eines Informatica-Domänenbenutzerkontos nach einer bestimmten Anzahl fehlgeschlagener Anmeldungen. Standardmäßig erzwingt diese Option keine Kontosperre der Administrator-Benutzerkonten. Sie müssen die Option **Administratorkontosperre aktivieren** auswählen, um die Kontosperre für Administrator-Benutzerkonten zu erzwingen.
Administratorkontosperre aktivieren	Erzwingt die Kontosperre eines Informatica-Domänenadministrator-Benutzerkontos nach einer bestimmten Anzahl fehlgeschlagener Anmeldungen. Sie müssen die Option **Kontosperre aktivieren** auswählen, bevor Sie die Kontosperre für Administrator-Benutzerkonten erzwingen können.
Maximale Anmeldeversuche	Gibt die maximale Anzahl an aufeinander folgenden zulässigen Anmeldefehlern an, bevor ein Benutzerkonto für die Informatica-Domäne gesperrt wird.

Regeln und Richtlinien für die Kontosperre

Beachten Sie die folgenden Regeln und Richtlinien, wenn Sie die Kontosperre für Informatica-Benutzer erzwingen:

- Wenn ein Anwendungsdienst unter einem Benutzerkonto ausgeführt wird und das falsche Passwort wird für den Anwendungsdienst angegeben, wird das Benutzerkonto möglicherweise beim Starten des Anwendungsdienstes gesperrt. Der Data Integration Service, Web Services Hub Service und PowerCenter Integration Service sind resiliente Anwendungsdienste, die einen Benutzernamen und ein Passwort zur Authentifizierung beim Modell-Repository Service oder PowerCenter Repository Service verwenden. Wenn der Datenintegrationsdienst, Webdienst-Hub-Dienst oder PowerCenter-Integrationsdienst fortlaufend versucht, nach einer fehlgeschlagenen Anmeldung neu zu starten, wird das zugeordnete Benutzerkonto für die Domäne eventuell gesperrt.
- Wenn ein LDAP-Benutzerkonto für die Informatica-Domäne und den LDAP-Authentifizierungsserver gesperrt wird, kann der Informatica-Domänenadministrator das Konto in der Informatica-Domäne entsperren. Der LDAP-Administrator kann das Benutzerkonto im LDAP-Server entsperren.
- Wenn Sie die Kontosperre in der Informatica-Domäne und im LDAP-Server aktivieren, konfigurieren Sie denselben Schwellenwert für Anmeldefehler in der Informatica-Domäne und im LDAP-Server, um Verwirrung über die Richtlinie zur Kontosperre zu vermeiden.
- Wenn die Kontosperre nicht in der Informatica-Domäne aktiviert ist, ein Benutzer aber gesperrt ist, stellen Sie sicher, dass der Benutzer nicht im LDAP-Server gesperrt ist.

KAPITEL 8

Berechtigungen und Rollen

Dieses Kapitel umfasst die folgenden Themen:

Berechtigungen und Rollen - Übersicht

Die Benutzersicherheit wird durch Berechtigungen und Rollen hergestellt und verwaltet.

Sie können Berechtigungen und Rollen je nach Typ der PowerCenter Express-Lizenz ändern.

Berechtigungen

Berechtigungen bestimmen die Aktionen, die Benutzer in Anwendungs-Clients ausführen können. Informatica beinhaltet die folgenden Berechtigungen:

- Domänenberechtigungen. Bestimmen der Aktionen auf der Informatica-Domäne, die Benutzer mit dem Administrator-Tool und den Befehlszeilenprogrammen infacmd und pmrep ausführen können.

- Domänenberechtigungen. Legen Aktionen in der Informatica-Domäne fest, die Benutzer mithilfe des Administrator-Tools durchführen können.
- Analyst Service-Berechtigungen. Bestimmen der Aktionen, die Benutzer mit Informatica Analyst ausführen können.
- Berechtigung für den Content-Managementdienst. Bestimmt Aktionen, die Benutzer mit Referenztabellen im Informatica Developer-Tool und im Informatica Analyst-Tool durchführen können.
- Data Integration Service-Berechtigung. Bestimmen der Aktionen bei Anwendungen, die Benutzer mit dem Administrator-Tool und dem Befehlszeilenprogramm infacmd ausführen können. Diese Berechtigung legt auch fest, ob Benutzer Drilldown und Export bei Profilergebnissen durchführen können.
- Data Integration Service-Berechtigung. Legt Aktionen für Anwendungen fest, die Benutzer mithilfe des Administrator-Tools durchführen können. Diese Berechtigung legt auch fest, ob Benutzer Drilldown und Export bei Profilergebnissen durchführen können.
- Metadata Manager Service-Berechtigungen. Bestimmen der Aktionen, die Benutzer mit Metadata Manager ausführen können.
- Modellrepository-Dienst-Berechtigung. Bestimmen der Aktionen bei Projekten, die Benutzer mit Informatica Analyst ausführen können.
- Modellrepository-Dienst-Berechtigung. Legt Aktionen für Projekte fest, die Benutzer mithilfe von Informatica Developer durchführen können.
- PowerCenter Repository Service-Berechtigungen. Bestimmen die PowerCenter Repository-Aktionen, die Benutzer mit Repository Manager, Designer, Workflow Manager, Workflow Monitor und den Befehlszeilenprogrammen pmrep und pmcmd ausführen können.
- PowerExchange Anwendungsdienst-Berechtigungen. Bestimmen der Aktionen, die Benutzer beim PowerExchange Listener Service und PowerExchange Logger Service mit den infacmd pwx-Befehlen ausführen können.
- Reporting Service-Berechtigungen. Bestimmen der Reporting-Aktionen, die Benutzer mit Data Analyzer ausführen können.
- Reporting and Dashboards Service-Berechtigungen. Bestimmen der Aktionen, die Benutzer mit Jaspersoft ausführen können.
- Berechtigungen für den Test Data Manager-Dienst. Bestimmen Sie Datenerkennungs-, Datenmaskierungs-, Datenteilmengen- und Testdatengenerierungs-Aufgaben, die Benutzer mithilfe des Test Data Managers durchführen können.

Berechtigungen bestimmen die Aktionen, die Benutzer in Anwendungs-Clients ausführen können. Informatica stellt Berechtigungen zur Verfügung, die Aktionen bestimmen, die Benutzer mit dem Administrator-Tool durchführen können.

Sie ordnen Benutzern und Gruppen Berechtigungen für Anwendungsdienste zu. Sie können einem Benutzer verschiedene Berechtigungen für jeden Anwendungsdienst desselben Diensttyps zuweisen.

Auf der Registerkarte "Sicherheit" des Administrator-Tools weisen Sie Benutzern und Gruppen Berechtigungen zu.

Das Administrator-Tool ordnet Berechtigungen in Stufen an. Eine Berechtigung ist unter der Berechtigung aufgeführt, die sie beinhaltet. Einige Berechtigungen umfassen andere Berechtigungen. Wenn Sie Benutzern und Gruppen eine Berechtigung zuweisen, weist das Administrator-Tool auch alle darin enthaltenen Berechtigungen zu.

Berechtigungsgruppen

Die Berechtigungen für die Domäne und den Anwendungsdienst sind in Berechtigungsgruppen eingeteilt. Eine Berechtigungsgruppe ist eine Zusammenfassung von Berechtigungen, die allgemeine Benutzeraktionen definieren. Zum Beispiel: Die Domänenberechtigungen umfasst folgende Berechtigungsgruppen:

- Tools. Beinhaltet Berechtigungen zum Anmelden im Administrator-Tool.
- Sicherheits-Administration. Beinhaltet Berechtigungen zum Verwalten von Benutzern, Gruppen, Rollen und Berechtigungen.
- Domänenadministration. Beinhaltet Berechtigungen zum Verwalten der Domäne, Ordner, Knoten, Gitter, Lizenzen und Anwendungsdienste.
- Domänenadministration. Beinhaltet Berechtigungen zum Verwalten der Domäne sowie der Ordner und Anwendungsdienste.
- Sicherheits-Administration. Beinhaltet Berechtigungen zum Verwalten von Benutzern, Gruppen, Rollen und Berechtigungen.
- Domänenadministration. Beinhaltet Berechtigungen zum Verwalten der Domäne, Ordner, Knoten, Gitter, Lizenzen und Anwendungsdienste.
- Tools. Beinhaltet Berechtigungen zum Anmelden im Administrator-Tool.
- Überwachen. Enthält Berechtigungen zum Überwachen von Ultra Messaging-Bereitstellungen und zum Anzeigen von Statistiken.

Tipp: Wenn Sie Benutzern und Benutzergruppen Berechtigungen zuweisen, können Sie eine Berechtigungsgruppe auswählen, um alle Berechtigungen aus dieser Gruppe gleichzeitig zuzuweisen.

Rollen

Eine Rolle ist eine Sammlung von Berechtigungen, die Sie einem Benutzer oder einer Gruppe zuordnen. Jeder Benutzer innerhalb einer Organisation hat eine bestimmte Rolle, je nachdem, ob der Benutzer Entwickler, Administrator, einfacher Benutzer oder fortgeschrittener Anwender ist.

Zum Beispiel umfasst die Rolle "PowerCenter-Entwickler" alle PowerCenter Repository Service-Berechtigungen oder -Aktionen, die ein Entwickler ausführt.

Sie ordnen Benutzern und Gruppen für die Domäne und für Anwendungsdienste in der Domäne eine Rolle zu.

Tipp: Indem Sie Benutzer in Gruppen zusammenfassen und dann Zuweisungen von Rollen und Berechtigungen für die Gruppen vergeben, können Sie die Benutzerverwaltungsaufgaben vereinfachen. Wenn zum Beispiel ein Benutzer seinen Arbeitsplatz innerhalb der Organisation wechselt, verschieben Sie den Benutzer in eine andere Gruppe. Wenn ein neuer Benutzer zur Organisation hinzukommt, fügen Sie den Benutzer zu einer Gruppe hinzu. Die Benutzer übernehmen die Rollen und Berechtigungen, die der Gruppe zugewiesen wurden. Berechtigungen und Rollen müssen nicht erneut zugewiesen werden. Weitere Informationen finden Sie im Artikel Using Groups and Roles to Manage Informatica Access Control der Informatica-Ratgeber-Bibliothek.

Tipp: Indem Sie Benutzer in Gruppen zusammenfassen und dann Zuweisungen von Rollen und Berechtigungen für die Gruppen vergeben, können Sie die Benutzerverwaltungsaufgaben vereinfachen. Wenn zum Beispiel ein Benutzer seinen Arbeitsplatz innerhalb der Organisation wechselt, verschieben Sie den Benutzer in eine andere Gruppe. Wenn ein neuer Benutzer zur Organisation hinzukommt, fügen Sie den Benutzer zu einer Gruppe hinzu. Die Benutzer übernehmen die Rollen und Berechtigungen, die der Gruppe zugewiesen wurden. Berechtigungen und Rollen müssen nicht erneut zugewiesen werden.

Domänenberechtigungen

Domänenberechtigungen legen fest, welche Aktionen Benutzer mit dem Administrator-Tool und den Befehlszeilenprogrammen infacmd und pmrep ausführen können.

Domänenberechtigungen bestimmen die Aktionen, die Benutzer mit dem Administrator-Tool durchführen können.

Die nachstehende Tabelle beschreibt jede Domänenberechtigungsgruppe:

Berechtigungsgruppe	Beschreibung
Sicherheitsverwaltung	Beinhaltet Berechtigungen zum Verwalten von Benutzern, Gruppen, Rollen und Berechtigungen.
Domänenverwaltung	Enthält die Berechtigungen zum Verwalten der Domäne, Ordner, Knoten, Gitter, Lizenzen, Anwendungsdienste und Verbindungen.
Überwachung	Enthält Berechtigungen zum Konfigurieren der Überwachungseinstellungen, zum Anzeigen der Überwachung von Integrationsobjekten sowie zum Zugreifen auf die Überwachung.
Tools	Beinhaltet Berechtigungen zum Anmelden beim Administrator-Tool.
Cloud-Verwaltung	Beinhaltet Berechtigungen zum Hinzufügen und Anzeigen von Informatica Cloud-Organisationen im Administrator-Tool.

Berechtigungsgruppe	Beschreibung
Sicherheitsverwaltung	Beinhaltet Berechtigungen zum Verwalten von Benutzern, Gruppen, Rollen und Berechtigungen.
Domänenverwaltung	Beinhaltet Berechtigungen zum Verwalten der Domäne sowie der Anwendungsdienste und Verbindungen.
Überwachung	Enthält Berechtigungen zum Konfigurieren der Überwachungseinstellungen, zum Anzeigen der Überwachung von Integrationsobjekten sowie zum Zugreifen auf die Überwachung.
Tools	Beinhaltet Berechtigungen zum Anmelden beim Administrator-Tool.

Berechtigungsgruppe	Beschreibung
Sicherheitsverwaltung	Beinhaltet Berechtigungen zum Verwalten von Benutzern, Gruppen, Rollen und Berechtigungen.
Domänenverwaltung	Beinhaltet Berechtigungen zum Verwalten der Domäne sowie der Anwendungsdienste und Verbindungen.
Überwachung	Enthält Berechtigungen zum Überwachen von UM-Bereitstellungen und zum Anzeigen von Statistiken.
Tools	Beinhaltet Berechtigungen zum Anmelden beim Administrator-Tool.

Berechtigungsgruppe Sicherheitsverwaltung

Welche Aktionen zur Sicherheitsverwaltung ein Benutzer ausführen kann, wird durch die Berechtigungen in der Berechtigungsgruppe Sicherheitsverwaltung und in den Domänenobjektberechtigungen Berechtigungsgruppe Sicherheitsverwaltung.

Bestimmte Aufgaben der Sicherheitsverwaltung werden durch die Administratorrolle und nicht durch Berechtigungen festgelegt.

Bestimmte Aufgaben der Sicherheitsverwaltung werden durch die Administratorrolle und nicht durch Berechtigungen festgelegt. Ein Benutzer, dem die Administratorrolle für die Domäne zugewiesen wurde, kann folgende Aufgaben ausführen:

- Betriebssystemprofile erstellen.
- Berechtigungen für Betriebssystemprofile vergeben.
- Betriebssystemprofile löschen.

Hinweis: Um die Aufgaben der Sicherheitsverwaltung im Administrator-Tool ausführen zu können, müssen Benutzer auch die Zugriffsberechtigung zum Informatica Administrator haben.

Berechtigungen und Rollen gewähren

Benutzer denen das Recht "Berechtigungen und Rollen gewähren" zugewiesen wurde, können Benutzern und Gruppen Berechtigungen und Rollen zuweisen.

Die folgende Tabelle listet die zusätzlich erforderlichen Berechtigungen auf und die Aktionen, die Benutzer mit der Berechtigung "Berechtigungen und Rollen gewähren" durchführen können:

Berechtigung gilt auf:	Beschreibung
Domäne oder Anwendungsdienst	Der Benutzer kann die folgenden Aktionen durchführen: - Zuweisen von Berechtigungen zu Benutzern und Gruppen für die Domäne oder den Anwendungsdienst. - Berechtigungen und Rollen zu bearbeiten und entfernen, die Benutzern und Gruppen zugewiesen sind.

Berechtigung zum Verwalten von Benutzern, Gruppen und Rollen

Benutzern, denen die Berechtigung zum Verwalten von Benutzern, Gruppen und Rollen zugewiesen wurde, können die LDAP-Authentifizierung konfigurieren und Benutzer, Gruppen und Rollen verwalten.

Die Berechtigung zum Verwalten von Benutzern, Gruppen und Rollen enthält auch die Berechtigung "Berechtigungen und Rollen gewähren".

Die folgende Tabelle listet die zusätzlich erforderlichen Berechtigungen auf und die Aktionen, die Benutzer mit der Berechtigung "Benutzer, Gruppen und Rollen verwalten" durchführen können:

Berechtigung für	Beschreibung
-	Der Benutzer kann die folgenden Aktionen durchführen: - Die LDAP-Authentifizierung für die Domäne zu konfigurieren. - Benutzer, Gruppen und Rollen zu erstellen, zu bearbeiten und zu löschen. - LDAP-Benutzer und -gruppen zu importieren.
Betriebssystemprofil	Der Benutzer kann Eigenschaften von Betriebssystemprofilen bearbeiten.

Domänenadministrations-Berechtigungsgruppe

Die Domänenverwaltungsaktionen, die die Benutzer durchführen können, sind von den Berechtigungen in der Domänenadministrationsgruppe und den Berechtigungen für Domänenobjekte abhängig.

Einige Domänenverwaltungsaufgaben unterliegen keinen Berechtigungen, sondern der Administratorrolle. Ein Benutzer, der die Administratorrolle für die Domäne inne hat, kann folgende Aufgaben durchführen:

- Domäneneigenschaften konfigurieren.
- Erteilen der Berechtigung für die Domäne.
- Verwalten und Bereinigen von Protokollereignissen.
- Empfangen von Domänenwarnungen.
- Ausführen des Lizenzberichts.
- Anzeigen von Protokollereignissen zur Benutzeraktivität.
- Herunterfahren der Domäne.
- Zugreifen auf den Upgrade-Assistenten für Dienste.

Einige Domänenverwaltungsaufgaben erfordern vom Benutzer zugewiesene Domänenobjekt-Berechtigungen und können nicht mit normalen Berechtigungen durchgeführt werden. In der folgenden Tabelle sind die Aktionen aufgelistet, die die Benutzer nur mit Domänenobjekt-Berechtigungen durchführen können:

Berechtigung für	Beschreibung
Domäne	Der Benutzer kann die folgenden Aktionen durchführen: - Anzeigen von Domäneneigenschaften und Protokollereignissen. - Konfigurieren der globalen Einstellungen.
Ordner	Der Benutzer kann die Ordnereigenschaften anzeigen.
Anwendungsdienst	Der Benutzer kann Eigenschaften von Anwendungsdiensten und Protokollereignisse anzeigen.
Lizenzobjekt	Der Benutzer kann die Eigenschaften von Lizenzobjekten anzeigen.
Gitter	Der Benutzer kann Gittereigenschaften anzeigen.
Knoten	Der Benutzer kann Knoteneigenschaften anzeigen.
Webdienst-Hub	Der Benutzer kann den Webdienstbericht ausführen.

Berechtigung für	Beschreibung
Domäne	Der Benutzer kann die folgenden Aktionen durchführen: - Anzeigen von Domäneneigenschaften und Protokollereignissen. - Konfigurieren der globalen Einstellungen.
Anwendungsdienst	Der Benutzer kann Eigenschaften von Anwendungsdiensten und Protokollereignisse anzeigen.
Knoten	Der Benutzer kann Knoteneigenschaften anzeigen.

Hinweis: Für Domänenverwaltungsaufgaben im Administrator-Tool müssen die Benutzer ebenfalls über die Zugriffsberechtigung von Informatica-Administratoren verfügen.

Berechtigung zum Verwalten der Dienstausführung

Benutzern, denen die Berechtigung zum Verwalten der Dienstausführung zugewiesen wurde, können Anwendungsdienste aktivieren und deaktivieren und Warnungen des Anwendungsdienstes empfangen.

Die folgende Tabelle listet die zusätzlich erforderlichen Berechtigungen auf und die Aktionen, die Benutzer mit der Berechtigung "Dienstausführung verwalten" ausführen können:

Berechtigung für	Beschreibung
Anwendungsdienst	Der Benutzer kann die folgenden Aktionen durchführen: - Aktivieren und Deaktivieren von Anwendungsdiensten und Dienstprozessen. Zum Aktivieren und Deaktivieren eines Metadata Manager Service müssen Benutzer auch die Berechtigung auf dem verbundenen PowerCenter Integration Service und PowerCenter Repository Service besitzen. - Empfangen von Alarmen des Anwendungsdiensts.

Berechtigung für	Beschreibung
Anwendungsdienst	Der Benutzer kann die folgenden Aktionen durchführen: - Aktivieren und Deaktivieren von Anwendungsdiensten und Dienstprozessen. - Empfangen von Alarmen des Anwendungsdiensts.

Berechtigung zum Verwalten der Dienste

Benutzern, denen die Berechtigung zum Verwalten von Diensten zugewiesen wurde, können Anwendungsdienste und Lizenzobjekte erstellen, bearbeiten, entfernen und Berechtigungen für Anwendungsdienste und Lizenzobjekte gewähren.

Die Berechtigung zum Verwalten von Diensten beinhaltet die Berechtigung zum Verwalten der Dienstausführung.

Die folgende Tabelle listet die erforderlichen Berechtigungen und die Aktionen auf, die Benutzer mit Berechtigungen zum Verwalten von Diensten ausführen können:

Berechtigung für	Beschreibung
Domäne oder übergeordneter Ordner	Der Benutzer kann Lizenzobjekte erstellen.
Domäne oder übergeordneter Ordner, Knoten oder Gitter, auf dem der Anwendungsdienst ausgeführt wird, Lizenzobjekt und alle zugehörigen Anwendungsdienste.	Der Benutzer kann Anwendungsdienste erstellen.
Anwendungsdienst	Der Benutzer kann die folgenden Aktionen durchführen: - Konfigurieren von Anwendungsdiensten. - Gewähren von Berechtigungen für Anwendungsdienste.
Ursprungs- und Zielordner	Der Benutzer kann Anwendungsdienste oder Lizenzobjekte aus einem Ordner in einen anderen verschieben.
Domäne oder übergeordneter Ordner und Anwendungsdienst	Der Benutzer kann Anwendungsdienste entfernen.

Berechtigung für	Beschreibung
Analyst-Dienst	Der Benutzer kann Audit-Trail-Tabellen erstellen und löschen.
Metadata Manager-Dienst	Der Benutzer kann die folgenden Aktionen durchführen: - Sichern von Metadata Manager-Repository-Inhalt. - Löschen von Metadata Manager-Repository-Inhalt. - Aktualisieren des Inhalts des Metadata Manager-Diensts. **Hinweis:** Zum Erstellen oder Wiederherstellen von Metadata Manager-Repository-Inhalt muss der Benutzer zur Standardgruppe „Administrator“ gehören.
Metadata Manager-Dienst PowerCenter-Repository-Dienst	Der Benutzer kann das PowerCenter-Repository für den Metadata Manager wiederherstellen.
Modellrepository-Dienst	Der Benutzer kann die folgenden Aktionen durchführen: - Erstellen und Löschen von Modellrepository-Inhalt. - Erstellen, Löschen und Neuindizieren des Suchindex. - Aktualisieren Sie den Inhalt des Modellrepository-Diensts über das Menü **Aktionen** oder über die Befehlszeile. Die Benutzer müssen über die Berechtigung zum Erstellen, Bearbeiten und Löschen von Projekten im Modellrepository-Dienst und über Schreibberechtigung für die Projekte verfügen.
PowerCenter-Integrationsdienst	Der Benutzer kann den PowerCenter-Integrationsdienst im sicheren Modus ausführen.
PowerCenter-Repository-Dienst	Der Benutzer kann die folgenden Aktionen durchführen: - Sichern, Wiederherstellen und Aktualisieren des PowerCenter-Repository. - Konfigurieren der Datenherkunft für das PowerCenter-Repository. - Kopieren von Inhalt aus einem anderen PowerCenter-Repository. - Beenden von Benutzerverbindungen und Aufheben von PowerCenter-Repository-Sperren. - Erstellen und Löschen von PowerCenter-Repository-Inhalten. - Erstellen, Bearbeiten und Löschen wiederverwendbarer Metadatenerweiterungen im PowerCenter-Repository Manager. - Aktivieren der Versionskontrolle für das PowerCenter-Repository. - Verwalten einer PowerCenter-Repository-Domäne. - Ausführen einer erweiterten Bereinigung von Objektversionen auf Repository-Ebene im PowerCenter-Repository Manager. - Registrieren und Aufheben der Registrierung von PowerCenter-Repository-Plug-Ins. - Ausführen des PowerCenter-Repository im exklusiven Modus. - Senden von PowerCenter-Repository-Benachrichtigungen an Benutzer. - Aktualisieren von PowerCenter-Repository-Statistiken. - Aktualisieren des Inhalts des PowerCenter-Repository-Diensts.
Berichterstellungsdienst	Der Benutzer kann die folgenden Aktionen durchführen: - Sichern, Wiederherstellen und Aktualisieren des Data Analyzer Repository. - Erstellen und Löschen des Inhalts des Data Analyzer Repository.
Test Data Manager-Dienst	Der Benutzer kann die folgenden Aktionen durchführen: - Test Data Manager-Repository-Inhalt erstellen und löschen. - Inhalt des Test Data Manager-Diensts aktualisieren.
Lizenzobjekt	Der Benutzer kann die folgenden Aktionen durchführen: - Bearbeiten von Lizenzobjekten. - Gewähren von Berechtigungen für Lizenzobjekte.

Berechtigung für	Beschreibung
Lizenzobjekt und Anwendungsdienst	Der Benutzer kann einem Anwendungsdienst eine Lizenz zuweisen.
Domäne oder übergeordneter Ordner und Lizenzobjekt	Benutzer können Lizenzobjekte entfernen.

Berechtigung für	Beschreibung
Domäne, in der der Anwendungsdienst ausgeführt wird, sowie alle zugehörigen Anwendungsdienste	Der Benutzer kann Anwendungsdienste erstellen.
Anwendungsdienst	Der Benutzer kann die folgenden Aktionen durchführen: - Konfigurieren von Anwendungsdiensten. - Gewähren von Berechtigungen für Anwendungsdienste.
Modellrepository-Dienst	Der Benutzer kann die folgenden Aktionen durchführen: - Erstellen und Löschen von Modellrepository-Inhalt. - Erstellen, Löschen und Neuindizieren des Suchindex.

Berechtigung zum Verwalten von Knoten und Gittern

Benutzern, denen die Berechtigung zum Verwalten von Knoten und Gittern zugewiesen wurde, können Knoten und Gitter erstellen, konfigurieren, verschieben, entfernen, herunterfahren und Berechtigungen für Knoten und Gitter gewähren.

Die folgende Tabelle listet die zusätzlich erforderlichen Berechtigungen auf und die Aktionen, die Benutzer mit der Berechtigung "Knoten und Gitter verwalten" durchführen können:

Berechtigung für	Beschreibung
Domäne oder übergeordneter Ordner	Der Benutzer kann Knoten erstellen.
Domäne oder übergeordneter Ordner und Knoten, die Gittern zugewiesenen sind	Der Benutzer kann Gitter erstellen.
Knoten oder Gitter	Der Benutzer kann die folgenden Aktionen durchführen: - Knoten und Gitter zu konfigurieren und herunterzufahren. - Berechtigungen auf Knoten und Gittern gewähren.
Ursprungs- und Target-Ordner	Der Benutzer kann Knoten und Gitter von einem Ordner in einen anderen verschieben.
Domänen oder übergeordneten Ordnern und Knoten oder Gittern	Der Benutzer kann Knoten und Gitter entfernen.

Berechtigung zum Verwalten von Domänenordnern

Benutzern, denen die Berechtigung zum Verwalten von Domänenordnern zugewiesen wurde, können Domänenordner erstellen, bearbeiten, entfernen und Berechtigungen für Domänenordner gewähren.

Die folgende Tabelle listet die zusätzlich erforderlichen Berechtigungen auf und die Aktionen, die Benutzer mit der Berechtigung "Domänenordner verwalten" ausführen können:

Berechtigung gilt auf:	Beschreibung
Domäne oder übergeordneter Ordner	Der Benutzer kann Ordner erstellen.
Ordner	Der Benutzer kann die folgenden Aktionen durchführen: - Ordner zu bearbeiten. - Berechtigungen für Ordner gewähren.
Ursprungs- und Targetordner	Der Benutzer kann Ordner von einem übergeordneten Ordner in einen anderen verschieben.
Domänenordnern oder übergeordneter Ordnern und entfernten Ordnern	Der Benutzer kann Ordner entfernen.

Berechtigungen zum Verwalten von Verbindungen

Benutzer, denen Berechtigungen zum Verwalten von Verbindungen zugewiesen sind, können Verbindungen im Administrator-Tool, Analyst-Tool, Developer-Tool, und im Befehlszeilenprogramm infacmd erstellen, bearbeiten und löschen. Benutzer können ebenfalls Verbindungen im Developer-Tool kopieren und Berechtigungen für Verbindungen im Administrator-Tool und im Befehlszeilenprogramm infacmd erteilen.

Benutzer mit Berechtigungen zum Verwalten von Verbindungen können Verbindungen im Administrator-Tool, Developer-Tool und im infacmd-Befehlszeilenprogramm erstellen, bearbeiten und löschen. Benutzer können ebenfalls Verbindungen im Developer-Tool kopieren und Berechtigungen für Verbindungen im Administrator-Tool und im Befehlszeilenprogramm infacmd erteilen.

Benutzer, denen Verbindungsberechtigungen aber keine Berechtigungen zum Verwalten von Verbindungen zugewiesen wurden, können die folgenden Aktionen der Verbindungsverwaltung ausführen:

- Alle Verbindungs-Metadaten anzeigen, außer Passwörtern. Dafür sind Leseberechtigungen für die Verbindung erforderlich.
- Daten in der Vorschau anzeigen oder Zuordnungen, Scorecards oder Profile ausführen. Erfordert Ausführungsberechtigungen für die Verbindung.
- Anzeigen von Daten in der Vorschau oder Ausführungen eines Mappings oder Profils. Erfordert Ausführungsberechtigungen für die Verbindung.

Die folgende Tabelle listet die erforderlichen Berechtigungen und die Aktionen auf, die Benutzer mit Berechtigungen zum Verwalten von Verbindungen ausführen können:

Berechtigung	Beschreibung
-	Der Benutzer kann Verbindungen erstellen.
Schreiben in Verbindungen	Der Benutzer kann Verbindungen kopieren, bearbeiten und löschen.
Verbindung zuweisen	Der Benutzer kann Berechtigungen für Verbindungen gewähren und aufheben.

Überwachen-Berechtigungsgruppe

Die Berechtigungen in der Überwachen-Gruppe legen fest, welche Benutzer die Überwachung anzeigen und konfigurieren können.

Die folgende Tabelle listet die erforderlichen Berechtigungen und die Aktionen auf, die Benutzer mit Berechtigungen in der Überwachen-Gruppe ausführen können:

Berechtigung	Berechtigung für	Beschreibung
Globale Einstellungen konfigurieren	Domäne	Der Benutzer kann die globalen Einstellungen konfigurieren.
Statistik und Berichte konfigurieren	Domäne	Der Benutzer kann Einstellungen für die Überwachung von Statistiken und Berichten konfigurieren.
Jobs von anderen Benutzern anzeigen	-	Der Benutzer kann Jobs von anderen Benutzern anzeigen.
Statistik anzeigen	-	Der Benutzer kann Statistiken für Domänenobjekte anzeigen.
Berichte anzeigen	-	Der Benutzer kann Berichte für Domänenobjekte anzeigen.
Zugriff über Analyst-Tool	-	Der Benutzer kann auf die Überwachungsfunktion aus dem Analyst-Tool zugreifen.
Zugriff über das Developer-Tool	-	Der Benutzer kann über das Developer-Tool auf die Überwachungsfunktion zugreifen.
Zugriff über das Administrator-Tool	-	Der Benutzer kann über das Administration-Tool auf die Überwachungsfunktion zugreifen.
Aktionen für Jobs zulassen	-	Der Benutzer kann die folgenden Aktionen durchführen: - Abbrechen von Jobs. - Mapping-Jobs erneut ausgeben. - Protokolle für einen Job anzeigen

Berechtigung	Berechtigung für	Beschreibung
Konfigurieren globaler Einstellungen	Domäne	Der Benutzer kann die globalen Einstellungen konfigurieren.
Statistiken und Berichten konfigurieren	Domäne	Der Benutzer kann Einstellungen für die Überwachung von Statistiken und Berichten konfigurieren.
Jobs von anderen Benutzern anzeigen	-	Der Benutzer kann Jobs von anderen Benutzern anzeigen.
Statistik anzeigen	-	Der Benutzer kann Statistiken für Domänenobjekte anzeigen.
Berichte anzeigen	-	Der Benutzer kann Berichte für Domänenobjekte anzeigen.
Zugriff über das Developer-Tool	-	Der Benutzer kann über das Developer-Tool auf die Überwachungsfunktion zugreifen.

Berechtigung	Berechtigung für	Beschreibung
Zugriff über das Administrator-Tool	-	Der Benutzer kann über das Administration-Tool auf die Überwachungsfunktion zugreifen.
Aktionen für Jobs zulassen	-	Der Benutzer kann die folgenden Aktionen durchführen: - Abbrechen von Jobs. - Mapping-Jobs erneut ausgeben. - Protokolle für einen Job anzeigen

Um die schreibgeschützte Ansicht der Überwachen-Registerkarte zu öffnen, brauchen Benutzer keine Berechtigung für den Zugriff auf Informatica Administrator.

Tools-Berechtigungsgruppe

Die Berechtigung in der Domänen-Tool-Gruppe bestimmt, welche Benutzer Zugang zum Administrator Tool haben.

Die folgende Tabelle listet die zusätzlich erforderlichen Berechtigungen auf und die Aktionen, die Benutzer mit der Berechtigung in der Tool-Gruppe durchführen können:

Berechtigung	Berechtigung	Beschreibung
Zugriff auf Informatica Administrator	-	Der Benutzer kann die folgenden Aktionen durchführen: - Melden Sie sich beim Administrator Tool an. - Das eigene Benutzerkonto im Administrator Tool zu verwalten. - Log-Ereignisse zu exportieren.

Um die Tasks im Administrator Tool ausführen zu können, müssen Benutzer auch die Zugriffsberechtigung zum Informatica Administrator haben.

Um die infacmd Befehlsprogramme ausführen zu können oder auf die schreibgeschützte Ansicht der Registerkarte "Überwachen" Zugriff zu erhalten, benötigen die Benutzer keine Zugriffsberechtigung für den Informatica Administrator.

Berechtigungsgruppe „Cloud-Verwaltung“

Die Berechtigungen in der Gruppe „Überwachen“ legen fest, welche Benutzer Informatica Cloud-Organisationen anzeigen und konfigurieren können.

Die folgende Tabelle listet die erforderlichen Berechtigungen und die Aktionen auf, die Benutzer mit Berechtigungen in der Gruppe „Cloud-Verwaltung“ ausführen können:

Berechtigung	Berechtigung für	Beschreibung
Anzeigen der Organisation	Domäne	Benutzer können die Informatica Cloud-Organisationen und die zugehörigen Sicherheitsagenten und Cloud-Verbindungen anzeigen.
Unternehmen verwalten	Domäne	Benutzer können Informatica Cloud-Organisationen im Administrator-Tool hinzufügen.

Berechtigungen für den Analyst Service

Die Berechtigungen für den Analyst Service beinhalten Aktionen, die lizenzierte Benutzer mit dem Analyst-Tool für Projekte ausführen können.

Die folgende Tabelle listet die Berechtigungen auf, die erforderlich sind, um Projekte und Objekte in Projekten zu verwalten:

Berechtigung	Berechtigung	Beschreibung
Profile und Scorecards ausführen	Lesen im Projekt. Ausführen auf einer relationalen Datenquellenverbindung.	Der Benutzer kann Profile und Scorecards für lizenzierte Benutzer im Analyst-Tool ausführen.
Zugriff auf Mapping-Spezifikationen	Lesen im Projekt.	Der Benutzer kann im Analyst-Tool auf Mapping-Spezifikationen für lizenzierte Benutzer zugreifen.
Mapping-Spezifikationsergebnisse laden	Schreiben in Projekten.	Der Benutzer kann die Ergebnisse einer Mapping-Spezifikation für lizenzierte Benutzer in eine Tabelle oder Einfachdatei laden. **Hinweis:** Wenn Sie diese Berechtigung auswählen, ist die Berechtigung **Zugriff auf Mapping-Spezifikationen** standardmäßig eingerichtet.
Verwalten von Glossaren	-	Der Benutzer kann das Unternehmensglossar verwalten.
Zugriff auf Arbeitsbereich	-	Der Benutzer hat Zugriff auf die folgenden Arbeitsbereiche im Analyst-Tool: - **Design**-Arbeitsbereich. - **Entdeckungs**-Arbeitsbereich. - **Glossary**-Arbeitsbereich. - **Scorecards**-Arbeitsbereich. **Hinweis:** Wenn Sie diese Berechtigung auswählen, ist der Zugriff auch auf Projekte im Analyst-Tool eingerichtet. Wenn der Benutzer nicht über diese Berechtigung verfügt, muss der Benutzer entweder über die Berechtigung **Design-Arbeitsbereich**, **Erkennungs-Arbeitsbereich**, **Glossar-Arbeitsbereich** oder **Scorecards-Arbeitsbereich** verfügen, um auf Projekte zuzugreifen.
Design-Arbeitsbereich	-	Der Benutzer hat Zugriff auf den **Design**-Arbeitsbereich.
Entdeckungs-Arbeitsbereich	-	Der Benutzer hat Zugriff auf den **Entdeckungs**-Arbeitsbereich
Glossar-Arbeitsbereich	-	Der Benutzer hat Zugriff auf den **Glossar**-Arbeitsbereich
Scorecards-Arbeitsbereich	-	Der Benutzer hat Zugriff auf den **Scorecards**-Arbeitsbereich.

Berechtigungen für den Content-Management-Dienst

Die Berechtigungen für den Content-Management-Dienst bestimmen Aktionen, die lizenzierte Benutzer mit Referenztabellen durchführen können.

In der folgenden Tabelle finden Sie eine Auflistung der Berechtigungen und Rechte, die zum Verwalten von Referenztabellen erforderlich sind:

Berechtigung	Berechtigung	Beschreibung
Referenztabellen erstellen	Schreiben in Projekt	- Erstellen einer Referenztabelle im Analyst-Tool und im Developer-Tool. - Erstellen einer Referenztabelle mit infacmd rtm import. - Importieren eines Referenztabellenobjekt im Modellrepository. - Kopieren einer Referenztabelle in das Analyst-Tool und Developer-Tool. - Erstellen einer Referenztabelle aus Profildaten. **Hinweis:** Die Berechtigung "Erstellen" gewährt ebenfalls standardmäßig die Berechtigung "Bearbeiten".
Referenztabellendaten und -Metadaten bearbeiten	Lesen im Projekt	- Bearbeiten von Referenztabellen-Datenwerten im Developer-Tool und Analyst-Tool. - Hinzufügen von Profildaten zu einer Referenztabelle. - Hinzufügen oder Löschen von Spalten in einer Referenztabelle. Ändern der Referenztabellen-Metadaten wie Spaltennamen Beschreibungen und Standardwerte.

Datenintegrationsdienst-Berechtigungen

Mit den Datenintegrationsdienst-Berechtigungen werden die Aktionen festgelegt, die Benutzer unter Verwendung des Administrator-Tools und des infacmd-Befehlszeilenprogramms in Anwendungen durchführen können. Von ihnen ist es auch abhängig, ob die Benutzer Profilergebnisse mit dem Analyst-Tool und dem Developer-Tool verfeinern und exportieren können.

Mit den Datenintegrationsdienst-Berechtigungen werden die Aktionen festgelegt, die Benutzer unter Verwendung des Administrator-Tools und des infacmd-Befehlszeilenprogramms in Anwendungen durchführen können. Mit ihnen wird auch festgelegt, ob Benutzer Drilldown und Export bei Profilergebnissen im Developer-Tool durchführen können.

Die folgende Tabelle enthält die Aktionen, die die Benutzer mit der Berechtigung in der Anwendungs-Administrations-Berechtigungsgruppe durchführen können:

Berechtigungsname	Beschreibung
Anwendungen verwalten	Der Benutzer kann die folgenden Aktionen durchführen: - Sichern und Wiederherstellen einer Anwendung in einer Datei. - Eine Anwendung in einem Datenintegrationsdienst bereitzustellen und Namenskonflikte zu lösen - Eine Anwendung nach der Bereitstellung zu starten - Eine Anwendung zu suchen - Objekte in einer Anwendung starten oder stoppen. - Anwendungseigenschaften zu konfigurieren.

Der folgenden Tabelle können Sie die erforderlichen Berechtigungen und die Aktionen entnehmen, welche die Benutzer mit den Berechtigungen in der Profiling-Administration-Berechtigungsgruppe durchführen können:

Berechtigungsname	Berechtigung für	Beschreibung
Drilldown und Exportieren der Ergebnisse	Lesen im Projekt Zum Drilldown von Live-Daten ist außerdem das Ausführen der relationalen Datenquellenverbindung erforderlich.	Der Benutzer kann die folgenden Aktionen durchführen: - Drilldown von Profiling-Ergebnissen - Profiling-Ergebnisse zu exportieren.

Metadata Manager Service-Berechtigungen

Die Berechtigungen des Metadata Manager Service legen fest, welche Aktionen der Benutzer mit dem Metadata Manager ausführen kann.

Die nachstehende Tabelle beschreibt jede Metadata Manager-Berechtigungsgruppe:

Berechtigungsgruppe	Beschreibung
Katalog	Beinhaltet Berechtigungen zum Verwalten von Objekten auf der Seite Durchsuchen der Benutzeroberfläche des Metadata Manager.
Laden	Beinhaltet Berechtigungen zum Verwalten von Objekten auf der Seite Laden der Benutzeroberfläche des Metadata Manager.
Modell	Enthält Berechtigungen zum Verwalten von Objekten auf der Seite Modell der Benutzeroberfläche des Metadata Manager.
Sicherheit	Enthält Berechtigungen zum Verwalten von Objekten auf der Seite Sicherheit der Benutzeroberfläche des Metadata Manager.

Katalogberechtigungsgruppe

Die Berechtigungen in der Berechtigungsgruppe „Katalog“ bestimmen die Aufgaben, die Benutzer auf der Registerkarte **Durchsuchen** der Metadata Manager-Anwendung ausführen können. Ein Benutzer mit der Berechtigung zum Ausführen einer bestimmter Aktion muss auch berechtigt sein, die Aktion für ein

bestimmtes Objekt auszuführen. Sie können Berechtigungen auf der Registerkarte **Sicherheit** der Metadata Manager-Anwendung konfigurieren.

Die folgende Tabelle enthält eine Liste der Berechtigungen in der Katalogberechtigungsgruppe und die für die Ausführung eines Tasks an einem Objekt erforderlichen Berechtigungen.

Berechtigung	Beinhaltet Berechtigungen	Berechtigung	Beschreibung
Verknüpfungen gemeinsam nutzen	n/v	Schreiben	Der Benutzer kann einen Ordner freigeben, der eine Verknüpfung mit anderen Benutzern und Gruppen enthält.
Herkunft anzeigen	n/v	Lesen	Der Benutzer kann die folgenden Aktionen durchführen: - Data Lineage-Analysen für Metadatenobjekte, Kategorien und Fachbegriffe vornehmen. - Data Lineage-Analysen vom PowerCenter-Designer aus vornehmen. Hierzu brauchen die Benutzer Leseberechtigung für den PowerCenter-Repository-Ordner.
Zugehörige Kataloge anzeigen	n/v	Lesen	Der Benutzer kann zugehörige Kataloge anzeigen.
Berichte anzeigen	n/v	Lesen	Der Benutzer kann Metadata Manager-Berichte in Data Analyzer anzeigen.
Profilergebnisse anzeigen	n/v	Lesen	Der Benutzer kann Profiling-Informationen für Metadatenobjekte im Katalog aus einer relationalen Quelle anzeigen.
Katalog anzeigen	n/v	Lesen	Der Benutzer kann die folgenden Aktionen durchführen: - Anzeigen von Ressourcen und Metadatenobjekten im Metadatenkatalog. - Durchsuchen des Metadatenkatalogs.
Beziehungen anzeigen	n/v	Lesen	Der Benutzer kann Beziehungen für Metadatenobjekte, Kategorien und Geschäftsbegriffe anzeigen.
Beziehungen verwalten	Beziehungen anzeigen	Schreiben	Der Benutzer kann Beziehungen für benutzerdefinierte Metadatenobjekte, Kategorien und Geschäftsbegriffe erstellen, bearbeiten und löschen.
Kommentare anzeigen	n/v	Lesen	Der Benutzer kann Kommentare zu Metadatenobjekten, Kategorien und Geschäftsbegriffen anzeigen.
Kommentare posten	Kommentare anzeigen	Schreiben	Der Benutzer kann Kommentare zu Metadatenobjekten, Kategorien und Geschäftsbegriffen hinzufügen.
Kommentare löschen	- Kommentare posten - Kommentare anzeigen	Schreiben	Der Benutzer kann Kommentare zu Metadatenobjekten, Kategorien und Geschäftsbegriffen löschen.

Berechtigung	Beinhaltet Berechtigungen	Berechtigung	Beschreibung
Verknüpfungen anzeigen	n/v	Lesen	Der Benutzer kann Verknüpfungen zu Metadatenobjekten, Kategorien und Geschäftsbegriffen anzeigen.
Verknüpfungen verwalten	Verknüpfungen anzeigen	Schreiben	Der Benutzer kann Verknüpfungen zu Metadatenobjekten, Kategorien und Geschäftsbegriffen erstellen, bearbeiten und löschen.
Glossar anzeigen	n/v	Lesen	Der Benutzer kann die folgenden Aktionen durchführen: - Anzeigen von Geschäftsglossaren in der Ansicht **Glossar**. - Suchen von Geschäftsglossaren.
Objekte verwalten	n/v	Schreiben	Der Benutzer kann die folgenden Aktionen durchführen: - Bearbeiten von Metadaten im Katalog. - Erstellen, Bearbeiten und Löschen benutzerdefinierter Metadatenobjekte. Hierzu benötigen die Benutzer außerdem die Berechtigung für die Anzeige von Modellen. - Erstellen, Bearbeiten und Löschen benutzerdefinierter Metadatenressourcen. Dies erfordert außerdem die Berechtigung zum Verwalten von Ressourcen.

Berechtigungsgruppe „Laden“

Die Berechtigungen in der Berechtigungsgruppe „Laden“ bestimmen die Aufgaben, die Benutzer auf der Registerkarte **Laden** der Metadata Manager-Anwendung ausführen können. Ein Benutzer mit der Berechtigung zum Ausführen einer bestimmter Aktion muss auch berechtigt sein, die Aktion für ein

bestimmtes Objekt auszuführen. Konfigurieren Sie Berechtigungen auf der Registerkarte **Sicherheit** der Metadata Manager-Anwendung.

In der folgenden Tabelle werden die Rechte und Berechtigungen aufgelistet, die zum Verwalten einer Ressourceninstanz im Metadata Manager-Warehouse erforderlich sind:

Berechtigung	Beinhaltet Berechtigungen	Berechtigung	Beschreibung
Anzeigen der Ressource	-	Lesen	Der Benutzer kann die folgenden Aktionen durchführen: - Anzeigen von Ressourcen und Ressourceneigenschaften im Metadata Manager-Warehouse. - Exportieren von Ressourcenkonfigurationen. - Herunterladen des Metadata Manager-Agent-Installationsprogramms.
Ressource laden	Anzeigen der Ressource	Schreiben	Der Benutzer kann die folgenden Aktionen durchführen: - Laden von Metadaten für eine Ressource in das Metadata Manager-Warehouse.* - Verknüpfungen zwischen Objekten in verbundenen Ressourcen für die Datenherkunft erstellen. - Konfigurieren der Suchindizierung für Ressourcen. - Importieren von Ressourcenkonfigurationen.
Verwalten von Zeitplänen	Anzeigen der Ressource	Schreiben	Der Benutzer kann die folgenden Aktionen durchführen: - Erstellen und Bearbeiten von Zeitplänen. - Hinzufügen von Zeitplänen zu Ressourcen.
Metadaten bereinigen	Anzeigen der Ressource	Schreiben	Der Benutzer kann Metadaten für eine Ressource aus dem Metadata Manager-Warehouse entfernen.
Ressource verwalten	- Metadaten bereinigen - Anzeigen der Ressource	Schreiben	Der Benutzer kann Ressourcen erstellen, bearbeiten und löschen.
* Zum Laden von Metadaten für Business Glossary-Ressourcen sind die Berechtigungen „Ressource laden“, „Ressource verwalten“ und „Modell anzeigen“ erforderlich.			

Modell-Berechtigungsgruppe

Die Berechtigungen in der Berechtigungsgruppe „Modell“ bestimmen die Aufgaben, die Benutzer auf der Registerkarte **Modell** der Metadata Manager-Anwendung ausführen können. Sie können keine Berechtigungen für ein Modell konfigurieren.

Die folgende Tabelle listet die Berechtigungen auf, die für die Verwaltung von Modellen erforderlich sind:

Berechtigung	Beinhaltet Berechtigungen	Berechtigung	Beschreibung
Modell anzeigen	-	-	Der Benutzer kann Modelle und Klassen öffnen und Modell- und Klasseneigenschaften anzeigen. Beziehungen und Attribute für Klassen anzeigen.
Modell verwalten	Modell anzeigen	-	Der Benutzer kann benutzerdefinierte Modelle erstellen, bearbeiten und löschen. Attribute zu gepackten Modellen hinzufügen.
Modelle exportieren und importieren	Modell anzeigen	-	Der Benutzer kann benutzerdefinierte Modelle und geänderte, gepackte Modelle importieren und exportieren.

Sicherheitsberechtigungsgruppe

Die Berechtigungen in der Berechtigungsgruppe „Sicherheit“ bestimmen die Aufgaben, die Benutzer auf der Registerkarte **Sicherheit** der Metadata Manager-Anwendung ausführen können.

Standardmäßig wird die Berechtigung "Katalogberechtigungen verwalten" der Sicherheit-Berechtigungsgruppe dem Administrator oder einem Benutzer mit Administrator-Rolle auf dem Metadata Manager-Dienst zugewiesen. Sie können die Berechtigung "Katalogberechtigungen verwalten" an andere Benutzer vergeben.

In der folgenden Tabelle wird das Recht und die Berechtigung aufgelistet, die zum Verwalten von Metadata Manager-Sicherheit erforderlich sind:

Berechtigung	Beinhaltet Berechtigungen	Berechtigung	Beschreibung
Katalogberechtigungen verwalten	-	Komplettsteuerung	Der Benutzer kann die folgenden Aktionen durchführen: - Weisen Sie Benutzer- und Gruppenberechtigungen für Ressourcen, Metadaten-Objekte, Kategorien und Geschäftsbedingungen zu. - Bearbeiten Sie die Zugriffsrechte für Ressourcen, Metadaten-Objekte, Kategorien und Geschäftsbedingungen.

Berechtigungen für den Modellrepository-Dienst

Die Berechtigungen für den Modellrepository-Dienst bestimmen Aktionen, die Benutzer mit Informatica Analyst und Informatica Developer in Projekten ausführen können.

Die Berechtigungen für den Modellrepository-Dienst bestimmen Aktionen, die Benutzer mit Informatica Developer in Projekten ausführen können.

Die Berechtigungen für den Modellrepository-Dienst und für die Modellrepository-Objekte bestimmen, welche Aufgaben die Benutzer in Projekten und Objekten in Projekten durchführen können.

Die folgende Tabelle listet die erforderlichen Berechtigungen und die Aktionen auf, die Benutzer mit den Berechtigungen für den Modellrepository-Dienst ausführen können:

Berechtigung	**Berechtigung**	**Beschreibung**
-	Lesen im Projekt	Der Benutzer kann Projekte und Objekte in Projekten anzeigen.
-	Schreiben in Projekt	Der Benutzer kann Objekte in Projekten erstellen, bearbeiten und löschen.
-	Gewähren bei Projekten	Der Benutzer kann Berechtigungen für Projekte für Benutzer und Gruppen gewähren und aufheben.
Zugriff auf Analyst	-	Der Benutzer kann über das Analyst-Tool auf das Modellrepository zugreifen.
Zugriff auf Developer	-	Der Benutzer kann über das Developer-Tool auf das Modellrepository zugreifen.
Erstellen, Bearbeiten und Löschen von Projekten	-	Der Benutzer kann die folgenden Aktionen durchführen: - Erstellen von Projekten.
Erstellen, Bearbeiten und Löschen von Projekten	Schreiben in Projekten	Der Benutzer kann die folgenden Aktionen durchführen: - Bearbeiten von Projekten. - Projekte löschen, wenn der Benutzer die Projekte erstellt. - Aktualisieren des Inhalts des Modellrepository-Diensts. Um den Dienst über das Menü **Aktionen** oder über die Befehlszeile zu aktualisieren, muss der Benutzer ebenfalls über die Berechtigung zum Verwalten des Diensts für die Domäne sowie über die Berechtigung für den Modellrepository-Dienst verfügen. Um den Dienst mithilfe des Upgrade-Assistenten zu aktualisieren, muss der Benutzer auch über die Administrator-Rolle für die Domäne verfügen.
Verwalten von Datendomänen	-	Der Benutzer kann Datendomänen in dem Verzeichnis der Datendomäne erstellen, bearbeiten und löschen. Diese Berechtigungen werden unter der Überschrift **Datendomänenverwaltung** angezeigt.

Berechtigung	Berechtigung	Beschreibung
Verwalten von Benachrichtigungen	-	Der Benutzer kann Scorecard-Benachrichtigungen konfigurieren. Diese Berechtigung wird unter der Überschrift **Profiling-Verwaltung** angezeigt.
Anzeigen von Sicherheitsdetails	-	Der Benutzer kann die Namen der Projekte anzeigen, für die Benutzer keine Leseberechtigung in den Fehler- und Warnmeldungsdetails haben.

Berechtigung	Berechtigung	Beschreibung
-	Lesen im Projekt	Der Benutzer kann Projekte und Objekte in Projekten anzeigen.
-	Schreiben in Projekt	Der Benutzer kann Objekte in Projekten erstellen, bearbeiten und löschen.
-	Gewähren bei Projekten	Der Benutzer kann Berechtigungen für Projekte für Benutzer und Gruppen gewähren und aufheben.
Zugriff auf Developer	-	Der Benutzer kann über das Developer-Tool auf das Modellrepository zugreifen.
Erstellen, Bearbeiten und Löschen von Projekten	-	Der Benutzer kann die folgenden Aktionen durchführen: - Erstellen von Projekten. - Aktualisieren des Modellrepository-Diensts.
Erstellen, Bearbeiten und Löschen von Projekten	Schreiben in Projekt	Der Benutzer kann die folgenden Aktionen durchführen: - Bearbeiten von Projekten. - Projekte löschen, wenn der Benutzer die Projekte erstellt.
Anzeigen von Sicherheitsdetails	-	Der Benutzer kann die Namen der Projekte anzeigen, für die Benutzer keine Leseberechtigung in den Fehler- und Warnmeldungsdetails haben.

PowerCenter Repository Service-Berechtigungen

Die Berechtigungen für den PowerCenter Repository Service bestimmen die PowerCenter Repository-Aktionen, die Benutzer mithilfe von PowerCenter Repository Manager, Designer, Workflow Manager, Workflow Monitor und dem Befehlszeilenprogramm pmrep ausführen können.

Die folgende Tabelle beschreibt die einzelnen Berechtigungsgruppen für den PowerCenter Repository Service:

Berechtigungsgruppe	Beschreibung
Tools	Beinhaltet Berechtigungen für den Zugriff auf PowerCenter Client-Tools und Befehlszeilenprogramme.
Ordner	Beinhaltet Berechtigungen zur Verwaltung von Repository-Ordnern.

Berechtigungsgruppe	Beschreibung
Designobjekte	Beinhaltet Berechtigungen zum Verwalten von Geschäftskomponenten, Zuordnungsparametern und -variablen, Zuordnungen, Mapplets, Umwandlungen und benutzerdefinierten Funktionen.
Quellen und Targets	Beinhaltet Berechtigungen zum Verwalten von Cubes, Dimensionen, Quelldefinitionen und Target-Definitionen.
Laufzeitobjekte	Beinhaltet Berechtigungen zum Verwalten von Sitzungskonfigurationsobjekten, Tasks, Arbeitsabläufen und Worklets.
Globale Objekte	Beinhaltet Berechtigungen zum Verwalten von Verbindungsobjekten, Bereitstellungsgruppen, Beschriftungen und Abfragen.

Benutzer müssen über die Manage Services-Domänenberechtigungen und Berechtigungen für den PowerCenter Repository Service verfügen, um die folgenden Aktionen im Repository Manager durchführen zu können:

- Erweiterte Bereinigung von Objektversionen auf PowerCenter Repository-Ebene durchführen.
- Wiederverwendbare Metadaten-Erweiterungen erstellen, bearbeiten und löschen.

Tools-Berechtigungsgruppe

Die Berechtigungen in der PowerCenter Repository Service-Tools-Berechtigungsgruppe bestimmen die PowerCenter-Client-Tools und Befehlszeilenprogramme, auf die Benutzer zugreifen können.

Die folgende Tabelle listet die Aktionen auf, die Benutzer mit Berechtigungen in der Tools-Gruppe ausführen können:

Berechtigung	Berechtigung	Beschreibung
Designer öffnen	-	Der Benutzer kann sich mit dem PowerCenter-Repository verbinden, indem der Designer verwendet wird.
Zugriff auf Repository Manager	-	Der Benutzer kann die folgenden Aktionen durchführen: - Verbindung mit dem PowerCenter-Repository mithilfe von Repository Manager herstellen. - *pmrep*-Befehle ausführen.
Workflow Manager öffnen	-	Der Benutzer kann die folgenden Aktionen durchführen: - Verbindung mit dem PowerCenter-Repository mithilfe von Workflow Manager herstellen. - Einen PowerCenter Integration Service aus dem Workflow Manager entfernen.
Workflow Monitor öffnen	-	Der Benutzer kann die folgenden Aktionen durchführen: - Verbindung mit dem PowerCenter-Repository mithilfe von Workflow Monitor herstellen. - Verbindung mit dem PowerCenter-Repository im Workflow Monitor herstellen.

Hinweis: Wenn der PowerCenter Integration Service im abgesicherten Modus läuft, müssen die Benutzer über die Administrator-Rolle für den zugehörige PowerCenter Repository Service verfügen.

Die entsprechende Berechtigung in der Tools-Berechtigungsgruppe ist für alle Benutzer erforderlich, die Tasks in PowerCenter Client-Tools und Befehlszeilenprogramme ausführen. Zum Beispiel: Um Ordner im Repository-Manager zu erstellen, muss ein Benutzer über die Berechtigungen zum Erstellen von Ordnern und für den Zugriff auf Repository Manager verfügen.

Wenn Benutzer über eine Berechtigung in der Tools-Berechtigungsgruppe für ein PowerCenter Repository-Objekt verfügen, aber nicht die Berechtigung zum Ändern des Objekttyps haben, können Sie dennoch einige Aktionen am Objekt durchführen. Zum Beispiel: Ein Benutzer hat die Berechtigung für den Zugriff auf den Repository Manager und Leseberechtigung für einige Ordner. Der Benutzer hat keine der Berechtigungen in der Ordner-Berechtigungsgruppe. Der Benutzer kann Objekte in den Ordnern anzeigen und die Ordner vergleichen.

Ordnerberechtigungsgruppe

Ordnerverwaltungsaktionen unterliegen Berechtigungen in der Ordnerberechtigungsgruppe, PowerCenter Repository Objektberechtigungen und Domänenobjektberechtigungen. Die Benutzer führen Ordnerverwaltungsaktionen im Repository Manager und mit dem Befehlszeilenprogramm pmrep durch.

Mache Ordnerverwaltungstasks unterliegen dem Ordnereigentum und der Administratorrolle, sind jedoch von Berechtigungen unabhängig. Der Eigentümer des Ordners oder ein Benutzer mit Administratorrolle für den PowerCenter Repository Service kann folgende Ordnerverwaltungstasks durchführen:

- Zuweisen von Betriebssystemprofilen zu den Ordnern, wenn der PowerCenter Integration Service Betriebssystemprofile nutzt. Erfordert die Berechtigung für das Betriebssystemprofil.
- Ändern des Ordnereigentümers.
- Konfigurieren der Ordnerberechtigungen.
- Löschen des Ordners.
- Benennen des gemeinsam zu verwendenden Ordners.
- Bearbeiten des Namens und der Beschreibung des Ordners.

Benutzer mit Ordnerberechtigungen, die jedoch nicht über normale Berechtigungen verfügen, können manche Ordnerverwaltungsaktionen durchführen. In der folgenden Tabelle sind die Aktionen aufgezählt, die die Benutzer ausführen können, wenn sie nur über Ordnerberechtigungen verfügen:

Berechtigung	Beschreibung
Lesen in Ordner	Der Benutzer kann die folgenden Aktionen durchführen: - Ordner vergleichen. - Anzeigen von Objekten in Ordnern.

Hinweis: Um Aktionen in Ordnern auszuführen, müssen die Benutzer außerdem die Berechtigung für den Zugriff auf den Repository Manager besitzen.

Berechtigung zum Erstellen von Ordnern

Benutzer, denen die Berechtigung "Ordner erstellen" zugewiesen wurde, können Ordner im PowerCenter Repository erstellen.

Die folgende Tabelle listet die zusätzlich erforderlichen Berechtigungen auf und die Aktionen, die Benutzer mit der Berechtigung "Ordner erstellen" ausführen können:

Berechtigung	Beschreibung
-	Der Benutzer kann Ordner erstellen.

Berechtigung zum Kopieren von Ordnern

Benutzer, die die Berechtigung "Ordner kopieren" erhalten haben, können Ordner aus einem PowerCenter Repository in ein anderes PowerCenter Repository kopieren.

Die folgende Tabelle listet die zusätzlich erforderlichen Berechtigungen auf und die Aktionen, die Benutzer mit der Berechtigung "Ordner kopieren" ausführen können.

Berechtigung	Beschreibung
Lesen in Ordner	Der Benutzer kann Ordner innerhalb desselben PowerCenter-Repository oder auf ein anderes PowerCenter-Repository kopieren. Die Benutzer müssen ferner über die Berechtigung "Ordner erstellen" im Target-Repository verfügen.

Verwalten von Ordnerversionen

Falls Sie nicht über eine team-basierte Entwicklungsoption verfügen, weisen Sie Benutzern die Berechtigung zum Verwalten von Ordnerversionen in einem PowerCenter-Repository mit Versionsangabe zu. Die Benutzer können den Status der Ordner ändern und weitreichende Löschaktionen für Objektversionen auf Ordnerebene durchführen.

In der folgenden Tabelle werden die zusätzlich erforderlichen Berechtigungen aufgelistet und die Aktionen, die Benutzer mit der Berechtigung "Ordnerversionen verwalten" ausführen können:

Berechtigung	Beschreibung
Lesen und Schreiben in Ordner	Der Benutzer kann die folgenden Aktionen durchführen: - Den Status von Ordnern zu ändern. - Weitreichende Löschaktionen für Objektversionen auf Ordnerebene durchzuführen.

Designobjekt-Berechtigungsgruppe

Berechtigungen in der Designobjekt-Berechtigungsgruppe und PowerCenter Repository Objektberechtigungen bestimmen, welche Aktionen die Benutzer mit den folgenden Designobjekten durchführen können:

- Business-Komponenten
- Mapping-Parameter und -Variablen
- Mappings
- Mapplets
- Umwandlungen

- Benutzerdefinierte Funktionen

Einige Aktionen für Designobjekte können mit Benutzern zugeordneten Berechtigungen, nicht jedoch mit normalen Berechtigungen durchgeführt werden. Aus der folgenden Tabelle gehen die Aktionen hervor, die Benutzer ausführen können, wenn ihnen nur normale Berechtigungen zugewiesen wurden:

Berechtigung	Beschreibung
Lesen in Ordner	Der Benutzer kann die folgenden Aktionen durchführen: - Designobjekte vergleichen. - Designobjekte als Bild zu kopieren. - Designobjekte exportieren. - Code für benutzerspezifische Umwandlungen und externe Prozeduren zu generieren. - PowerCenter Repository-Benachrichtigungen empfangen. - Data Lineage für Designobjekte ausführen. Die Benutzer müssen außerdem über Lineage-Anzeigeberechtigung für den Metadata Manager Service und Leseberechtigung für Metadatenobjekte im Metadata Manager Katalog verfügen. - Suchen nach Designobjekten - Anzeigen von Designobjekten, Designobjekt-Abhängigkeiten und der Designobjekt-Historie.
Lesen in freigegebenem Ordner Lesen und Schreiben in Targetordner	Der Benutzer kann Shortcuts erstellen.

Hinweis: Um Aktionen mit Designobjekten auszuführen, müssen die Benutzer außerdem über die entsprechende Berechtigung in der Berechtigungsgruppe für Tools verfügen.

Berechtigung zum Erstellen, Bearbeiten und Löschen von Designobjekten

Benutzer mit der Berechtigung zum Erstellen, Bearbeiten und Löschen von Designobjekten können Business-Komponenten, Mapping-Parameter, Mapping-Variablen, Mappings, Mapplets, Umwandlungen und benutzerdefinierte Funktionen erstellen, bearbeiten und löschen.

Die folgende Tabelle listet die erforderlichen Berechtigungen und die Aktionen auf, die Benutzer mit der Berechtigung zum Erstellen, Bearbeiten und Löschen von Designobjekten ausführen können:

Berechtigung	Beschreibung
Lesen in ursprünglichem Ordner Lesen und Schreiben in Targetordner	Der Benutzer kann die folgenden Aktionen durchführen: - Kopieren von Designobjekten von einem Ordner in einen anderen. - Kopieren von Design-Objekten in ein anderes PowerCenter-Repository. Die Benutzer müssen außerdem über die Berechtigung zum Erstellen, Bearbeiten und Löschen von Designobjekten im Target-Repository verfügen.
Lesen und Schreiben in Ordner	Der Benutzer kann die folgenden Aktionen durchführen: - Anmerkungen für ein versionsspezifisches Designobjekt ändern. - Designobjekte anmelden und Abmeldungen von Designobjekten, die von deren eigenem Benutzerkonto vorgenommen wurden, wieder aufheben. - Abmelden von Designobjekten. - Kopieren und Einfügen von Design-Objekten in ein- und demselben Ordner. - Erstellen, Bearbeiten und Löschen von Datenprofilen und Starten des Profile Manager. Die Benutzer müssen außerdem über die Berechtigung zum Erstellen, Bearbeiten und Löschen von Laufzeitobjekten verfügen. - Erstellen, Bearbeiten und Löschen von Designobjekten. - Generieren und Bereinigen von SAP ABAP-Programmen. - Generieren von Integrations-Mappings für Business-Inhalte. Die Benutzer müssen außerdem über die Berechtigung zum Erstellen, Bearbeiten und Löschen von Quellen und Targets verfügen. - Importieren von Designobjekten mit dem Designer. Die Benutzer müssen außerdem über die Berechtigung zum Erstellen, Bearbeiten und Löschen von Quellen und Targets verfügen. - Importieren von Designobjekten mit dem Repository Manager. Die Benutzer müssen außerdem über die Berechtigung zum Erstellen, Bearbeiten und Löschen von Laufzeitobjekten und zum Erstellen, Bearbeiten und Löschen von Quellen und Targets verfügen. - Wiederherstellen einer früheren Designobjektversion. - Validieren von Mappings, Mapplets und benutzerdefinierten Funktionen.

Berechtigung zum Verwalten von Designobjektversionen

Wenn Sie über eine teambasierte Bereitstellungsoption verfügen, weisen Sie Benutzern die Berechtigung zum Verwalten von Designobjektversionen in einem PowerCenter-Repository mit Versionsangabe zu. Die Benutzer können den Status der Designobjektversionen ändern, wiederherstellen oder löschen. Ferner können sich die Benutzer einchecken und das Auschecken anderer Benutzer rückgängig machen.

Die Berechtigung "Designobjektversionen verwalten" enthält die Berechtigung zum Erstellen, Bearbeiten und Löschen von Designobjekten.

Die folgende Tabelle listet die zusätzlich erforderlichen Berechtigungen auf und die Aktionen, die Benutzer mit der Berechtigung "Designobjektversionen verwalten" durchführen können:

Berechtigung	Beschreibung
Lesen und Schreiben in Ordner	Der Benutzer kann die folgenden Aktionen durchführen: - Den Status von Designobjekte zu ändern - Einzuchecken und das Auschecken der Designobjekte durch andere Benutzer rückgängig zu machen. - Versionen der Designobjekte zu löschen. - Gelöschte Designobjekte wiederherzustellen.

Quell- und Target-Berechtigungsgruppe

Berechtigungen in den Quell- und Target-Berechtigungsgruppe und bei den PowerCenter Repository-Objektberechtigungen bestimmen die Aktionen, die Benutzer bei den folgenden Quell- und Target-Objekten ausführen können:

- Würfel
- Dimensionen
- Quelldefinitionen
- Target-Definitionen

Benutzer mit zugewiesenen Erlaubnissen, aber ohne entsprechende Berechtigungen, können einige Aktionen für Quell- und Target-Objekte durchführen. Die folgende Tabelle listet die Aktionen auf, die Benutzer ausführen können, wenn sie nur Berechtigungen zugewiesen bekommen haben:

Berechtigung	Beschreibung
Lesen in Ordner	Der Benutzer kann die folgenden Aktionen durchführen: - Vergleichen von Quell- und Target-Objekten. - Exportieren von Quell- und Target-Objekten. - Vorschau auf Quell- und Targetdaten. - PowerCenter Repository-Benachrichtigungen erhalten. - Ausführen von Datenherkunft auf Quell- und Target-Objekten. Benutzer müssen auch über die Berechtigung zum Anzeigen der Herkunft für den Metadata Manager Service und Leserechte für Metadaten-Objekten im Metadata Manager-Katalog verfügen. - Suchen nach Quell- und Target-Objekten. - Alle Quell-und Target-Objekte, Quell-und Target-Objektabhängigkeiten und Quell-und Target-Objekthistorie.
Lesen in freigegebenem Ordner Lesen und Schreiben in Targetordner	Verknüpfungen erstellen.

Hinweis: Um Aktionen auf Quell- und Target-Objekten durchzuführen, müssen Benutzer auch die dazugehörigen Berechtigungen in der Tools-Berechtigungsgruppe haben.

Erstellen, Bearbeiten und Löschen einer Quellen- und Target-Berechtigung

Benutzer, die über die Berechtigung zum Erstellen, Bearbeiten und Löschen von Quellen und Targets verfügen, können Würfel, Dimensionen, Quelldefinitionen und Zieldefinition erstellen, bearbeiten und löschen.

Die folgende Tabelle enthält eine Liste der Berechtigungen und Aktionen, die die Benutzer mit der Berechtigung zum Erstellen, Bearbeiten und Löschen von Quellen und Targets ausführen können:

Berechtigung	Beschreibung
Lesen in ursprünglichem Ordner Lesen und Schreiben in Targetordner	Der Benutzer kann die folgenden Aktionen durchführen: - Quell- und Target-Objekte in einen anderen Ordner zu kopieren. - Quell- und Target-Objekte in ein anderes PowerCenter-Repository zu kopieren. Die Benutzer benötigen außerdem die Berechtigung zum Erstellen, Bearbeiten und Löschen von Quellen und Targets im Target-Ordner.
Lesen und Schreiben in Ordner	Der Benutzer kann die folgenden Aktionen durchführen: - Anmerkungen für ein versionsspezifisches Quell- oder Target-Objekt ändern. - Anmelden und Rückgängigmachen einer Abmeldung von Quell- und Target-Objekten, die von ihrem eigenen Benutzerkonto abgemeldet wurden. - Abmelden von Quell- und Target-Objekten. - Kopieren und Einfügen von Quell- und Target-Objekten in demselben Ordner. - Erstellen, Bearbeiten und Löschen von Quell- und Target-Objekten. - Importieren von SAP-Funktionen. - Importieren von Quell- und Target-Objekten mit dem Designer. Die Benutzer müssen außerdem über die Berechtigung zum Erstellen, Bearbeiten und Löschen von Design-Objekten verfügen. - Importieren von Quell- und Target-Objekten mit dem Repository Manager. Die Benutzer müssen außerdem über die Berechtigung zum Erstellen, Bearbeiten und Löschen von Design-Objekten und zum Erstellen, Bearbeiten und Löschen von Laufzeitobjekten verfügen. - Generieren und Ausführen von SQL zum Erstellen von Targets in einer relationalen Datenbank. - Zurückführen auf eine frühere Quellen- oder Target-Objektversion.

Berechtigung zum Verwalten von Quell- und Zielversionen

Wenn Sie über eine teambasierte Entwicklungsoption verfügen, weisen Sie Benutzern die Berechtigung zum Verwalten von Quell- und Target-Versionen in einem PowerCenter-Repository mit Versionsangabe zu. Benutzer können den Status von Quell- und Zielobjekten ändern, sie wiederherstellen und ihre Versionen bereinigen. Ferner können sich die Benutzer einchecken und das Auschecken anderer Benutzer rückgängig machen.

Die Berechtigung zum Verwalten von Quell- und Zielversionen beinhaltet die Berechtigungen zum Erstellen, Bearbeiten und Löschen von Quellen und Zielen.

Die folgende Tabelle listet die erforderlichen Berechtigungen und die Aktionen auf, die Benutzer mit Berechtigungen zum Verwalten von Quell- und Zielversionen ausführen können:

Berechtigung	Beschreibung
Lesen und Schreiben in Ordner	Der Benutzer kann die folgenden Aktionen durchführen: - Status von Quell- und Zielobjekten ändern. - Quell- und Zielobjekte einchecken und das Auschecken von Quell- und Zielobjekten rückgängig machen, das von anderen Benutzern ausgeführt wurde. - Versionen von Quell- und Zielobjekten bereinigen. - Gelöschte Quell- und Zielobjekten wiederherstellen.

Laufzeitobjekte-Berechtigungsgruppe

Berechtigungen in der Laufzeitobjekte-Berechtigungsgruppe und bei den PowerCenter Repository-Objektberechtigungen bestimmen die Objektberechtigungen, die Benutzer bei den folgenden Laufzeitobjekten ausführen können:

- Sitzungskonfigurationsobjekte
- Tasks
- Arbeitsabläufe
- Worklets

Einige der Tasks bei Laufzeitobjekten werden von der Administrator-Rolle bestimmt, nicht durch Berechtigungen. Ein Benutzer mit Administrator-Rolle für den PowerCenter Repository Service kann einen PowerCenter Integration Service aus dem Navigator des Workflow Managers löschen.

Benutzer mit zugewiesenen Erlaubnissen, aber ohne entsprechende Berechtigungen, können einige Aktionen für Laufzeitobjekte durchführen. Die folgende Tabelle listet die Aktionen auf, die Benutzer ausführen können, wenn sie nur Berechtigungen zugewiesen bekommen haben:

Berechtigung	Beschreibung
Lesen in Ordner	Der Benutzer kann die folgenden Aktionen durchführen: - Vergleichen von Laufzeitobjekten. - Exportieren von Laufzeitobjekten. - PowerCenter Repository-Benachrichtigungen erhalten. - Suchen nach Datenobjekten. - Verwenden von Mapping-Parameter und Variablen in einer Sitzung. - Anzeigen von Laufzeitobjekten, Laufzeitobjektabhängigkeiten und Laufzeitobjektverlauf.
Schreiben und Ausführen in Ordner	Stoppen und Abbrechen von Tasks, die von ihrem eigenen Benutzerkonto gestartet wurden. Wenn der PowerCenter Integration Service im abgesicherten Modus läuft, müssen die Benutzer über die Administrator-Rolle für den zugehörige PowerCenter Repository Service verfügen.

Hinweis: Um Aktionen bei Laufzeitobjekten durchzuführen, müssen Benutzer auch die dazugehörigen Berechtigungen in der Tools-Berechtigungsgruppe haben.

Erstellen, Bearbeiten und Löschen der Laufzeitobjektberechtigung

Benutzer mit Berechtigung zum Erstellen, Bearbeiten und Löschen von Laufzeitobjekten können Sitzungskonfigurationsobjekte, Tasks, Arbeitsabläufe und Worklets erstellen, bearbeiten und löschen.

Die folgende Tabelle enthält eine Liste der erforderlichen Berechtigungen und der Aktionen, die die Benutzer mit Berechtigung zum Erstellen, Bearbeiten und Löschen von Laufzeitobjekten ausführen können.

Berechtigung	Beschreibung
Lesen in ursprünglichem Ordner Lesen und Schreiben in Targetordner	Der Benutzer kann die folgenden Aktionen durchführen: - Tasks, Arbeitsabläufe oder Worklets von einem in einen anderen Ordner zu kopieren. - Tasks, Arbeitsabläufe oder Worklets in ein anderes PowerCenter-Repository zu kopieren. Die Benutzer müssen außerdem über die Berechtigung zum Erstellen, Bearbeiten und Löschen von Laufzeitobjekten im Target-Repository verfügen.
Lesen und Schreiben in Ordner	Der Benutzer kann die folgenden Aktionen durchführen: - Einem Arbeitsablauf in den Arbeitsablauf-Eigenschaften einen PowerCenter Integration Service zuweisen. - Einem Arbeitsablauf eine Dienstebene zuweisen. - Anmerkungen zu einem versionsspezifischen Laufzeitobjekt ändern. - Laufzeitobjekte anzumelden und die Abmeldung von Laufzeitobjekten durch deren eigenes Benutzerkonto rückgängig zu machen. - Abmelden von Laufzeitobjekten. - Tasks, Arbeitsabläufe und Worklets in ein- und demselben Ordner zu kopieren und einzufügen. - Datenprofile zu erstellen, zu bearbeiten und zu löschen und den Profile Manager zu starten. Die Benutzer benötigen außerdem die Berechtigung zu Erstellen, Bearbeiten und Löschen von Designobjekten. - Sitzungskonfigurationsobjekte zu erstellen, zu bearbeiten und zu löschen. - Tasks, Arbeitsabläufe und Worklets löschen und validieren. - Laufzeitobjekte mit dem Repository Manager zu importieren. Darüber hinaus brauchen die Benutzer die Berechtigungen zum Erstellen, Bearbeiten und Löschen von Designobjekten und zum Erstellen, Bearbeiten und Löschen von Quellen und Targets. - Laufzeitobjekte mit dem Workflow Manager zu importieren. - Eine frühere Objektversion wiederherzustellen.
Lesen und Schreiben in Ordner Lesen in Verbindungsobjekten	Der Benutzer kann die folgenden Aktionen durchführen: - Tasks, Arbeitsabläufe und Worklets erstellen und bearbeiten. - Eine relationale Datenbankverbindung für alle Sitzungen, die die Verbindung nutzen, auszuwechseln.

Berechtigung zum Verwalten der Versionen von Laufzeitobjekten

Wenn Sie über eine teambasierte Bereitstellungsoption verfügen, weisen Sie Benutzern die Berechtigung zum Ändern des Status der Laufzeitobjektversionen in einem PowerCenter-Repository mit Versionsangabe zu. Die Benutzer können den Status der Laufzeitobjektversionen ändern, wiederherstellen oder löschen. Ferner können sich die Benutzer einchecken und das Auschecken anderer Benutzer rückgängig machen.

Die Berechtigung "Laufzeitobjektversionen verwalten" enthält die Berechtigung zum Erstellen, Bearbeiten und Löschen von Designobjekten.

In der folgenden Tabelle werden die zusätzlich erforderlichen Berechtigungen aufgelistet und die Aktionen, die Benutzer mit der Berechtigung "Laufzeitobjektversionen verwalten" durchführen können:

Berechtigung	Beschreibung
Lesen und Schreiben in Ordner	Der Benutzer kann die folgenden Aktionen durchführen: - Den Status von Laufzeitobjekten zu ändern. - Einzuchecken und das Auschecken der Laufzeitobjekte durch andere Benutzer rückgängig zu machen. - Versionen der Laufzeitobjekte zu löschen. - Gelöschte Laufzeitobjekte wiederherzustellen.

Berechtigung zur Überwachung von Laufzeitobjekten

Benutzer, die die Berechtigung besitzen, Laufzeitobjekte zu überwachen, können Arbeitsabläufe und Tasks im Workflow Monitor überwachen.

Die folgende Tabelle listet die zusätzlich erforderlichen Berechtigungen auf und die Aktionen, die Benutzer mit der Berechtigung "Laufzeitobjekte überwachen" durchführen können:

Berechtigung	Benutzer haben folgende Möglichkeiten:
Lesen in Ordner	Der Benutzer kann die folgenden Aktionen durchführen: - Eigenschaften von Laufzeitobjekten im Workflow Monitor anzeigen. - Sitzungs- und Arbeitsablauf-Logs im Workflow Monitor anzeigen. - Laufzeitobjekte und Performancedetails im Workflow Monitor anzeigen. Wenn der PowerCenter Integration Service im abgesicherten Modus läuft, müssen die Benutzer über die Administrator-Rolle für den zugehörige PowerCenter Repository Service verfügen.

Berechtigung zum Ausführen von Laufzeitobjekten

Benutzer, denen die Berechtigung zum Ausführen von Laufzeitobjekten erteilt wurde, können Tasks und Arbeitsabläufe starten, kalt starten und wiederherstellen.

Die Berechtigung zum Ausführen von Laufzeitobjekten schließt die Berechtigung zum Überwachen der Laufzeitobjekte ein.

Die folgende Tabelle listet die erforderlichen Berechtigungen auf und die Aktionen, die Benutzer mit der Berechtigung zum Ausführen von Laufzeitobjekten ausführen können:

Berechtigung	Beschreibung
Schreiben und Ausführen in Ordner	Der Benutzer kann einen PowerCenter-Integration Service mithilfe des Menüs "Service" oder des Navigators einem Arbeitsablauf zuweisen.
Schreiben, Lesen und Ausführen in Ordner Lesen und Ausführen in Verbindungsobjekten	Der Benutzer kann ein Mapping debuggen, indem er eine Debug-Sitzungsinstanz erstellt oder eine vorhandene, wiederverwendbare Sitzung nutzt. Die Benutzer benötigen außerdem die Berechtigung zum Erstellen, Bearbeiten und Löschen von Laufzeitobjekten. Wenn der PowerCenter Integration Service im abgesicherten Modus läuft, müssen die Benutzer über die Administrator-Rolle für den zugehörige PowerCenter Repository Service verfügen.

Berechtigung	Beschreibung
Schreiben und Ausführen in Ordner Lesen und Ausführen in Verbindungsobjekten	Der Benutzer kann ein Mapping debuggen, indem er eine vorhandene, nicht wiederverwendbare Sitzung nutzt. Wenn der PowerCenter Integration Service im abgesicherten Modus läuft, müssen die Benutzer über die Administrator-Rolle für den zugehörige PowerCenter Repository Service verfügen.
Schreiben und Ausführen in Ordner Lesen und Ausführen in Verbindungsobjekten	Der Benutzer kann die folgenden Aktionen durchführen: - Starten, Kaltstarten und Neustarten von Tasks und Arbeitsabläufen. - Wiederherstellen von Tasks und Arbeitsabläufen, die von ihrem eigenen Benutzerkonto gestartet wurden. Wenn der PowerCenter Integration Service Betriebssystemprofile nutzt, müssen die Benutzer auch über Berechtigungen für das Betriebssystemprofil verfügen. Wenn der PowerCenter Integration Service im abgesicherten Modus läuft, müssen die Benutzer über die Administrator-Rolle für den zugehörige PowerCenter Repository Service verfügen.

Berechtigung zum Verwalten der Ausführung von Laufzeitobjekten

Benutzer, denen die Berechtigung zum Verwalten der Ausführung von Laufzeitobjekten zugewiesen ist, können Zeitpläne für Arbeitsabläufe in den erstellen und löschen. Diese Benutzer können von anderen Benutzern gestartete Arbeitsabläufe stoppen, abbrechen und wiederherstellen.

Die Berechtigung zum Verwalten der Ausführung von Laufzeitobjekten beinhaltet die Berechtigung zur Ausführung von Laufzeitobjekten und die Berechtigung zum Überwachen von Laufzeitobjekten.

Die folgende Tabelle listet die erforderlichen Berechtigungen und die Aktionen auf, die Benutzer mit Berechtigungen zum Verwalten der Ausführung von Laufzeitobjekten ausführen können:

Berechtigung	Beschreibung
Schreiben und Ausführen in Ordner	Der Benutzer kann Arbeitsablauf- und Sitzungsprotokoll-Einträge abschneiden.
Schreiben und Ausführen in Ordner	Der Benutzer kann die folgenden Aktionen durchführen: - Stoppen und Abbrechen von Tasks, die von anderen Benutzern gestartet wurden. - Stoppen und Abbrechen von Tasks, die automatisch wiederhergestellt wurden. - Zeitplanung für Arbeitsabläufe löschen. Wenn der PowerCenter Integration Service im abgesicherten Modus läuft, müssen die Benutzer über die Administrator-Rolle für den zugehörige PowerCenter Repository Service verfügen.

Berechtigung	Beschreibung
Schreiben und Ausführen in Ordner Lesen und Ausführen in Verbindungsobjekten	Der Benutzer kann die folgenden Aktionen durchführen: - Wiederherstellen von Tasks und Arbeitsabläufen, die von anderen Benutzern gestartet wurden. - Wiederherstellen von Tasks, die automatisch wiederhergestellt wurden. Wenn der PowerCenter Integration Service Betriebssystemprofile nutzt, müssen die Benutzer auch über Berechtigungen für das Betriebssystemprofil verfügen. Wenn der PowerCenter Integration Service im abgesicherten Modus läuft, müssen die Benutzer über die Administrator-Rolle für den zugehörige PowerCenter Repository Service verfügen.
Schreiben, Lesen und Ausführen in Ordner Lesen und Ausführen in Verbindungsobjekten	Der Benutzer kann die folgenden Aktionen durchführen: - Erstellen und Bearbeiten eines wiederverwendbaren Schedulers über das Menü "Arbeitsablauf > Scheduler". - Bearbeiten eines nicht wiederverwendbaren Schedulers über die Arbeitsablauf-Eigenschaften. - Bearbeiten eines wiederverwendbaren Schedulers über die Arbeitsablauf-Eigenschaften. Die Benutzer müssen auch über die Berechtigung zum Erstellen, Bearbeiten und Löschen von Laufzeitobjekten verfügen. Wenn der PowerCenter Integration Service Betriebssystemprofile nutzt, müssen die Benutzer auch über Berechtigungen für das Betriebssystemprofil verfügen. Wenn der PowerCenter Integration Service im abgesicherten Modus läuft, müssen die Benutzer über die Administrator-Rolle für den zugehörige PowerCenter Repository Service verfügen.

Berechtigungsgruppe für globale Objekte

Die Aktionen, die die Benutzer mit den folgenden globalen Objekten durchführen können, unterliegen den Berechtigungen in der Berechtigungsgruppe Globale Objekte und den Objektberechtigungen für das PowerCenter-Repository:

- Verbindungsobjekte
- Bereitstellungsgruppen
- Beschriftungen
- Abfragen

Einige globale Objekttasks werden durch globales Objekteigentum und die Administratorrolle bestimmt und unterliegen weder Rechten noch Berechtigungen. Der globale Objekteigentümer oder ein Benutzer, dem die Administratorrolle für den PowerCenter Repository Service zugeordnet wurde, kann folgende globalen Objekttasks ausführen:

- Konfigurieren globaler Objektberechtigungen.
- Ändern des globalen Objekteigentümers.
- Löschen des globalen Objekts.

Benutzer, denen Berechtigungen, jedoch keine Rechte zugewiesen wurden, können einige Aktionen für globale Objekte ausführen. Die folgende Tabelle listet die Aktionen auf, die Benutzer ausführen können, denen nur Berechtigungen zugewiesen wurden:

Berechtigung	Beschreibung
Lesen in Verbindungsobjekten	Der Benutzer kann Verbindungsobjekte anzeigen.
Lesen in Bereitstellungsgruppen	Der Benutzer kann Bereitstellungsgruppen anzeigen.
Lesen in Beschriftung	Der Benutzer kann Beschriftungen anzeigen.
Lesen in Anfrage	Der Benutzer kann Objektabfragen anzeigen.
Lesen und Schreiben von Verbindungsobjekten	Der Benutzer kann Verbindungsobjekte bearbeiten.
Lesen und Schreiben in Beschriftung	Der Benutzer kann Beschriftungen bearbeiten und sperren.
Lesen und Schreiben in Anfragen	Der Benutzer kann Objektabfragen bearbeiten und validieren.
Lesen und Ausführen der Anfrage	Der Benutzer kann Objektabfragen ausführen.
Lesen in Ordner Lesen und Ausführen der Beschriftung	Der Benutzer kann Beschriftungen anwenden und Beschriftungsreferenzen entfernen.

Hinweis: Um Aktionen mit globalen Objekten ausführen zu können, müssen die Benutzer außerdem über das entsprechende Recht in der Rechtegruppe Tools verfügen.

Berechtigung zum Erstellen von Verbindungen

Benutzer, denen die Berechtigung "Verbindung erstellen" zugewiesen wurde, können Verbindungsobjekte erstellen.

Die folgende Tabelle listet die zusätzlich erforderlichen Berechtigungen auf und die Aktionen, die Benutzer mit der Berechtigung "Verbindung erstellen" ausführen können:

Berechtigung	Beschreibung
-	Der Benutzer kann Verbindungsobjekte erstellen und kopieren.

Bereitstellungsgruppenberechtigungen verwalten

Wenn Sie über eine teambasierte Bereitstellungsoption verfügen, können Benutzer mit der Berechtigung zum Verwalten von Bereitstellungsgruppen in einem PowerCenter Repository mit Versionsangabe

Bereitstellungsgruppen erstellen, bearbeiten, kopieren und ein Rollback durchführen. Bei einem Repository ohne Versionsangabe können Benutzer Bereitstellungsgruppen erstellen, bearbeiten und kopieren.

In der folgenden Tabelle werden die erforderlichen Berechtigungen und die Aktionen aufgelistet, die Benutzer mit Berechtigungen zum Verwalten von Bereitstellungsgruppen ausführen können:

Berechtigung	Beschreibung
-	Der Benutzer kann Bereitstellungsgruppen erstellen.
Bereitstellungsgruppe lesen und schreiben	Der Benutzer kann die folgenden Aktionen durchführen: - Bereitstellungsgruppen bearbeiten. - Objekte aus einer Bereitstellungsgruppe entfernen.
Lesen in ursprünglichem Ordner Bereitstellungsgruppe lesen und schreiben	Der Benutzer kann Objekte zu einer Bereitstellungsgruppe hinzufügen.
Lesen in ursprünglichem Ordner Lesen und Schreiben in Targetordner Bereitstellungsgruppe lesen und ausführen	Der Benutzer kann Bereitstellungsgruppen kopieren.
Lesen und Schreiben in Targetordner	Der Benutzer kann Bereitstellungsgruppen zurücksetzen.

Berechtigung zur Ausführung von Bereitstellungsgruppen

Benutzer, denen die Berechtigung zur Ausführung von Bereitstellungsgruppen zugewiesen wurde, können eine Bereitstellungsgruppe kopieren, ohne eine Schreibberechtigung in den Zielordnern zu benötigen.

Die folgende Tabelle listet die zusätzlich erforderlichen Berechtigungen auf und die Aktionen, die Benutzer mit der Berechtigung "Ausführen von Bereitstellungsgruppen" durchführen können:

Berechtigung	Beschreibung
Lesen in ursprünglichem Ordner Eine Bereitstellungsgruppe auszuführen	Der Benutzer kann Bereitstellungsgruppen kopieren.

Berechtigung zum Erstellen von Beschriftungen

Wenn Sie über eine teambasierte Bereitstellungsoption verfügen, können Benutzer mit der Berechtigung zum Erstellen von Bezeichnungen in einem PowerCenter-Repository mit Versionsangabe Bezeichnungen erstellen.

Die folgende Tabelle listet die zusätzlich erforderlichen Berechtigungen auf und die Aktionen, die Benutzer mit der Berechtigung "Beschriftung erstellen" ausführen können:

Berechtigung	Beschreibung
-	Der Benutzer kann Beschriftungen erstellen.

Berechtigung zum Erstellen von Anfragen

Benutzer, denen die Berechtigung "Anfragen erstellen" zugewiesen wurde, können Objektanfragen erstellen.

Die folgende Tabelle listet die zusätzlich erforderlichen Berechtigungen auf und die Aktionen, die Benutzer mit der Berechtigung "Anfrage erstellen" ausführen können:

Berechtigung	Beschreibung
-	Der Benutzer kann Objektabfragen erstellen.

Berechtigungen des PowerExchange Listener Service

Die Berechtigungen des PowerExchange Listener Service legen fest, welche infacmd pwx Befehlsprogramm die Benutzer ausführen können.

Die folgende Tabelle beschreibt die PowerExchange Listener Service-Berechtigung in der Berechtigungsgruppe "Informelle Befehle":

Name der Berechtigung	Beschreibung
listtask	Führt den Befehl infacmd pwx ListTaskListener aus.

Die folgende Tabelle beschreibt jede PowerExchange Listener Service-Berechtigung in der Berechtigungsgruppe "Verwaltungsbefehle":

Name der Berechtigung	Beschreibung
schließen	Führt den Befehl infacmd pwx CloseListener aus.
closeforce	Führt den Befehl infacmd pwx CloseForceListener aus.
stoptask	Führt den Befehl infacmd pwx StopTaskListener aus.

PowerExchange Logger Service-Berechtigungen

Die Berechtigungen für den PowerExchange Logger Service bestimmen infacmd pwx-Befehle, die Benutzer ausführen können.

Die folgende Tabelle beschreibt die einzelnen PowerExchange Logger Service-Berechtigungen in der Berechtigungsgruppe "Informationsbefehle":

Name der Berechtigung	Beschreibung
displayall	Ausführen des Befehls infacmd pwx DisplayAllLogger.
displaycpu	Ausführen des Befehls infacmd pwx DisplayCPULogger.
displaycheckpoints	Ausführen des Befehls infacmd pwx DisplayCheckpointsLogger.
displayevents	Ausführen des Befehls infacmd pwx DisplayEventsLogger.
displaymemory	Ausführen des Befehls infacmd pwx DisplayMemoryLogger.
displayrecords	Ausführen des Befehls infacmd pwx DisplayRecordsLogger.
displaystatus	Ausführen des Befehls infacmd pwx DisplayStatusLogger.

Die folgende Tabelle beschreibt die einzelnen PowerExchange Logger Service-Berechtigungen in der Berechtigungsgruppe "Verwaltungsbefehle":

Name der Berechtigung	Beschreibung
condense	Ausführen des Befehls infacmd pwx CondenseLogger.
fileswitch	Ausführen des Befehls infacmd pwx FileSwitchLogger.
Herunterfahren	Ausführen des Befehls infacmd pwx ShutDownLogger.

Reporting Service-Berechtigungen

Die Berechtigungen für den Reporting Service bestimmen die Aktionen, die Benutzer mit Data Analyzer ausführen können.

Die folgende Tabelle beschreibt die einzelnen Berechtigungsgruppen für den Reporting Service:

Berechtigungsgruppe	Beschreibung
Administration	Beinhaltet Berechtigungen zum Verwalten von Objekten auf der Registerkarte "Administration" im Data Analyzer.
Alarme	Beinhaltet Berechtigungen zum Verwalten von Objekten auf der Registerkarte "Alarme" im Data Analyzer.
Kommunikation	Beinhaltet Berechtigungen zur gemeinsamen Nutzung von Dashboard- oder Berichtsinformationen mit anderen Benutzern.
Inhaltsverzeichnis	Beinhaltet Berechtigungen zum Verwalten von Objekten auf der Registerkarte "Suchen" im Data Analyzer.

Berechtigungsgruppe	Beschreibung
Dashboards	Beinhaltet Berechtigungen zum Verwalten von Dashboards im Data Analyzer.
Indikatoren	Beinhaltet Berechtigungen zum Verwalten von Indikatoren im Data Analyzer.
Konto verwalten	Beinhaltet Berechtigungen zum Verwalten von Objekten auf der Registerkarte "Konto verwalten" im Data Analyzer.
Berichte	Beinhaltet Berechtigungen zum Verwalten von Berichten im Data Analyzer.

Administrations-Berechtigungsgruppe

Berechtigungen in der Administrations-Berechtigungsgruppe bestimmen die Tasks, die Benutzer auf der Registerkarte Administration des Data Analyzer ausführen können.

Die folgende Tabelle enthält eine Aufzählung der Berechtigungen in der Administrations-Berechtigungsgruppe:

Berechtigung	Enthaltene Berechtigungen	Berechtigung	Beschreibung
Schema warten	-	Lesen, Schreiben und Löschen für: - metrischen Ordner - Attributsordner - Ordner für Vorlagenmaße - Metrik - Attribut - Vorlagenmaß	Der Benutzer kann Schematabellen erstellen, bearbeiten und löschen.
Export/Import von XML-Dateien	-	-	Der Benutzer kann Metadaten als XML-Dateien exportieren oder importieren.
Benutzerzugriffsverwaltung	-	-	Der Benutzer kann Benutzer, Gruppen und Rollen verwalten.
Einrichten von Plänen und Tasks	-	Lesen, Schreiben und Löschen in zeitbasierten und ereignisbasierten Plänen	Der Benutzer kann Zeitpläne und Aufgaben erstellen und verwalten.
Verwalten der Systemeigenschaften	-	-	Der Benutzer kann Systemeinstellungen und Eigenschaften verwalten.
Einrichten von Abfrage-Begrenzungen	- Verwalten der Systemeigenschaften	-	Der Benutzer hat Zugriff auf die Einstellungen, die die Abfrage regeln.
Konfigurieren von Echtzeitnachrichten strömen	-	-	Der Benutzer kann Nachrichten-Streams in Echtzeit hinzufügen, bearbeiten und entfernen.

Alarmberechtigungsgruppe

Die Berechtigungen in der Alarmberechtigungsgruppe legen fest, welche Tasks ein Benutzer auf der Registerkarte Alarm des Data Analyzer ausführen kann.

Die folgende Tabelle führt die Berechtigungen in der Alarmberechtigungsgruppe auf:

Berechtigung	Beinhaltet Berechtigungen	Berechtigung	Beschreibung
Alarme erhalten	-	-	Der Benutzer kann ausgelöste Alarme empfangen und anzeigen.
Echtzeitalarme erstellen	- Alarme erhalten	-	Der Benutzer kann einen Alarm für einen Echtzeit-Bericht erstellen.
Zustelloptionen einrichten	- Alarme erhalten	-	Der Benutzer kann Alarmzustellungsoptionen konfigurieren.

Kommunikations-Berechtigungsgruppe

Die Berechtigungen in der Kommunikations-Berechtigungsgruppe legen fest, welche Tasks ein Benutzer ausführen kann, um Dashboard- oder Berichtsinformationen mit anderen Benutzern zu teilen.

In der folgenden Tabelle sind die Berechtigungen der Kommunikations-Berechtigungsgruppe aufgelistet:

Berechtigung	Beinhaltet Berechtigungen	Berechtigung	Beschreibung
Drucken	-	Lesen im Bericht Lesen im Dashboard	Der Benutzer kann Berichte und Dashboards drucken.
E-Mail-Objektverknüpfungen	-	Lesen im Bericht Lesen im Dashboard	Der Benutzer kann Verknüpfungen von Berichten oder Dashboards in einer E-Mail versenden.
E-Mail-Objektinhalte	- E-Mail-Objektverknüpfungen	Lesen im Bericht Lesen im Dashboard	Der Benutzer kann den Inhalt von Berichten oder Dashboards in einer E-Mail versenden.
Exportieren	-	Lesen im Bericht Lesen im Dashboard	Der Benutzer kann Berichte und Dashboards exportieren.
Nach Excel oder CSV exportieren	- Exportieren	Lesen im Bericht Lesen im Dashboard	Der Benutzer kann Berichte in Excel- oder CSV-Dateien exportieren.
Export in Pivot-Tabellen	- Exportieren - Nach Excel oder CSV exportieren	Lesen im Bericht Lesen im Dashboard	Der Benutzer kann Berichte an Excel Pivottabellen exportieren.

Berechtigung	Beinhaltet Berechtigungen	Berechtigung	Beschreibung
Diskussionen anzeigen	-	Lesen im Bericht Lesen im Dashboard	Der Benutzer kann Diskussionen lesen.
Diskussionen hinzufügen	- Diskussionen anzeigen	Lesen im Bericht Lesen im Dashboard	Der Benutzer kann Nachrichten zu Diskussionen hinzufügen.
Diskussionen verwalten	- Diskussionen anzeigen	Lesen im Bericht Lesen im Dashboard	Der Benutzer kann Meldungen und Kommentare aus den Diskussionen löschen.
Feedback geben	-	Lesen im Bericht Lesen im Dashboard	Der Benutzer kann Feedback-Nachrichten erstellen.

Inhaltsverzeichnis-Berechtigungsgruppe

Berechtigungen in der Inhaltsverzeichnis-Berechtigungsgruppe bestimmen die Tasks, die die Benutzer auf der Registerkarte Suchen des Data Analyzer durchführen können.

Die folgende Tabelle enthält eine Aufzählung der Berechtigungen in der Inhaltsverzeichnis-Berechtigungsgruppe:

Berechtigung	Enthält die Berechtigungen	Berechtigung	Beschreibung
Zugriff zum Inhaltsverzeichnis	-	Lesen in Ordner	Der Benutzer kann die folgenden Aktionen durchführen: - Zugreifen auf Ordner und Inhalte der Registerkarte Suchen - Zugreifen auf persönliche Ordner. - Suchen nach Elementen, die Benutzern mit grundlegender Verbraucherrolle zur Verfügung stehen - Suchen von Berichten nach Namen oder Suchen von häufig verwendeten Berichten - Anzeigen von Berichten aus dem PowerCenter Designer oder dem Workflow Manager.
Zugreifen auf erweiterte Suchfunktionen	- Zugreifen auf das Inhaltsverzeichnis	Lesen in Ordner	Der Benutzer kann die folgenden Aktionen durchführen: - Suchen nach erweiterten Einträgen - Suchen nach von Ihnen erstellten oder von einem bestimmten Benutzer verwendeten Berichten

Berechtigung	Enthält die Berechtigungen	Berechtigung	Beschreibung
Verwalten des Inhaltsverzeichnisses	- Zugriff auf das Inhaltsverzeichnis	Lesen und Schreiben im Ordner	Der Benutzer kann die folgenden Aktionen durchführen: - Ordner erstellen. - Kopieren von Ordnern - Ausschneiden und Einfügen von Ordnern - Umbenennen von Ordnern
Verwalten des Inhaltsverzeichnisses	- Zugriff auf das Inhaltsverzeichnis	Löschen in Ordnern	Der Benutzer kann Ordner löschen.
Verwalten gemeinsam genutzter Dokumente	- Zugriff auf das Inhaltsverzeichnis - Verwalten des Inhaltsverzeichnisses	Lesen in Ordner Schreiben in Ordnern	Der Benutzer kann freigegebene Dokumente in den Ordnern löschen.

Dashboards-Berechtigungsgruppe

Die Berechtigungen in der Dashboards-Berechtigungsgruppe bestimmen die Tasks, die die Benutzer mit Dashboard im Data Analyzer wahrnehmen können.

Die folgende Tabelle enthält eine Aufzählung der Berechtigungen in der Dashboards-Berechtigungsgruppe:

Berechtigung	Enthaltene Berechtigungen	Berechtigung	Beschreibung
Anzeigen von Dashboards	-	Lesen in Dashboards	Der Benutzer kann Inhalte von persönlichen und öffentlichen Dashboards anzeigen.
Verwalten persönlicher Dashboards	- Anzeigen von Dashboards	Lesen und Schreiben von Dashboards	Der Benutzer kann das persönliche Dashboard verwalten.
Erstellen, Bearbeiten und Löschen von Dashboards	- Anzeigen von Dashboards	Lesen und Schreiben von Dashboards	Der Benutzer kann die folgenden Aktionen durchführen: - Dashboards erstellen. - Bearbeiten von Dashboards.
Erstellen, Bearbeiten und Löschen von Dashboards	- Anzeigen von Dashboards	Löschen in Dashboards	Der Benutzer kann Dashboards löschen.

Berechtigung	Enthaltene Berechtigungen	Berechtigung	Beschreibung
Zugreifen auf die Erstellung grundlegender Dashboards	- Anzeigen von Dashboards - Erstellen, Bearbeiten und Löschen von Dashboards	Lesen und Schreiben von Dashboards	Der Benutzer kann die folgenden Aktionen durchführen: - Arbeiten mit grundlegenden Dashboard-Konfigurationsoptionen. - Übertragen von Dashboards als Links.
Zugriffserstellung auf erweiterte Dashboards	- Anzeigen von Dashboards - Erstellen, Bearbeiten und Löschen von Dashboards - Zugriffserstellung auf erweiterte Dashboards	Lesen und Schreiben von Dashboards	Der Benutzer kann alle Dashboard-Konfigurationsoptionen verwenden.

Indikatoren-Berechtigungsgruppe

Die Berechtigungen in der Indikatoren-Berechtigungsgruppe legen fest, welche Tasks die Benutzer mit den Indikatoren ausführen können.

Die folgende Tabelle führt die Berechtigungen in der Indikatoren-Berechtigungsgruppe auf:

Berechtigung	Beinhaltet Berechtigungen	Berechtigung	Beschreibung
Mit Indikatoren interagieren	-	Lesen im Bericht Schreiben in Dashboard	Der Benutzer kann Indikatoren verwenden und mit ihnen interagieren.
Echtzeit-Indikator erstellen	-	Lesen und Schreiben in Bericht Schreiben in Dashboard	Der Benutzer kann die folgenden Aktionen durchführen: - Indikator für einen Echtzeit-Bericht erstellen. - Anzeigenindikator erstellen.
Kontinuierliche, automatische Echtzeit-Indikatoraktualisierungen erhalten	-	Lesen im Bericht	Der Benutzer kann kontinuierliche, automatische und animierte Echtzeitaktualisierungen von Indikatoren anzeigen.

Berechtigungsgruppen für das Verwalten von Benutzerkonten

Die Berechtigungen in der Benutzerberechtigungsgruppe legen fest, welche Tasks ein Benutzer auf der Registerkarte "Benutzerkonto verwalten" des Data Analyzer ausführen kann.

Die folgende Tabelle führt die Berechtigungen in der Berechtigungsgruppe "Benutzerkonto verwalten" auf:

Berechtigung	Beinhaltet Berechtigungen	Berechtigung	Beschreibung
Persönliche Einstellungen verwalten	-	-	Der Benutzer kann die persönlichen Kontoeinstellungen konfigurieren.

Berichte-Berechtigungsgruppe

Die Berechtigungen in der Berichte-Berechtigungsgruppe legen fest, welche Tasks die Benutzer im Data Analyzer ausführen können.

Die folgende Tabelle führt die Berechtigungen in der Berichte-Berechtigungsgruppe auf:

Berechtigung	Beinhaltet Berechtigungen	Berechtigung	Beschreibung
Berichte anzeigen	-	Lesen im Bericht	Berichte und zugehörige Metadaten anzeigen.
Berichte analysieren	- Berichte anzeigen	Lesen im Bericht	Der Benutzer kann die folgenden Aktionen durchführen: - Berichte analysieren. - Berichtsdaten, Metadaten und Charts anzeigen.
Mit Daten interagieren	- Berichte anzeigen - Berichte analysieren	Lesen und Schreiben in Bericht	Der Benutzer kann die folgenden Aktionen durchführen: - Zugriff auf die Symbolleiste auf der Registerkarte "Analysieren" und Ausführen von Aufgaben auf Datenebene bei Tabellen und Grafiken des Berichts. - Rechtsklicken auf Elemente auf der Registerkarte "Analysieren".
Beliebigen Drill ausführen	- Berichte anzeigen - Berichte analysieren - Mit Daten interagieren	Lesen im Bericht	Der Benutzer kann jedes Attribut für den Drill in Berichten auswählen.
Filtersätze erstellen	- Berichte anzeigen - Berichte analysieren - Mit Daten interagieren	Lesen und Schreiben in Bericht	Der Benutzer kann Filtersätze in Berichten erstellen und speichern.
Benutzerdefinierte Metrik fortführen	- Berichte anzeigen - Berichte analysieren - Mit Daten interagieren	In Bericht schreiben	Benutzer können benutzerdefinierte Metriken aus Berichten in Schemata hochstufen.
Abfrage anzeigen	- Berichte anzeigen - Berichte analysieren - Mit Daten interagieren	Lesen im Bericht	Der Benutzer kann Berichtsabfragen anzeigen.
Lifecycle-Metadaten anzeigen	- Berichte anzeigen - Berichte analysieren - Mit Daten interagieren	In Bericht schreiben	Der Benutzer kann Zeitschlüssel auf der Registerkarte "Zeit" bearbeiten.

Berechtigung	Beinhaltet Berechtigungen	Berechtigung	Beschreibung
Berichte erstellen und löschen	- Berichte anzeigen	Schreiben und Löschen in Berichten	Der Benutzer kann Berichte erstellen oder Löschen.
Auf grundlegende Berichtserstellung zugreifen	- Berichte anzeigen - Berichte erstellen und löschen	In Bericht schreiben	Der Benutzer kann die folgenden Aktionen durchführen: - Berichte mit einfachen Berichtsoptionen erstellen. - Übertragen der Verknüpfung zu einem Bericht in Data Analyzer und die SQL-Abfrage für den Bericht bearbeiten.
Auf erweiterte Berichtserstellung zugreifen	- Berichte anzeigen - Berichte erstellen und löschen - Auf grundlegende Berichtserstellung zugreifen	In Bericht schreiben	Der Benutzer kann die folgenden Aktionen durchführen: - Berichte mit allen verfügbaren Berichtsoptionen erstellen. - Übertragen von Berichtsinhalten als E-Mail-Anhang und Verknüpfung. - Berichte archivieren. - Excel-Vorlagen erstellen und verwalten. - Provider-basierte Sicherheit für einen Bericht festlegen.
Berichtskopien speichern	- Berichte anzeigen	In Bericht schreiben	Der Benutzer kann die Funktion "Speichern unter" verwenden, um mit einem anderen Namen zu speichern.
Berichte bearbeiten	- Berichte anzeigen	In Bericht schreiben	Der Benutzer kann Berichte bearbeiten.

Reporting and Dashboards Service-Berechtigungen

Berichts- und Dashboarddienstberechtigungen werden Rollen in Jaspersoft zugeordnet.

Die Zugriffsberechtigungsgruppe enthält alle Berichts- und Dashboarddienstberechtigungen.

Die folgende Tabelle beschreibt die einzelnen Berechtigungen für den Berichts- und Dashboarddienst:

Name der Berechtigung	Beschreibung
Administrator	Benutzer, denen eine Administrator-Berechtigung zugewiesen ist, können die folgenden Tasks auf dem JasperReports Server ausführen: - Unterorganisationen erstellen. - Benutzer erstellen, ändern und löschen. - Rollen erstellen, ändern und löschen. - Sich als ein beliebiger Benutzer in der Organisation anmelden. - Ordner und Repository-Objekte jeglicher Art erstellen, ändern und löschen. - Benutzern Rollen zuweisen, einschließlich der Rolle ROLE_ADMINISTRATOR, die Organisationsadministratorrechte gewährt. - Zugriffsberechtigungen für Repository-Ordner und -objekte festlegen. Diese Berechtigung wird der Rolle ROLE_ADMINISTRATOR bei Jaspersoft zugeordnet.
Superuser	Benutzer mit Superuser-Berechtigung können alle Tasks ausführen, die ein Benutzer mit Administratorrechten ausführen kann. Außerdem können Benutzer mit Administrator-Berechtigung die folgenden Tasks auf dem JasperReports Server ausführen: - Organisationen auf oberste Ebene erstellen. - Benutzer erstellen, die auf alle Organisationen zugreifen können. - Benutzern die Rolle ROLE_ADMINISTRATOR zuweisen, die Systemadministratorrechte gewährt. - Systemweite Konfigurationsparameter festlegen. Diese Berechtigung wird der Rolle ROLE_SUPERUSER bei Jaspersoft zugeordnet.
Normaler Benutzer	Benutzer, denen eine normale Benutzer-Berechtigung zugewiesen ist, können die folgenden Tasks auf dem JasperReports Server ausführen. Diese Berechtigung wird der Rolle ROLE_USER bei Jaspersoft zugeordnet.

Weitere Informationen zu Berechtigungen, die diesen Rollen bei Jaspersoft zugeordnet sind, finden Sie in der Jaspersoft-Dokumentation.

Berechtigungen für Test Data Manager-Dienst

Die Berechtigungen für den Test Data Manager-Dienst bestimmen die Aktionen, die Benutzer mithilfe des Test Data Manager durchführen können. Ein Benutzer mit Berechtigung zum Ausführen bestimmter Aktionen

muss auch berechtigt sein, die Aktion an einem bestimmten Objekt auszuführen. Sie können Berechtigungen auf der Registerkarte „Sicherheit“ des Administrator-Tools konfigurieren.

Die folgende Tabelle enthält Informationen zu allen Test Data Manager-Berechtigungsgruppen.

Berechtigungsgruppe	Beschreibung
Administration	Beinhaltet Berechtigungen zum Erstellen und Verwalten von Verbindungen sowie zum Zuweisen von Rollen und Berechtigungen zu Benutzern und Benutzergruppen in Informatica Administrator, zum Verwalten von Repositorys, zum Hinzufügen von Lizenzen und zum Festlegen von Arbeitsablauf- und Projektattributen. **Hinweis:** Vor dem Erstellen von Benutzern und Gruppen muss der standardmäßige Informatica-Administratorbenutzer dem Test Data Administrator-Benutzer Sicherheitsverwaltungsberechtigungen zuweisen.
Datendomänen	Beinhaltet Berechtigungen zum Anzeigen und Verwalten von Domänen im Test Data Manager.
Datenmaskierung	Beinhaltet Berechtigungen zum Anzeigen und Verwalten von Maskierungsregeln und Richtlinienzuweisungen im Test Data Manager.
Datenteilmenge	Beinhaltet Berechtigungen zum Anzeigen und Verwalten von Datenteilmengenobjekten, einschließlich Entitäten, Gruppen und Vorlagen im Test Data Manager.
Richtlinien	Beinhaltet Berechtigungen zum Anzeigen und Verwalten von Richtlinien im Test Data Manager.
Projekte	Beinhaltet Berechtigungen zum Anzeigen und Verwalten von Projekten sowie zum Prüfen und Importieren von Metadaten und zum Ausführen von Plänen und Arbeitsabläufen im Test Data Manager.
Regeln	Beinhaltet Berechtigungen zum Anzeigen und Verwalten von Maskierungs- und Generierungsregeln im Test Data Manager.
Datengenerierung	Beinhaltet Berechtigungen zum Anzeigen und Verwalten der Testdatengenerierung im Test Data Manager.

Administrations-Berechtigungsgruppe

Die Berechtigungen in der Administrations-Berechtigungsgruppe bestimmen die Verwaltungsaufgaben, die Testdaten-Administratoren durchführen können.

Die folgende Tabelle enthält eine Liste der Berechtigungen in der Administrations-Berechtigungsgruppe und die für die Ausführung einer Aufgabe an einem Objekt erforderlichen Berechtigungen.

Berechtigung	Beinhaltet Berechtigungen	Berechtigung	Beschreibung
Einstellungen verwalten	-	Schreiben	Benutzer können die folgenden Aktionen in Informatica Administrator und im Test Data Manager durchführen: - Rollen erstellen - Rollen bearbeiten - Rollen löschen - Rollen anzeigen - Benutzern Rollen zuordnen - Benutzern Berechtigungen zuordnen - Benutzergruppen Rollen zuordnen - Benutzergruppen Berechtigungen zuordnen - Lizenzen hinzufügen - TDM-Repository einrichten - PowerCenter-Repository einrichten - Vertraulichkeitsstufen für Datendomänen festlegen - Benutzerdefinierte Projekt-Attribute festlegen - Arbeitsablaufgenerierungsattribute festlegen - Daten-Profiling aktivieren - Profiling-Dienste einrichten - Verwaltungsobjekte anzeigen - Optionen für die Indizierung der Schlüsselbegriffssuche konfigurieren
Verbindungen anzeigen	-	Lesen	Benutzer können die folgenden Aktionen auf der Seite „Verbindungen“ im Test Data Manager durchführen: - Verbindungen anzeigen - Verbindungen testen
Verbindungen verwalten	Verbindungen anzeigen	Schreiben	Benutzer können die folgenden Aktionen auf der Seite „Verbindungen“ im Test Data Manager durchführen: - Verbindungen erstellen. - Verbindungen bearbeiten - Verbindungen löschen - Verbindungen anzeigen - Verbindungen testen

Berechtigungsgruppe für Verbindungen

Die Berechtigungen in der Berechtigungsgruppe für Verbindungen bestimmen die Aufgaben, die Benutzer auf der Verbindungsseite in der TDM Workbench ausführen können. Die folgende Tabelle enthält eine Liste der

Berechtigungen in der Berechtigungsgruppe für Verbindungen und die für die Ausführung einer Aufgabe an einem Objekt erforderlichen Berechtigungen:

Berechtigung	Beinhaltet Berechtigungen	Berechtigung	Beschreibung
Verbindungen anzeigen	-	Lesen	Benutzer können Verbindungen anzeigen und in der TDM Workbench testen.
Verbindungen verwalten	Verbindungen anzeigen	Schreiben	Benutzer können die folgenden Aktionen auf der Seite „Verbindungen“ in der TDM Workbench durchführen: - Verbindungen erstellen. - Verbindungen bearbeiten - Verbindungen löschen - Verbindungen anzeigen - Verbindungen testen

Datendomänen-Berechtigungsgruppe

Die Berechtigungen in der Datendomänen-Berechtigungsgruppe bestimmen die Aufgaben, die Benutzer auf Datendomänen auf der Seite „Richtlinien“ des Test Data Manager durchführen können.

Die folgende Tabelle enthält eine Liste der Berechtigungen in der Datendomänen-Berechtigungsgruppe und die für die Ausführung einer Aufgabe an einem Objekt erforderlichen Berechtigungen.

Berechtigung	Beinhaltet Berechtigungen	Berechtigung	Beschreibung
Datendomänen anzeigen	-	Lesen	Benutzer können Datendomänen im Test Data Manager anzeigen.
Datendomänen verwalten	Datendomänen anzeigen	Schreiben	Benutzer können die folgenden Aktionen für Datendomänen im Test Data Manager durchführen: - Datendomänen erstellen - Datendomänen bearbeiten - Datendomänen löschen - Datendomänen anzeigen

Berechtigungsgruppe für Datenmaskierung

Die Berechtigungen in der Berechtigungsgruppe für Datenmaskierung bestimmen die Aufgaben, die Benutzer in der Ansicht Projekt | Definieren | Datenmaskierung des Test Data Manager durchführen können. In dieser Ansicht können Sie Tabellenspalten Regeln und Richtlinien zuweisen.

Die folgende Tabelle enthält eine Liste der Berechtigungen in der Berechtigungsgruppe für Datenmaskierung und die für die Ausführung einer Aufgabe an einem Objekt erforderlichen Berechtigungen.

Berechtigung	Beinhaltet Berechtigungen	Berechtigung	Beschreibung
Datenmaskierung anzeigen	-	Lesen	Benutzer können Datenmaskierungszuweisungen im Test Data Manager anzeigen.
Datenmaskierung verwalten	Datenmaskierung anzeigen	Schreiben	Benutzer können die folgenden Aktionen für Datenmaskierungszuweisungen im Test Data Manager durchführen: - Regel- und Richtlinienzuweisungen hinzufügen - Regel- und Richtlinienzuweisungen löschen - Regeleigenschaften überschreiben - Datenmaskierungszuweisungen anzeigen

Data Subset-Berechtigungsgruppe

Die Berechtigungen in der Datenteilmengen-Berechtigungsgruppe bestimmen die Aufgaben, die Benutzer an Datenteilmengenobjekten im Test Data Manager durchführen können.

Die folgende Tabelle enthält eine Liste der Berechtigungen in der Data Subset-Berechtigungsgruppe und die für die Ausführung einer Aufgabe an einem Objekt erforderlichen Berechtigungen.

Berechtigung	Beinhaltet Berechtigungen	Berechtigung	Beschreibung
Datenteilmenge anzeigen	-	Lesen	Benutzer können die folgenden Datenteilmengenaktionen im Test Data Manager durchführen: - Gruppen anzeigen - Vorlagen anzeigen - Entitäten anzeigen - Neuere Projektobjekte anzeigen.
Datenteilmenge verwalten	Datenteilmenge anzeigen	Schreiben	Benutzer können die folgenden Datenteilmengenaktionen im Test Data Manager durchführen: - Gruppen erstellen - Gruppen bearbeiten - Gruppen löschen - Gruppenparameter hinzufügen - Vorlagen erstellen - Vorlagen bearbeiten - Vorlagen löschen - Vorlagenparameter hinzufügen - Entität erstellen - Entität bearbeiten - Entität löschen - Entitätskriterien hinzufügen - Beziehungen aktivieren - Beziehungen deaktivieren - Beziehungen bearbeiten - Änderungen überprüfen und bearbeiten - Änderungsüberprüfung als abgeschlossen markieren

Richtlinien-Berechtigungsgruppe

Die Berechtigungen in der Richtlinien-Berechtigungsgruppe bestimmen die Aufgaben, die Benutzer an Richtlinien im Test Data Manager durchführen können.

Die folgende Tabelle enthält eine Liste der Berechtigungen in der Richtlinien-Berechtigungsgruppe und die für die Ausführung einer Aufgabe an einem Objekt erforderlichen Berechtigungen.

Berechtigung	Beinhaltet Berechtigungen	Berechtigung	Beschreibung
Richtlinien anzeigen	-	Lesen	Benutzer können Richtlinien im Test Data Manager anzeigen.
Richtlinien verwalten	Richtlinien anzeigen	Schreiben	Benutzer können die folgenden Richtlinienaktionen im Test Data Manager durchführen: - Richtlinien erstellen - Richtlinien bearbeiten - Richtlinien löschen - Richtlinien anzeigen

Berechtigungsgruppe für Projekte

Die Berechtigungen in der Berechtigungsgruppe für Projekte bestimmen die Aufgaben, die Benutzer an Projekten im Test Data Manager durchführen können.

Die folgende Tabelle enthält eine Liste der Berechtigungen in der Berechtigungsgruppe für Projekte und die für die Ausführung einer Aufgabe an einem Objekt erforderlichen Berechtigungen.

Berechtigung	Beinhaltet Berechtigungen	Berechtigung	Beschreibung
Projekt anzeigen	-	Lesen	Benutzer können die folgenden Aktionen für Projekte im Test Data Manager durchführen: - Projekte anzeigen - Pläne anzeigen - Plandetailberichte anzeigen - Planauditberichte anzeigen - Neue Projekte anzeigen
Projekt verwalten	Projekt anzeigen	Schreiben	Benutzer können die folgenden Aktionen für Projekte im Test Data Manager durchführen: - Projekte erstellen - Projekte bearbeiten - Projekte löschen - Projekte anzeigen - Benutzer zu Projekten zuordnen - Benutzergruppen zu Projekten zuordnen - Regeln zu Projekten zuordnen oder entfernen - Richtlinien zu Projekten zuordnen oder entfernen - Pläne erstellen - Pläne bearbeiten - Pläne löschen - Pläne generieren

Berechtigung	Beinhaltet Berechtigungen	Berechtigung	Beschreibung
Projekt ermitteln	-	Schreiben	Benutzer können die folgenden Ermittlungsaktionen für Projekte im Test Data Manager durchführen: - Tabellen klassifizieren - Ermittlung als abgeschlossen markieren - Datendomänen zu Spalten zuordnen - Spalten als eingeschränkt markieren - Spalten als vertraulich markieren - Spalte mit ähnlichen Werten festlegen - Spalte mit ähnlichen Werten entfernen - Primärschlüssel hinzufügen - Primärschlüssel entfernen - Logische Beschränkungen erstellen - Logische Beschränkungen anzeigen - Logische Beschränkungen bearbeiten - Logische Beschränkungen löschen - Projekte anzeigen - Profilierte Datendomänen anzeigen - Profildatendomänen genehmigen oder ablehnen - Datendomänenklassifizierung als abgeschlossen markieren - Profilierte Primärschlüssel anzeigen - Profilierte Primärschlüssel genehmigen oder ablehnen - Primärschlüsselermittlung als abgeschlossen markieren - Profilierte Entitäten anzeigen - Profilierte Entitäten genehmigen oder ablehnen - Entitätsermittlung als abgeschlossen markieren - Projektrisikoanalyse anzeigen - Letzte Verteilung empfindlicher Daten im Projekt anzeigen
Projekt generieren	-	Schreiben	Benutzer können Arbeitsabläufe im Test Data Manager generieren.
Projekt ausführen	-	Schreiben	Benutzer können die folgenden Ausführungsaktionen für Projekte im Test Data Manager durchführen: - Pläne ausführen - Arbeitsabläufe ausführen - Arbeitsabläufe anhalten - Arbeitsabläufe abbrechen - Arbeitsabläufe wiederherstellen - Planausführung anzeigen
Projekt überwachen	-	Lesen	Benutzer können die folgenden Überwachungsaktionen für Projekte im Test Data Manager durchführen: - Projekt-Jobs überwachen - Projekt-Job-Protokolle anzeigen - Jobs in verschiedenen Projekten überwachen - Job-Protokolle in verschiedenen Projekten anzeigen
Projekt prüfen	-	Lesen	Benutzer können letzte Aktivitäten bei Projekten und Plänen im Test Data Manager anzeigen.
Metadaten importieren	-	Schreiben	Benutzer können die folgenden Aktionen für Projekte im Test Data Manager durchführen: - Quellen importieren - Quellen löschen

Hinweis: Ein Benutzer mit Berechtigungen zum Verwalten von Projekten muss über mindestens die folgenden Ebenen von Berechtigungen verfügen, um einen Plan mit jeder Komponente zu erstellen.

- Verbindung aus der Administrations-Berechtigungsgruppe anzeigen. Zum Erstellen eines Plans.
- Datenteilmenge aus der Berechtigungsgruppe für Datenteilmenge anzeigen. Zum Erstellen eines Plans mit Teilmengenkomponenten.
- Maskierungsregeln aus der Berechtigungsgruppe für Regeln anzeigen. Zum Erstellen eines Plans mit Maskierungskomponenten.
- Generierungsregeln aus der Berechtigungsgruppe für Regeln anzeigen. Zum Erstellen eines Plans mit Generierungskomponenten.

Regel-Berechtigungsgruppe

Die Berechtigungen in der Regel-Berechtigungsgruppe bestimmen die Aufgaben, die Benutzer an Regeln für die Datenmaskierung und -generierung im Test Data Manager durchführen können.

Die folgende Tabelle enthält eine Liste der Berechtigungen in der Berechtigungsgruppe für Datenmaskierung und die für die Ausführung einer Aufgabe an einem Objekt erforderlichen Berechtigungen.

Berechtigung	Beinhaltet Berechtigungen	Berechtigung	Beschreibung
Maskierungsregeln anzeigen	-	Lesen	Benutzer können Maskierungsregeln im Test Data Manager anzeigen.
Maskierungsregeln verwalten	Maskierungsregeln anzeigen	Schreiben	Benutzer können die folgenden Aktionen für Datenmaskierungsregeln im Test Data Manager durchführen: - Maskierungsregeln erstellen - Maskierungsregeln bearbeiten - Maskierungsregeln löschen - Maskierungsregeln anzeigen

Berechtigung	Beinhaltet Berechtigungen	Berechtigung	Beschreibung
Generierungsregeln anzeigen	-	Lesen	Benutzer können Generierungsregeln im Test Data Manager anzeigen.
Generierungsregeln verwalten	Generierungsregeln anzeigen	Schreiben	Benutzer können die folgenden Aktionen für Datengenerierungsregeln im Test Data Manager durchführen: - Generierungsregeln erstellen - Generierungsregeln bearbeiten - Generierungsregeln löschen - Generierungsregeln anzeigen

Berechtigungsgruppe für Datengenerierung

Die Berechtigungen in der Berechtigungsgruppe für Testdatengenerierung bestimmen die Testdatengenerierungsaufgaben, die Benutzer im Test Data Manager durchführen können.

Die folgende Tabelle enthält eine Liste der Berechtigungen in der Berechtigungsgruppe für Datengenerierung und die für die Ausführung einer Aufgabe an einem Objekt erforderlichen Berechtigungen.

Berechtigung	Beinhaltet Berechtigungen	Berechtigung	Beschreibung
Datengenerierung anzeigen	-	Lesen	Benutzer können Regelzuweisungen für die Datengenerierung im Test Data Manager anzeigen.
Datengenerierung verwalten	Datengenerierung anzeigen	Schreiben	Benutzer können die folgenden Aktionen für die Datengenerierung im Test Data Manager durchführen: - Regelzuweisungen für die Datengenerierung anzeigen - Regelzuweisungen für die Datengenerierung hinzufügen - Regelzuweisungen für die Datengenerierung löschen - Regelzuweisungen für die Datengenerierung überschreiben

Verwalten von Rollen

Eine Rolle ist eine Zusammenstellung von Berechtigungen, die Sie Benutzern und Gruppen zuordnen können. Sie können die folgenden Arten von Rollen zuordnen:

- Systemdefiniert Rollen, die Sie nicht bearbeiten oder löschen können.
- Benutzerdefiniert Rollen, die Sie erstellen, bearbeiten und löschen können.

Eine Rolle beinhaltet Berechtigungen für die Domäne oder einen Anwendungsdiensttyp. Sie ordnen Benutzern und Gruppen für die Domäne und für jeden Anwendungsdienst in der Domäne Rollen zu. Beispielsweise können Sie eine Rolle „Entwickler“ erstellen, die Berechtigungen für den PowerCenter-Repository-Dienst beinhaltet. Eine Domäne kann mehrere PowerCenter-Repository-Dienste beinhalten. Sie können die Entwickler-Rolle einem Benutzer für den PowerCenter-Repository-Dienst „Entwicklung“ zuweisen. Sie können dem Benutzer eine andere Rolle für den PowerCenter-Repository-Dienst „Produktion“ zuweisen.

Eine Rolle beinhaltet Berechtigungen für die Domäne oder einen Anwendungsdiensttyp. Sie ordnen Benutzern und Gruppen für die Domäne und für jeden Anwendungsdienst in der Domäne Rollen zu.

Eine Rolle beinhaltet Berechtigungen für die Domäne oder einen Anwendungsdiensttyp. Sie ordnen Benutzern und Gruppen für die Domäne und für jeden Anwendungsdienst in der Domäne Rollen zu.

UMSM hat die folgenden Rollentypen:

- Administrator. Dies ist eine systemdefinierte Rolle mit Berechtigungen zum Verwalten des Administrator-Tools. Mit dieser Rolle können Sie Benutzerkonten erstellen und verwalten, den Ultra Messaging-Dienst erstellen und konfigurieren, UMSM-Komponenten und UM-Bereitstellungen konfigurieren.
- Operator. Dies ist eine benutzerdefinierte Rolle mit Berechtigungen zum Überwachen von UM-Bereitstellungen.

Wenn Sie im Abschnitt "Rollen" im Navigator eine Rolle auswählen, können Sie alle Benutzer und Gruppen anzeigen, denen die Rolle für die Domäne und die Anwendungsdienste direkt zugeordnet ist. Die Rollenzuweisungen können nach Benutzern und Gruppen oder nach Diensten angezeigt werden. Um zu einem Benutzer oder einer Gruppe im Zuweisungsbereich zu navigieren, klicken Sie mit der rechten Maustaste auf den Benutzer oder die Gruppe und wählen "Zu Eintrag navigieren" aus.

Sie können nach systemdefinierten und benutzerdefinierten Rollen suchen.

Systemdefinierte Rollen

Eine systemdefinierte Rolle lässt sich nicht bearbeiten oder löschen. Die Rolle des Administrators ist beispielsweise eine systemdefinierte Rolle.

Wenn Sie die Administratorrolle einem Benutzer oder einer Gruppe für die Domäne, den Analyst Service, Data Integration Service, Metadata Manager Service, Modellrepository-Dienst, PowerCenter Repository Service oder Reporting Service zuweisen, erhält dieser Benutzer bzw. diese Gruppe alle Berechtigungen für den Dienst. Die Administratorrolle umgeht die Berechtigungsprüfung. Benutzer mit der Administratorrolle können auf alle Objekte zugreifen, die vom Dienst verwaltet werden.

Wenn Sie die Administratorrolle einem Benutzer oder einer Gruppe für die Domäne, den Data Integration Service oder den Modellrepository-Dienst zuweisen, erhält dieser Benutzer bzw. diese Gruppe alle Berechtigungen für den Dienst. Die Administratorrolle umgeht die Berechtigungsprüfung. Benutzer mit der Administratorrolle können auf alle Objekte zugreifen, die vom Dienst verwaltet werden.

Wenn Sie die Administratorrolle einem Benutzer oder einer Gruppe für die Domäne oder den Ultra Messaging-Dienst zuweisen, erhält dieser Benutzer bzw. diese Gruppe alle Berechtigungen für den Dienst. Die Administratorrolle umgeht die Berechtigungsprüfung. Benutzer mit der Administratorrolle können auf alle Objekte zugreifen, die vom Dienst verwaltet werden.

Administratorrolle

Wenn Sie einem Benutzer oder einer Gruppe die Administratorrolle für die Domäne, den Datenintegrationsdienst oder den PowerCenter-Repository-Dienst zuweisen, kann der Benutzer oder die Gruppe verschiedene Aufgaben ausführen, die der Administratorrolle anstatt Rechten oder Berechtigungen unterliegen.

Wenn Sie einem Benutzer oder einer Gruppe die Administratorrolle für die Domäne oder den Datenintegrationsdienst zuweisen, kann der Benutzer oder die Gruppe verschiedene Aufgaben ausführen, die der Administratorrolle und nicht Berechtigungen unterliegen.

Wenn Sie einem Benutzer oder einer Gruppe die Administratorrolle für die Domäne oder den Ultra Messaging-Dienst zuweisen, kann der Benutzer oder die Gruppe verschiedene Aufgaben ausführen, die der Administratorrolle und nicht Berechtigungen unterliegen.

Sie können einem Benutzer oder einer Gruppe alle Berechtigungen für die Domäne, den Datenintegrationsdienst oder den PowerCenter-Repository-Dienst zuweisen und dem Benutzer oder der Gruppe dann volle Berechtigungen für alle Domänen- oder Repository-Objekte gewähren. Der Benutzer oder die Gruppe kann jedoch die der Administratorrolle unterliegenden Aufgaben nicht ausführen.

Sie können einem Benutzer oder einer Gruppe alle Berechtigungen für die Domäne oder den Datenintegrationsdienst zuweisen und dem Benutzer oder der Gruppe anschließend Vollzugriff auf alle Domänenobjekte gewähren. Der Benutzer oder die Gruppe kann jedoch die der Administratorrolle unterliegenden Aufgaben nicht ausführen.

Sie können einem Benutzer oder einer Gruppe alle Berechtigungen für die Domäne oder den Ultra Messaging-Dienst zuweisen und dem Benutzer oder der Gruppe anschließend Vollzugriff auf alle Domänenobjekte gewähren. Der Benutzer oder die Gruppe kann jedoch die der Administratorrolle unterliegenden Aufgaben nicht ausführen.

Zum Beispiel kann ein Benutzer mit Administratorrolle für die Domäne Domäneneigenschaften im Administrator-Tool konfigurieren. Ein Benutzer, der über alle Rechte und Berechtigungen für die Domäne verfügt, kann hingegen keine Domäneneigenschaften konfigurieren.

Die folgende Tabelle enthält eine Liste der Aufgaben, welche die Administratorrolle für die Domäne, den Datenintegrationsdienst und den PowerCenter-Repository-Dienst erfordern:

In der folgenden Tabelle werden die von der Administratorrolle für die Domäne oder den Datenintegrationsdienst festgelegten Aufgaben aufgelistet:

In der folgenden Tabelle werden die von der Administratorrolle für die Domäne oder den Ultra Messaging-Dienst festgelegten Aufgaben aufgelistet:

Dienst	Aufgaben
Domäne	- Konfigurieren von Domäneneigenschaften. - Betriebssystemprofile erstellen. - Löschen der Betriebssystemprofile. - Gewähren der Berechtigung für die Domänen- und Betriebssystemprofile. - Verwalten und Bereinigen von Protokollereignissen. - Empfangen von Domänenwarnungen. - Ausführen des Lizenzberichts. - Anzeigen von Protokollereignissen zur Benutzeraktivität. - Herunterfahren der Domäne. - Zugreifen auf den Upgrade-Assistenten für Dienste.
Datenintegrationsdienst	- Upgraden des Datenintegrationsdienstes mit dem Menü Aktionen.
PowerCenter-Repository-Dienst	- Zuweisen von Betriebssystemprofilen zu Repository-Ordnern, wenn der PowerCenter-Integrationsdienst Betriebssystemprofile nutzt.* - Ändern des Eigentümers von Ordnern und globalen Objekten.* - Konfigurieren der Berechtigungen für Ordner und globale Objekte.* - Verbinden mit dem PowerCenter-Integrationsdienst vom PowerCenter-Client aus beim Ausführen des PowerCenter-Integrationsdienstes im sicheren Modus. - Löschen eines PowerCenter-Integrationsdienstes vom Navigator des Workflow Managers aus. - Löschen von Ordnern und globalen Objekten.* - Benennen des gemeinsam zu verwendenden Ordners.* - Bearbeiten des Namens und der Beschreibung von Ordnern.* *Diese Aufgaben kann auch der Eigentümer des PowerCenter-Repository-Ordners oder der globale Objekteigentümer ausführen.

Dienst	Aufgaben
Domäne	- Konfigurieren von Domäneneigenschaften. - Erteilen der Berechtigung für die Domäne - Verwalten und Bereinigen von Protokollereignissen. - Empfangen von Domänenwarnungen. - Anzeigen von Protokollereignissen zur Benutzeraktivität.

Dienst	Aufgaben
Domäne	- Konfigurieren von Domäneneigenschaften. - Erteilen der Berechtigung für die Domäne - Verwalten und Bereinigen von Protokollereignissen. - Empfangen von Domänenwarnungen. - Anzeigen von Protokollereignissen zur Benutzeraktivität.

Benutzerdefinierte Rollen

Eine benutzerdefinierte Rolle lässt sich erstellen, bearbeiten und löschen. Das Administrator Tool enthält benutzerdefinierte Rollen für den Metadata Manager Service, den PowerCenter Repository Service und den Reporting Service. Sie können die Berechtigungen bearbeiten, die zu diesen Rollen gehören, und die Rollen den Benutzern und Gruppen zuweisen.

Alternativ können Sie benutzerdefinierte Rollen erstellen und diese Rollen den Benutzern und Gruppen zuweisen.

Benutzerdefinierte Rollen verwalten

Sie können die benutzerdefinierten Rollen erstellen, bearbeiten und löschen.

Erstellen von benutzerdefinierten Rollen

Beim Erstellen einer benutzerdefinierten Rolle weisen Sie der Rolle Berechtigungen für die Domäne oder für einen Anwendungsdiensttyp zu. Eine Rolle kann Berechtigungen für einen oder mehrere Dienste enthalten.

1. Klicken Sie im Administrator-Tool auf die Registerkarte „Sicherheit“.
2. Klicken Sie im Menü „Sicherheitsaktionen“ auf „Rolle erstellen“.

   Das Dialogfeld Rolle erstellen wird eingeblendet.
3. Geben Sie folgende Eigenschaften für die Rolle ein:

Eigenschaft	Beschreibung
Name	Name der Rolle. Beim Rollennamen ist Groß- und Kleinschreibung zu beachten. Maximal sind 128 Zeichen zulässig. Er darf weder einen Tabulator oder 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.
Beschreibung	Rollenbeschreibung. Die Beschreibung darf nicht mehr als 765 Zeichen, keinen Tabulator, kein Zeilenende-Zeichen und keines der folgenden Sonderzeichen enthalten: < > "

4. Klicken Sie auf die Registerkarte „Berechtigungen“.
5. Erweitern Sie die Domäne oder einen Anwendungsdiensttyp.
6. Wählen Sie die Berechtigungen, die Sie der Rolle für die Domäne oder den Anwendungsdiensttyp zuweisen möchten.
7. Klicken Sie auf „OK“.

Eigenschaften für benutzerdefinierte Rollen bearbeiten

Wenn Sie eine benutzerdefinierte Rolle bearbeiten, können Sie die Beschreibung der Rolle ändern. Sie können den Namen der Rolle nicht ändern.

1. Klicken Sie im Administrator Tool auf die Registerkarte Sicherheit.
2. Im Abschnitt Rollen des Navigator, wählen Sie eine Rolle.
3. Klicken Sie auf Bearbeiten.
4. Ändern Sie die Beschreibung der Rolle und klicken Sie auf OK.

Bearbeiten der benutzerdefinierten Rollen zugewiesenen Berechtigungen

Sie können die Berechtigungen ändern, die einer benutzerdefinierten Rolle für die Domäne und für jeden Anwendungsdiensttyp zugewiesen wurden.

1. Klicken Sie im Administrator-Tool auf die Registerkarte „Sicherheit“.
2. Wählen Sie im Abschnitt „Rollen“ des Navigators eine Rolle.
3. Klicken Sie auf die Registerkarte „Berechtigungen“.
4. Klicken Sie auf „Bearbeiten“.

   Das Dialogfeld Rollen und Rechte bearbeiten wird eingeblendet.
5. Erweitern Sie die Domäne oder einen Anwendungsdiensttyp.
6. Um der Rolle die Berechtigungen zuzuweisen, wählen Sie die Berechtigungen für die Domäne oder einen Anwendungsdiensttyp aus.
7. Um die Berechtigungen von der Rolle zu entfernen, löschen Sie die Berechtigungen für die Domäne oder den Anwendungsdiensttyp.
8. Wiederholen Sie diese Schritte für jeden Diensttyp, dessen Berechtigungen Sie ändern möchten.
9. Klicken Sie auf „OK“.

Benutzerdefinierte Rollen löschen

Wenn Sie eine benutzerdefinierte Rolle löschen, werden die benutzerdefinierte Rolle und alle damit verbundenen Berechtigungen für alle Benutzer und Gruppen entfernt, die der Rolle zugewiesen sind.

Um eine benutzerdefinierte Rolle zu löschen, klicken Sie die Rolle im Abschnitt Rollen des Navigators an und wählen Sie Rolle löschen. Bestätigen Sie, dass Sie die Rolle löschen möchten.

Benutzern und Gruppen Berechtigungen und Rollen zuweisen

Sie bestimmen die Aktionen, die die Benutzer ausführen können, indem Sie folgende Zuweisungen zu Benutzern und Gruppen vornehmen:

- Berechtigungen. Eine Berechtigung bestimmt die Aktionen, die die Benutzer in Anwendungs-Clients ausführen können.
- Rollen Eine Rolle ist eine Reihe von Berechtigungen. Wen Sie einem Benutzer oder einer Gruppe eine Rolle zuweisen, weisen Sie die zu der Rolle gehörenden Berechtigungen zu.

Bitte halten Sie folgende Regeln und Richtlinien ein, wenn Sie Benutzern und Gruppen Berechtigungen zuweisen:

- Sie weisen den Benutzern und Gruppen die Berechtigungen und Rollen für die Domäne und für jeden in der Domäne laufenden Anwendungsdienst zu.

  In den folgenden Situationen können Sie Benutzern und Gruppen keine Berechtigungen und Rollen für einen Metadata Manager Service, einen PowerCenter Repository Service oder einen Reporting Service zuweisen:

  - Der Anwendungsdienst ist deaktiviert.
  - Der PowerCenter Repository Service wird im exklusiven Modus ausgeführt.

- Sie können einem Benutzer oder einer Gruppe für jeden Anwendungsdienst unterschiedliche Berechtigungen und Rollen zuweisen.
- Eine Rolle kann Berechtigungen für die Domäne und mehrere Anwendungsdiensttypen einschließen. Wenn Sie die Rolle einem Benutzer oder einer Gruppe für einen Anwendungsdienst zuweisen, erhält der Benutzer oder die Gruppe die Berechtigungen für diesen Anwendungsdiensttyp.

Beim Ändern der einem Benutzer zugewiesenen Berechtigungen oder Rollen werden die geänderten Berechtigungen oder Rollen wirksam, wenn der Benutzer sich das nächste Mal anmeldet.

Hinweis: Die dem Standard-Administratorkonto zugewiesenen Berechtigungen und Rollen können Sie nicht bearbeiten.

Geerbte Berechtigungen

Ein Benutzer oder eine Gruppe kann Berechtigungen folgender Objekte erben:

- Gruppe Wenn Sie einer Gruppe Berechtigungen zuordnen, erben alle Untergruppen und Benutzer, die zu der Gruppe gehören, die Berechtigungen.
- Rolle. Ordnen Sie einem Benutzer eine Rolle zu, erbt der Benutzer die Berechtigungen, die zu dieser Rolle gehören. Beim Zuweisen einer Rolle zu einer Gruppe erben die Gruppe und alle Untergruppen und Benutzer, die zu dieser Gruppe gehören, die zu dieser Rolle gehörenden Berechtigungen. Die Untergruppen und Benutzer erben die Rolle nicht.

Von einer Gruppe oder Rolle geerbte Berechtigungen könne Sie nicht widerrufen. Sie können einem Benutzer oder einer Gruppe weitere Berechtigungen zuweisen, die keine von einer Gruppe oder Rolle geerbten sind.

Auf der Registerkarte Berechtigungen für einen Benutzer oder eine Gruppe sehen Sie alle Rollen und Berechtigungen, die dem Benutzer oder der Gruppe für die Domäne und jeden Anwendungsdienst zugewiesen wurden. Erweitern Sie die Domäne oder den Anwendungsdienst, um die Rollen und Berechtigungen anzuzeigen, die der Domäne oder dem Dienst zugewiesen wurden. Klicken Sie auf folgende Elemente, um weitere Informationen über die zugewiesenen Rollen und Berechtigungen einzublenden:

- Name einer zugewiesenen Rolle. Zeigt die Rollendetails im Fenster Details an.
- Informationssymbol für eine zugewiesene Rolle. Darin sind alle mit dieser Rolle geerbten Berechtigungen hervorgehoben.

Berechtigungen, die von einer Rolle oder Gruppe geerbt wurden, sind mit Erbsymbol gekennzeichnet. Aus dem Tooltip für eine geerbte Berechtigung wird ersichtlich, von welcher Rolle oder Gruppe der Benutzer die Berechtigung geerbt hat.

Schritte zum Zuweisen von Berechtigungen und Rollen an Benutzer und Gruppen

Sie können Benutzern oder Gruppen auf folgende Arten Berechtigungen und Rollen zuweisen:

- Navigieren Sie zu einem Benutzer oder einer Gruppe und bearbeiten Sie die Berechtigungs- und Rollenzuweisungen.
- Ziehen Sie die Rollen mit der Maus auf einen Benutzer oder eine Gruppe.

Einem Benutzer oder einer Gruppe Berechtigungen und Rollen über die Navigation zuweisen

1. Klicken Sie im Administrator Tool auf die Registerkarte Sicherheit.
2. Wählen Sie im Navigator einen Benutzer oder eine Gruppe aus.

3. Klicken Sie auf die Registerkarte Berechtigungen.
4. Klicken Sie auf Bearbeiten.

   Das Dialogfeld Rollen und Berechtigungen bearbeiten wird eingeblendet.
5. Wenn Sie Rollen zuordnen möchten, erweitern Sie die Domäne oder einen Anwendungsdienst auf der Registerkarte Rollen.
6. Um Rollen zu gewähren, wählen Sie die dem Benutzer oder der Gruppe für die Domäne oder den Anwendungsdienst zuzuordnenden Rollen.

   Sie können eine beliebige Rolle auswählen, die Berechtigungen für die ausgewählte Domäne oder den Anwendungsdiensttyp einschließt.
7. Um Rollen zu widerrufen, löschen Sie die dem Benutzer oder der Gruppe zugeordneten Rollen.
8. Wiederholen Sie die Schritte 5 bis 7, um Rollen für einen weiteren Dienst zuzuweisen.
9. Um Berechtigungen zuzuweisen, klicken Sie auf die Registerkarte Berechtigungen.
10. Erweitern Sie die Domäne oder einen Anwendungsdienst.
11. Wenn Sie Berechtigungen zuordnen möchten, wählen Sie die Berechtigungen, die dem Benutzer oder der Gruppe für die Domäne oder den Anwendungsdienst zugeordnet werden sollen.
12. Zum Widerrufen von Berechtigungen löschen Sie die dem Benutzer oder der Gruppe zugeordneten Berechtigungen.

    Berechtigungen, die von einer Rolle oder einer Gruppe geerbt wurden, können Sie nicht widerrufen.
13. Wiederholen Sie die Schritte 10 bis 12, um Berechtigungen für einen weiteren Dienst zuzuweisen.
14. Klicken Sie auf OK.

Einem Benutzer oder einer Gruppe Rollen durch Ziehen zuweisen

1. Klicken Sie im Administrator Tool auf die Registerkarte Sicherheit.
2. Im Abschnitt Rollen des Navigators wählen Sie den Ordner, der die Rollen enthält, die Sie zuweisen möchten.
3. Im Detailbereich wählen Sie die Rolle aus, die Sie zuweisen möchten.

   Verwenden Sie die Tasten Strg oder Umsch, um mehrere Rollen gleichzeitig auszuwählen.
4. Ziehen Sie die Rollen auf einen Benutzer oder eine Gruppe in den Abschnitt "Benutzer" oder "Gruppen" im Navigator.

   Das Dialogfeld "Rollen zuweisen" wird angezeigt.
5. Wählen Sie die Domäne oder den Anwendungsdienst aus, der oder dem Sie Rollen zuweisen möchten.
6. Klicken Sie auf OK.

Benutzer mit Berechtigungen für einen Dienst anzeigen

Sie können alle Benutzer anzeigen, die über Berechtigungen für die Domäne oder einen Anwendungsdienst verfügen.

1. Klicken Sie im Administrator-Tool auf die Registerkarte "Sicherheit".
2. Klicken Sie im Menü "Sicherheitsaktionen" auf "Dienstbenutzerberechtigungen".

Das Dialogfeld Dienste erscheint.

3. Wählen Sie die Domäne oder einen Anwendungsdienst aus.

   Der Detailbereich listet alle Benutzer, die Berechtigungen für die Domäne oder einen Anwendungsdienst haben, auf.

4. Klicken Sie mit der rechten Maustaste auf einen Benutzernamen und klicken Sie dann auf "Zu Eintrag navigieren", um zu diesem Benutzer zu gelangen.

Fehlerbehebung bei Berechtigungen und Rollen

Ich kann Benutzern keine Berechtigungen oder Rollen für einen vorhandenen Metadata Manager-Dienst, PowerCenter-Repository-Dienst oder Berichterstellungsdienst zuweisen.

Sie können Benutzern in den folgenden Situationen keine Berechtigungen oder Rollen für einen vorhandenen Metadata Manager-Dienst, PowerCenter-Repository-Dienst oder Berichterstellungsdienst zuweisen:

- Der Anwendungsdienst ist deaktiviert.
- Der PowerCenter-Repository-Dienst wird im exklusiven Modus ausgeführt.

Ich kann einem Benutzer keine Berichtigungen für einen aktivierten Berichterstellungsdienst zuweisen.

Data Analyzer bestimmt anhand des Benutzerkontonamens und des Sicherheitsdomänennamens im Format `UserName@SecurityDomain` die Länge des Benutzeranmeldenamens. Sie können einem Benutzer keine Berechtigungen oder Rollen für den Berichterstellungsdienst zuweisen, wenn die Kombination von Benutzername, @-Zeichen und Sicherheitsdomäne mehr als 128 Zeichen enthält.

Ich habe eine Berechtigung von einer Gruppe entfernt. Warum haben manche Benutzer in der Gruppe diese Berechtigung noch immer?

Zur Zuordnung Berechtigungen für einen Benutzer können Sie eine der folgenden Methoden verwenden:

- Weisen Sie einem Benutzer direkt eine Berechtigung zu.
- Weisen Sie einem Benutzer eine Rolle zu.
- Weisen Sie einer Gruppe, zu der der Benutzer gehört, eine Berechtigung oder Rolle zu.

Wenn Sie eine Berechtigung von einer Gruppe entfernen, können Benutzern, die zu dieser Gruppe gehören, Berechtigungen direkt zugewiesen werden, oder die Benutzer können die Berechtigungen von einer zugewiesenen Rolle erben.

Mir sind alle Domänenberechtigungen und Berechtigungen für alle Domänenobjekte zugewiesen, aber ich kann nicht alle Aufgaben im Administrator-Tool ausführen.

Einige der Aufgaben im Administrator-Tool werden von der Administrator-Rolle bestimmt, nicht durch Berechtigungen. Ihnen können alle Berechtigungen für die Domäne zugewiesen sein und Ihnen können volle Berechtigungen für alle Domänenobjekte gewährt sein. Sie können jedoch nicht die Aufgaben ausführen, die durch die Administrator-Rolle bestimmt sind.

Mir ist die Administrator-Rolle für einen Anwendungsdienst zugewiesen, aber ich kann den Anwendungsdienst im Administrator-Tool nicht konfigurieren.

Wenn Sie über die Administrator-Rolle für einen Anwendungsdienst verfügen, sind Sie ein Anwendungs-Client-Administrator. Ein Anwendungs-Client Administrator hat volle Berechtigungen und in einem Anwendungs-Client.

Allerdings verfügt ein Anwendungs-Client-Administrator nicht über die erforderlichen Berechtigungen in der Informatica-Domäne. Ein Anwendungs-Client-Administrator kann sich nicht beim Administrator-Tool anmelden, um den Dienst für den Anwendungs-Client zu verwalten, für den er über Administratorrechte verfügt.

Um einen Anwendungsdienst im Administrator-Tool zu verwalten, benötigen Sie die entsprechenden Domänenberechtigungen.

Mir ist die Administrator-Rolle für den PowerCenter-Repository-Dienst zugewiesen, aber ich kann den Repository Manager nicht nutzen, um eine erweiterte Bereinigung von Objekten durchzuführen oder wiederverwendbare Metadaten-Erweiterungen zu erstellen.

Sie müssen über die Domänenberechtigungen zum Verwalten von Diensten und Berechtigungen für den PowerCenter-Repository-Dienst im Administrator-Tool verfügen, um die folgenden Aktionen im Repository Manager durchführen zu können:

- Erweiterte Bereinigung von Objektversionen auf PowerCenter-Repository-Ebene durchführen.
- Wiederverwendbare Metadaten-Erweiterungen erstellen, bearbeiten und löschen.

Meine Berechtigungen zeigen, dass ich in der Lage sein sollte, Objekte in einem Anwendungs-Client zu bearbeiten, aber ich kann keine Metadaten bearbeiten.

Sie verfügen möglicherweise nicht über die erforderlichen Objektberechtigungen im Anwendungs-Client. Selbst wenn Sie Berechtigungen zur Ausführung bestimmter Aktionen haben, benötigen Sie eventuell Berechtigungen zur Durchführung der Aktion bei einem bestimmten Objekt.

Ich kann mit „pmrep“ keine Verbindung zu einem neuen PowerCenter-Repository-Dienst herstellen, der im exklusiven Modus ausgeführt wird.

Der Dienstmanager hat die Liste der Benutzer und Gruppen im PowerCenter-Repository möglicherweise nicht mit der Liste in der Domänenkonfigurations-Datenbank synchronisiert. Um die Liste der Benutzer und Gruppen zu synchronisieren, starten Sie den PowerCenter-Repository-Dienst.

Mir sind alle Berechtigungen in der Berechtigungsgruppe „Ordner“ für den PowerCenter-Repository-Dienst zugewiesen und ich habe Lese-, Schreib- und Ausführungsrechte für einen Ordner. Allerdings kann ich die Berechtigungen für den Ordner nicht konfigurieren.

Nur der Eigentümer des Ordners oder ein Benutzer, dem die Administrator-Rolle für den PowerCenter-Repository-Dienst zugewiesen ist, kann die folgenden Ordnerverwaltungsaufgaben ausführen:

- Betriebssystemprofile zu Ordnern zuweisen, wenn der PowerCenter-Integrationsdienst Betriebssystemprofile verwendet. Hierzu sind Berechtigungen für das Betriebssystemprofil erforderlich.
- Ordnereigentümer ändern.
- Ordnerberechtigungen ändern.
- Ordner löschen.
- Ordner freigeben.
- Ordnernamen und -beschreibung bearbeiten.

Mir wurde die Administratorrolle für den Metadata Manager-Dienst zugewiesen, aber ich kann das Metadata Manager-Repository weder erstellen noch wiederherstellen.

Zum Erstellen oder Wiederherstellen von Metadata Manager-Repository-Inhalt müssen Sie zur Standardgruppe „Administrator“ gehören. Benutzer in der Standardgruppe „Administrator“ haben mehr Rechte als Benutzer, denen die Administratorrolle für einen Anwendungsdienst zugewiesen wurde.

Mir wurde die Berechtigung „Ressourcen laden“ für den Metadata Manager-Dienst zugewiesen, ich erhalte jedoch eine Fehlermeldung mit dem Hinweis auf unzureichende Berechtigungen beim Versuch, Business Glossary-Ressourcen zu laden.

Zum Laden von Business Glossary-Ressourcen sind die Berechtigungen „Ressource laden“, „Ressource verwalten“ und „Modell anzeigen“ erforderlich. Sie benötigen weiterhin Schreibrechte für alle Business Glossary-Ressourcen, die geladen werden sollen.

KAPITEL 9

Berechtigungen

Dieses Kapitel umfasst die folgenden Themen:

Berechtigungen - Übersicht

Sie verwalten die Benutzersicherheit mithilfe von Berechtigungen. Mit Berechtigungen wird die Zugriffsebene von Benutzern und Gruppen für ein Domänenobjekt festgelegt.

Auch wenn ein Benutzer über die Berechtigung zur Durchführung bestimmter Aktionen verfügt, benötigt er ggf. eine Berechtigung zum Durchführen der Aktion für ein bestimmtes Objekt.

Zum Beispiel: Ein Benutzer verfügt über die Domänenberechtigung "Dienste verwalten" und die Berechtigung für den Development Repository Service, aber nicht für den Production Repository Service. Der Benutzer kann den Development Repository Service bearbeiten oder entfernen, aber nicht den Produktion Repository Service. Zur Verwaltung eines Applikation Service muss ein Benutzer über die Domänenberechtigung "Dienste verwalten" und Berechtigung für den Anwendungsdienst verfügen.

Sie verwenden verschiedene Tools, um Berechtigungen für die folgenden Objekte zu konfigurieren:

Sie verwenden verschiedene Tools, um Berechtigungen für die folgenden Objekte zu konfigurieren:

Objekttyp	Tool	Beschreibung
Verbindungsobjekte	Administrator-Tool Analyst-Tool Developer-Tool	Sie können Berechtigungen für Verbindungen zuweisen, die im Administrator-Tool, Analyst-Tool oder Developer-Tool definiert sind. Diese Tools nutzen die Verbindungsberechtigungen gemeinsam.
Data Analyzer-Objekte	Data Analyzer	Sie können Berechtigungen für Data Analyzer Ordner, Berichte, Dashboards, Attribute, Metriken, Vorlagendimensionen und Zeitpläne zuweisen.
Domänenobjekte	Administrator-Tool	Sie können Berechtigungen für die folgenden Domänenobjekte zuweisen: Domäne, Ordner, Knoten, Gitter, Lizenzen, Anwendungsdienste und Betriebssystemprofile.

Objekttyp	Tool	Beschreibung
Metadata Manager-Katalogobjekte	Metadata Manager	Sie können Berechtigungen für Metadata Manager-Ordner und -Katalogobjekte zuweisen.
Modellrepository-Projekte	Analyst-Tool Developer-Tool	Sie können Berechtigungen für Projekte zuweisen, die im Analyst-Tool oder Developer-Tool definiert sind. Diese Tools nutzen die Projektberechtigungen gemeinsam.
PowerCenter Repository-Objekte	PowerCenter-Client	Sie können Berechtigungen für PowerCenter-Ordner, -Bereitstellungsgruppen, -Beschriftungen, -Abfragen und -Verbindungsobjekte zuweisen.
SQL-Datendienstobjekte	Administrator-Tool	Sie können Berechtigungen für SQL-Datenobjekte zuweisen, wie z. B. SQL-Datendienste, virtuelle Schemas, virtuelle Tabellen und virtuelle gespeicherte Prozeduren.
Webdienstobjekte	Administrator-Tool	Sie können Berechtigungen für Webdienste oder Webdienstoperationen zuweisen.
Verbindungsobjekte	Administrator-Tool Developer-Tool	Sie können Berechtigungen für Verbindungen zuweisen, die im Administrator-Tool oder Developer-Tool definiert sind. Diese Tools nutzen die Verbindungsberechtigungen gemeinsam.
Domänenobjekte	Administrator-Tool	Sie können Berechtigungen für die folgenden Domänenobjekte zuweisen: Domäne, Ordner, Knoten und Anwendungsdienste.
Modellrepository-Projekte	Developer-Tool	Sie können Berechtigungen für Projekte zuweisen, die im Developer-Tool definiert sind.

Sie können das Administrator-Tool verwenden, um Berechtigungen für ein Domänenobjekt zu konfigurieren. Sie können Berechtigungen für die folgenden Domänenobjekte zuweisen:

- Domäne
- Knoten
- Anwendungsdienste

Arten von Berechtigungen

Benutzer und Gruppen können über die folgenden Arten von Berechtigungen in einer Domäne verfügen:

Direkte Berechtigungen

Berechtigungen, die direkt einem Benutzer oder einer Gruppe zugeordnet sind. Wenn Benutzer und Gruppen über eine Berechtigung für ein Objekt verfügen, können sie administrative Aufgaben für dieses Objekt durchzuführen, wenn sie auch die entsprechenden Berechtigungen haben. Sie können direkte Berechtigungen später bearbeiten.

Geerbte Berechtigungen

Berechtigungen, die Benutzer zu erben. Wenn Benutzer eine Berechtigung für eine Domänen oder einen Ordner haben, erben sie die Berechtigung für alle Objekte in der Domäne oder dem Ordner. Wenn Gruppen eine Berechtigung für ein Domänenobjekt aufweisen, erben alle zu der Gruppe gehörenden

Untergruppen und Benutzer die Berechtigung für das Domänenobjekt. Zum Beispiel: Eine Domäne enthält einen Ordner namens Nodes, der mehrere Knoten enthält. Wenn Sie eine Gruppe Berechtigung für den Ordner zuweisen, erben alle Untergruppen und Benutzer, die zu der Gruppe gehören, die Berechtigung für den Ordner und allen Knoten in dem Ordner.

Berechtigungen, die Benutzer zu erben. Benutzer, die die Berechtigung für eine Domäne haben, erben die Berechtigung für alle Objekte in der Domäne. Wenn Gruppen eine Berechtigung für ein Domänenobjekt aufweisen, erben alle zu der Gruppe gehörenden Untergruppen und Benutzer die Berechtigung für das Domänenobjekt.

Berechtigungen, die Benutzer zu erben. Benutzer, die die Berechtigung für eine Domäne haben, erben die Berechtigung für alle Objekte in der Domäne. Wenn Gruppen eine Berechtigung für ein Domänenobjekt aufweisen, erben alle zu der Gruppe gehörenden Untergruppen und Benutzer die Berechtigung für das Domänenobjekt.

Sie können nicht vererbten Berechtigungen widerrufen. Darüber hinaus können Berechtigungen von Benutzern oder Gruppen, denen die Administratorrolle zugeordnet ist, nicht widerrufen werden. Die Administratorrolle umgeht die Berechtigungsprüfung. Benutzer mit der Administratorrolle haben Zugriff auf alle Objekte.

Sie können die vererbten Berechtigungen bei einigen Objekttypen verweigern. Wenn Sie Berechtigungen verweigern, konfigurieren Sie Ausnahmen für die Berechtigungen, die Benutzer und Gruppen bereits haben.

effektive Berechtigungen

Obermenge aller Berechnungen für einen Benutzer oder eine Gruppe. Beinhaltet direkte Berechtigungen und vererbte Berechtigungen.

Beim Anzeigen von Berechtigungsdetails können Sie den Ursprung effektiver Berechtigungen anzeigen. Berechtigungsdetails zeigen direkt einem Benutzer oder einer Gruppe zugewiesenen Berechtigungen und direkte Berechtigungen, die einer übergeordneten Gruppe zugewiesen wurden, sowie Berechtigungen, die von übergeordneten Objekten geerbt wurden. Zusätzlich wird bei den Berechtigungsdetails angezeigt, ob dem Benutzer oder der Gruppe die Administratorrolle zugewiesen ist, wodurch die Prüfung von Berechtigungen übergangen wird.

Berechtigungssuchfilter

Wenn Sie Berechtigungen zuweisen, Berechtigungsdetails anzeigen oder die Berechtigungen für einen Benutzer oder eine Gruppe bearbeiten, können Sie Suchfilter verwenden, um nach einem Benutzer oder einer Gruppe zu suchen.

Bei der Verwaltung von Berechtigungen für einen Benutzer oder eine Gruppe, können Sie folgende Suchfilter nutzen:

Sicherheitsdomäne.

Wählen Sie die Sicherheitsdomäne, um nach Benutzern oder Gruppen zu suchen.

Suchmuster-Zeichenfolge

Geben Sie eine Zeichenfolge für die Suche nach Benutzern oder Gruppen ein. Das Administrator Tool gibt alle Namen zurück, die die gesuchte Zeichenfolge enthält. Die Groß-/Kleinschreibung spielt bei der Suche keine Rolle. Zum Beispiel: Die Zeichenfolge "DA" gibt "Cardamon", "das" und "DA_AdminGroup" zurück.

Sie können die Liste der Benutzer und Gruppen auch sortieren. Klicken Sie einen Spaltennamen mit der rechten Maustaste an, um die Spalte in auf- oder absteigender Reihenfolge zu sortieren.

Domänenobjektberechtigungen

Sie haben die Möglichkeit, Rechte und Berechtigungen zur Verwaltung der Benutzersicherheit innerhalb der Domäne zu konfigurieren. Mit Berechtigungen wird die Zugriffsebene eines Benutzers für ein Domänenobjekt festgelegt. Um sich beim Administrator-Tool anmelden zu können, braucht der Benutzer die Berechtigung für mindestens ein Domänenobjekt. Hat ein Benutzer die Berechtigung für ein Objekt, jedoch nicht die Domänenberechtigung zum Ändern des Objekttyps, kann dieser Benutzer das Objekt nur anzeigen.

Hat ein Benutzer zum Beispiel die Berechtigung für einen Knoten, jedoch nicht die Berechtigung zum Verwalten von Knoten und Gittern, kann der Benutzer zwar die Knoteneigenschaften anzeigen, den Knoten jedoch nicht konfigurieren, herunterfahren oder entfernen.

Berechtigungen können Sie für folgende Typen von Domänenobjekten konfigurieren:

Domänenobjekttyp	Beschreibung der Berechtigung
Domäne	Ermöglicht Benutzern des Administrator-Tools den Zugriff auf alle Objekte in der Domäne. Benutzer, die die Berechtigung für eine Domäne haben, erben die Berechtigung für alle Objekte in der Domäne.
Ordner	Ermöglicht den Benutzern des Administrator-Tools den Zugriff auf alle Objekte im Ordner des Administrator-Tools. Haben Benutzer die Berechtigung für einen Ordner, erben sie die Berechtigung für alle Objekte in diesem Ordner.
Knoten	Ermöglicht Benutzern des Administrator-Tools die Anzeige und Bearbeitung der Knoteneigenschaften. Ohne Berechtigung kann ein Benutzer den Knoten beim Definieren eines Anwendungsdienstes oder Erstellen eines Gitters nicht verwenden.
Gitter	Ermöglicht den Benutzern des Administrator-Tools die Anzeige und Bearbeitung der Gittereigenschaften. Ohne Berechtigung kann ein Benutzer das Gitter nicht zu einem Datenintegrationsdienst oder PowerCenter-Integrationsdienst zuweisen.
Lizenz	Ermöglicht Benutzern des Administrator-Tools die Anzeige und Bearbeitung der Lizenzeigenschaften. Ohne Berechtigung kann ein Benutzer die Lizenz beim Erstellen eines Anwendungsdienstes nicht benutzen.
Anwendungsdienst	Ermöglicht Benutzern des Administrator-Tools die Anzeige und Bearbeitung der Anwendungsdiensteigenschaften.
Betriebssystemprofil	Ermöglicht den Benutzern die Ausführung von Arbeitsabläufen, die dem Betriebssystemprofil zugeordnet sind. Hat der Benutzer, der einen Arbeitsablauf ausführt, keine Berechtigung für das dem Arbeitsablauf zugeordnete Betriebssystemprofil, schlägt der Arbeitsablauf fehl.

Domänenobjekttyp	Beschreibung der Berechtigung
Domäne	Ermöglicht Benutzern des Administrator-Tools den Zugriff auf alle Objekte in der Domäne. Benutzer, die die Berechtigung für eine Domäne haben, erben die Berechtigung für alle Objekte in der Domäne.
Knoten	Ermöglicht Benutzern des Administrator-Tools die Anzeige und Bearbeitung der Knoteneigenschaften.

Domänenobjekttyp	Beschreibung der Berechtigung
Anwendungsdienst	Ermöglicht Benutzern des Administrator-Tools die Anzeige und Bearbeitung der Anwendungsdiensteigenschaften.
Lizenz	Ermöglicht Benutzern des Administrator-Tools die Anzeige und Bearbeitung der Lizenzeigenschaften.

Domänenobjekttyp	Beschreibung der Berechtigung
Domäne	Ermöglicht Benutzern des Administrator-Tools den Zugriff auf alle Objekte in der Domäne. Benutzer, die die Berechtigung für eine Domäne haben, erben die Berechtigung für alle Objekte in der Domäne.
Knoten	Ermöglicht Benutzern des Administrator-Tools die Anzeige und Bearbeitung der Knoteneigenschaften.
Anwendungsdienst	Ermöglicht Benutzern des Administrator-Tools die Anzeige und Bearbeitung der Anwendungsdiensteigenschaften.
Lizenz	Ermöglicht Benutzern des Administrator-Tools die Anzeige und Bearbeitung der Lizenzeigenschaften.

Zum Verwalten der Domänenobjektberechtigungen können Sie folgende Methoden verwenden:

- Verwalten von Berechtigungen nach Domänenobjekt. In der Ansicht Berechtigungen eines Domänenobjekts können Sie mehreren Benutzern oder Gruppen Berechtigungen zuweisen und diese bearbeiten.
- Verwalten von Berechtigungen nach Benutzer oder Gruppe. Im Dialogfeld "Berechtigungen verwalten" können Sie einem bestimmten Benutzer oder einer Gruppe Berechtigungen für Domänenobjekte zuweisen und diese bearbeiten.

Hinweis: Berechtigungen für ein Betriebssystemprofil werden anders konfiguriert als Berechtigungen für andere Domänenobjekte.

Berechtigungen per Domänenobjekt

Verwenden Sie die Ansicht **Berechtigungen** eines Domänenobjekts, um die Berechtigungen des Domänenobjekts für mehrere Benutzer oder Gruppen zu vergeben, anzuzeigen und zu bearbeiten.

Berechtigungen für ein Domänenobjekt zuweisen

Wenn Sie einem Domänenobjekt Berechtigungen zuweisen möchten, gewähren Sie den Benutzern oder Gruppen Zugriff auf das Objekt.

1. Wählen Sie die Ansicht **Dienste und Knoten** auf der Registerkarte Domäne.
2. Wählen Sie das Domänenobjekt im Navigator aus.
3. Klicken Sie im Inhaltsbereich auf die Ansicht **Berechtigungen**
4. Klicken Sie auf die Registerkarte **Gruppen** oder **Benutzer**.
5. Klicken Sie auf **Aktionen** > **Berechtigung zuweisen**.

Das Dialogfenster **Berechtigungen zuweisen** zeigt alle Benutzer und Gruppen an, die keine Berechtigung für das Objekt haben.

6. Geben Sie die Filterbedingungen zum Suchen nach Benutzern und Gruppen ein und klicken Sie auf die Schaltfläche **Filtern**.
7. Wählen Sie einen Benutzer oder eine Gruppe aus und klicken Sie auf **Weiter**.
8. Wählen Sie **Zulassen** und klicken Sie auf **Fertig stellen**.

Berechtigungsdetails zu einem Domänenobjekt anzeigen

Beim Anzeigen von Berechtigungsdetails können Sie den Ursprung effektiver Berechtigungen anzeigen.

1. Wählen Sie die Ansicht **Dienste und Knoten** auf der Registerkarte Domäne.
2. Wählen Sie das Domänenobjekt im Navigator aus.
3. Klicken Sie im Inhaltsbereich auf die Ansicht **Berechtigungen**
4. Klicken Sie auf die Registerkarte **Gruppen** oder **Benutzer**.
5. Geben Sie die Filterbedingungen zum Suchen nach Benutzern und Gruppen ein und klicken Sie auf die Schaltfläche **Filtern**.
6. Wählen Sie einen Benutzer oder eine Gruppe aus und klicken Sie auf **Aktionen** > **Berechtigungsdetails anzeigen**.

   Das Dialogfeld **Berechtigungsdetails anzeigen** erscheint. Es enthält alle direkt einem Benutzer oder einer Gruppe zugewiesenen Berechtigungen und alle direkten Berechtigungen, die einer übergeordneten Gruppe zugewiesen wurden, sowie Berechtigungen, die von übergeordneten Objekten geerbt wurden. Zusätzlich wird bei den Berechtigungsdetails angezeigt, ob dem Benutzer oder der Gruppe die Administratorrolle zugewiesen ist, wodurch die Prüfung von Berechtigungen übergangen wird.
7. Klicken Sie auf **Schließen**
8. Oder klicken Sie auf **Berechtigungen bearbeiten**, um die Berechtigungen sofort zu ändern.

Bearbeiten von Berechtigungen für ein Domänenobjekt

Sie haben die Möglichkeit, direkte Berechtigungen für ein Domänenobjekt für einen Benutzer oder eine Gruppe zu bearbeiten. Geerbte Berechtigungen oder Ihre eigenen Berechtigungen können Sie nicht widerrufen.

Hinweis: Wenn Sie direkte Berechtigungen für ein Objekt widerrufen, kann der Benutzer oder die Gruppe trotzdem Berechtigungen von einer übergeordneten Gruppe oder einem solchen Objekt erben.

1. Wählen Sie die Ansicht **Dienste und Knoten** auf der Registerkarte Domäne.
2. Wählen Sie das Domänenobjekt im Navigator aus.
3. Klicken Sie im Inhaltsbereich auf die Ansicht **Berechtigungen**
4. Klicken Sie auf die Registerkarte **Gruppen** oder **Benutzer**.
5. Geben Sie die Filterbedingungen zum Suchen nach Benutzern und Gruppen ein und klicken Sie auf die Schaltfläche **Filtern**.
6. Wählen Sie einen Benutzer oder eine Gruppe und klicken Sie auf **Aktionen** > **Direkte Berechtigungen bearbeiten**.

   Das Dialogfeld **Direkte Berechtigungen bearbeiten** wird geöffnet.
7. Um dem Objekt Berechtigungen zuzuordnen, wählen Sie **Zulassen**.
8. Um Berechtigungen für das Objekt zu widerrufen, wählen Sie **Widerrufen**.

Durch Anklicken von **Berechtigungsdetails anzeigen** können Sie anzeigen, ob die Berechtigung direkt zugeordnet oder geerbt wurde.

9. Klicken Sie auf **OK**.

Berechtigungen per Benutzern oder Gruppen

Verwenden Sie das Dialogfeld **Berechtigungen verwalten** um die Berechtigungen des Domänenobjekts für einen bestimmten Benutzer oder eine bestimmte Gruppe zu vergeben, anzuzeigen und zu bearbeiten.

Berechtigungsdetails für einen Benutzer oder eine Gruppe anzeigen

Beim Anzeigen von Berechtigungsdetails können Sie die Herkunft effektiver Berechtigungen anzeigen.

1. Klicken Sie im Kopfteil des Infomatica-Administrators auf **Verwalten** > **Berechtigungen**.

   Das Dialogfeld **Berechtigungen verwalten** wird eingeblendet.
2. Klicken Sie auf die Registerkarte **Gruppen** oder **Benutzer**.
3. Geben Sie eine Zeichenfolge ein, um die Benutzer und Gruppen zu suchen; klicken Sie dann auf die Schaltfläche **Filter**.
4. Wählen Sie einen Benutzer oder eine Gruppe aus.
5. Wählen Sie ein Domänenobjekt und klicken Sie auf die Schaltfläche **Berechtigungsdetails anzeigen**.

   Das Dialogfeld **Berechtigungsdetails anzeigen** erscheint. Es enthält alle direkt einem Benutzer oder einer Gruppe zugewiesenen Berechtigungen und alle direkten Berechtigungen, die einer übergeordneten Gruppe zugewiesen wurden, sowie Berechtigungen, die von übergeordneten Objekten geerbt wurden. Zusätzlich wird bei den Berechtigungsdetails angezeigt, ob dem Benutzer oder der Gruppe die Administratorrolle zugewiesen ist, wodurch die Prüfung von Berechtigungen übergangen wird.
6. Klicken Sie auf **Schließen**
7. Oder klicken Sie auf **Berechtigungen bearbeiten**, um die Berechtigungen sofort zu ändern.

Zuweisen und Bearbeiten von Berechtigungen für einen Benutzer oder eine Gruppe

Beim Bearbeiten von Domänen-Objektberechtigungen für einen Benutzer oder eine Gruppe können Sie Berechtigungen zuordnen und direkte Berechtigungen bearbeiten. Geerbte Berechtigungen oder Ihre eigenen Berechtigungen können Sie nicht widerrufen.

Hinweis: Wenn Sie direkte Berechtigungen für ein Objekt widerrufen, kann der Benutzer oder die Gruppe trotzdem Berechtigungen von einer übergeordneten Gruppe oder einem solchen Objekt erben.

1. Klicken Sie im Kopfteil des Infomatica-Administrators auf **Verwalten** > **Berechtigungen**.

   Das Dialogfeld **Berechtigungen verwalten** wird eingeblendet.
2. Klicken Sie auf die Registerkarte **Gruppen** oder **Benutzer**.
3. Geben Sie einen String zum Suchen nach Benutzern und Gruppen ein und klicken Sie auf die Schaltfläche **Filtern**.
4. Wählen Sie einen Benutzer oder eine Gruppe aus.
5. Wählen Sie ein Domänenobjekt und klicken Sie auf die Schaltfläche **Direkte Berechtigungen bearbeiten**.

   Das Dialogfeld **Direkte Berechtigungen bearbeiten** wird eingeblendet.
6. Um dem Objekt Berechtigungen zuzuordnen, wählen Sie **Zulassen**.
7. Um Berechtigungen für das Objekt zu widerrufen, wählen Sie **Widerrufen**.

Durch Anklicken von **Berechtigungsdetails anzeigen** können Sie anzeigen, ob die Berechtigung direkt zugeordnet oder geerbt wurde.

8. Klicken Sie auf **OK**.
9. Klicken Sie auf **Schließen**

Betriebssystemprofil-Berechtigungen

Verwenden Sie das Dialogfeld **Betriebssystemprofile konfigurieren**, um die Berechtigungen für die Betriebssystemprofile zuzuweisen, anzuzeigen und zu bearbeiten.

Berechtigungen für Betriebssystemprofile zuweisen

Wenn Sie einem Betriebssystemprofil Berechtigungen zuweisen möchten, können die Benutzer des PowerCenter Arbeitsabläufe ausführen, die dem Betriebssystemprofil zugewiesen sind.

1. Auf der Registerkarte **Sicherheit** klicken Sie auf **Aktionen** > **Betriebssystemprofile konfigurieren**.

   Das Dialogfeld **Betriebssystemprofile konfigurieren** erscheint.
2. Wählen Sie das Betriebssystemprofile aus und klicken Sie auf die Registerkarte**Berechtigungen**.
3. Wählen Sie die Ansicht **Gruppen** oder **Benutzer** aus und klicken Sie auf die Schaltfläche **Berechtigungen zuweisen**.

   Das Dialogfenster **Berechtigungen zuweisen** zeigt alle Benutzer und Gruppen an, die keine Berechtigung für das Betriebssystemprofil haben.
4. Geben Sie die Filterbedingungen zum Suchen nach Benutzern und Gruppen ein und klicken Sie auf die Schaltfläche **Filtern**.
5. Wählen Sie einen Benutzer oder eine Gruppe aus und klicken Sie auf **Weiter**.
6. Wählen Sie **Zulassen** und klicken Sie auf **Fertig stellen**.

Berechtigungsdetails zu Betriebssystemprofilen anzeigen

Beim Anzeigen von Berechtigungsdetails können Sie die Herkunft effektiver Berechtigungen anzeigen.

1. Auf der Registerkarte **Sicherheit** klicken Sie auf **Aktionen** > **Betriebssystemprofile konfigurieren**.

   Das Dialogfeld **Betriebssystemprofile konfigurieren** erscheint.
2. Wählen Sie das Betriebssystemprofile aus und klicken Sie auf die Registerkarte**Berechtigungen**.
3. Wählen Sie die Ansicht **Gruppen** oder **Benutzer**.
4. Geben Sie die Filterbedingungen zum Suchen nach Benutzern und Gruppen ein und klicken Sie auf die Schaltfläche **Filtern**.
5. Wählen Sie einen Benutzer oder eine Gruppe aus und klicken Sie auf **Aktionen** > **Berechtigungsdetails anzeigen**.

   Das Dialogfeld **Berechtigungsdetails anzeigen** erscheint. Es enthält alle direkt einem Benutzer oder einer Gruppe zugewiesenen Berechtigungen und alle direkten Berechtigungen, die einer übergeordneten Gruppe zugewiesen wurden, sowie Berechtigungen, die von übergeordneten Objekten geerbt wurden. Zusätzlich wird bei den Berechtigungsdetails angezeigt, ob dem Benutzer oder der Gruppe die Administratorrolle zugewiesen ist, wodurch die Prüfung von Berechtigungen übergangen wird.
6. Klicken Sie auf **Schließen**
7. Oder klicken Sie auf **Berechtigungen bearbeiten**, um die Berechtigungen sofort zu ändern.

Bearbeiten von Berechtigungen für ein Betriebssystemprofil

Sie haben die Möglichkeit, für einen Benutzer oder eine Gruppe direkte Berechtigungen für ein Betriebssystemprofil zu bearbeiten. Geerbte Berechtigungen oder Ihre eigenen Berechtigungen können Sie nicht widerrufen.

Hinweis: Wenn Sie direkte Berechtigungen für ein Objekt widerrufen, kann der Benutzer oder die Gruppe trotzdem Berechtigungen von einer übergeordneten Gruppe oder einem solchen Objekt erben.

1. Auf der Registerkarte **Sicherheit** klicken Sie auf **Aktionen** > **Betriebssystemprofile konfigurieren**.

   Das Dialogfeld **Betriebssystemprofile konfigurieren** erscheint.
2. Wählen Sie das Betriebssystemprofile aus und klicken Sie auf die Registerkarte**Berechtigungen**.
3. Wählen Sie die Ansicht **Gruppen** oder **Benutzer**.
4. Geben Sie die Filterbedingungen zum Suchen nach Benutzern und Gruppen ein und klicken Sie auf die Schaltfläche **Filtern**.
5. Wählen Sie einen Benutzer oder eine Gruppe und klicken Sie auf **Aktionen** > **Direkte Berechtigungen bearbeiten**.

   Das Dialogfeld **Direkte Berechtigungen bearbeiten** wird geöffnet.
6. Um Berechtigungen für das Betriebssystemprofil zuzuweisen, wählen Sie **Zulassen**.
7. Wenn Sie Berechtigungen für das Betriebssystemprofil widerrufen möchten, wählen Sie **Widerrufen**.

   Durch Anklicken von **Berechtigungsdetails anzeigen** können Sie anzeigen, ob die Berechtigung direkt zugeordnet oder geerbt wurde.
8. Klicken Sie auf **OK**.

Verbindungsberechtigungen

Mit Berechtigungen wird die Zugriffsebene eines Benutzers oder einer Gruppe auf die Verbindung festgelegt.

Sie haben die Möglichkeit, Berechtigungen für Verbindungen im Analyst-Tool, im Developer-Tool oder im Administrator-Tool zu konfigurieren.

Sie können Berechtigungen für eine Verbindung im Developer- oder im Administrator-Tool konfigurieren.

Eine Verbindungsberechtigung, die einem Benutzer oder einer Gruppe in einem Tool zugeordnet wurde, gilt ebenfalls für andere Tools. Beispiel: Sie gewähren der Gruppe A eine Berechtigung für die Verbindung A im Developer-Tool. Die Gruppe A besitzt ebenfalls die Berechtigung für die Verbindung A im Analyst-Tool und im Administrator-Tool.

Eine Verbindungsberechtigung, die einem Benutzer oder einer Gruppe in einem Tool zugeordnet wurde, gilt ebenfalls für andere Tools. Beispiel: Sie gewähren der Gruppe A eine Berechtigung für die Verbindung A im Developer-Tool. GruppeA verfügt auch über eine Berechtigung für VerbindungA im Administrator-Tool.

Folgende Informatica-Komponenten nutzen die Verbindungsberechtigungen:

- Administrator-Tool. Erzwingt, Lese-, Schreib- und Ausführungsberechtigungen für Verbindungen.
- Analyst-Tool. Erzwingt, Lese-, Schreib- und Ausführungsberechtigungen für Verbindungen.
- Informatica-Befehlszeilen-Schnittstelle. Erzwingt Lese-, Schreib- und Gewährungsberechtigungen für Verbindungen.
- Developer-Tool. Erzwingt, Lese-, Schreib- und Ausführungsberechtigungen für Verbindungen.

Bei SQL-Datendiensten erzwingt das Developer-Tool keine Verbindungsberechtigungen. Stattdessen erzwingt es Spalten- und Pass-Through-Sicherheit für die Datenzugriffsbeschränkung.

- Datenintegrationsdienst. Erzwingt Ausführungsberechtigunen, wenn ein Benutzer versucht, eine Datenvorschau anzuzeigen oder ein Mapping, eine Scorecard bzw. ein Profil auszuführen.
- Datenintegrationsdienst. Erzwingt Ausführungsberechtigungen, wenn ein Benutzer versucht, eine Datenvorschau anzuzeigen oder ein Mapping bzw. ein Profil auszuführen.

Hinweis: Für folgende Verbindungen können Sie keine Berechtigungen zuordnen: Profiling-Warehouse, Datenobjekt-Cache-Datenbank oder Modellrepository.

Berechtigungstypen für Verbindungen

Sie können Benutzern für die Ausführung folgender Aktionen verschiedene Berechtigungstypen zuweisen:

Aktion	Berechtigungstypen
Anzeigen aller Verbindungsmetadaten, ausgenommen Passwörter. Zum Beispiel: Verbindungsname, Typ, Beschreibung, Verbindungs-Strings und Benutzernamen.	Lesen
Bearbeiten aller Verbindungs-Metadaten, einschließlich Passwörter. Löschen der Verbindung. Benutzer mit Schreibrechten erben Leserechte.	Schreiben
Greifen Sie auf die physischen Daten in der zugrunde liegenden Datenquelle zu, die durch die Verbindung definiert wurden. Benutzer können eine Vorschau der Daten erhalten, ein Mapping ausführen, ein Mapping in einer Arbeitsablauf-Mappingaufgabe ausführen oder ein Profil ausführen, das diese Verbindung verwendet. Greifen Sie auf die physischen Daten in der zugrunde liegenden Datenquelle zu, die durch die Verbindung definiert wurden. Benutzer können die Daten in der Vorschau anzeigen, ein Mapping, ein Mapping in einer Arbeitsablauf-Mapping-Aufgabe oder ein Profil ausführen, das die Verbindung verwendet.	Ausführen
Berechtigungen für Verbindungen vergeben und zurücknehmen.	Gewähren

Standardverbindungsberechtigungen

Der Domänenadministrator enthält alle Berechtigungen zu allen Verbindungen. Der Benutzer, der eine Verbindung erstellt, hat Lese-, Schreib-, Ausführungs- und Zuweisungsberechtigung für diese Verbindung. Standardmäßig haben alle Benutzer die Berechtigung folgende Aktionen für Verbindungen durchzuführen:

- Anzeigen von grundlegenden Verbindungs-Metadaten, z.B. den Namen, Typ und die Beschreibung einer Verbindung.
- Verwendung der Verbindung in Mappings des Developer-Tools.
- Erstellen von Profilen im Analyst-Tool für Objekte in der Verbindung.

Berechtigungen für eine Verbindung zuweisen

Wenn Sie einer Verbindung Berechtigungen zuweisen, definieren Sie den Zugriffslevel, den ein Benutzer oder eine Gruppe für diese Verbindung bekommen soll.

1. Auf der Registerkarte Domäne, wählen Sie die Ansicht **Verbindungen** aus.
2. Wählen Sie die Verbindung im Navigator aus.
3. Klicken Sie im Inhaltsbereich auf die Ansicht **Berechtigungen**

4. Klicken Sie auf die Registerkarte **Gruppen** oder **Benutzer**.
5. Klicken Sie auf **Aktionen** > **Berechtigung zuweisen**.

   Das Dialogfenster **Berechtigungen zuweisen** zeigt alle Benutzer und Gruppen an, die keine Berechtigung für die Verbindung haben.
6. Geben Sie die Filterbedingungen zum Suchen nach Benutzern und Gruppen ein und klicken Sie auf die Schaltfläche **Filtern**.
7. Wählen Sie einen Benutzer oder eine Gruppe aus und klicken Sie auf **Weiter**.
8. Für jeden Berechtigungstyp, den Sie zuweisen möchten, wählen Sie **Zulassen**.
9. Klicken Sie auf **Fertig stellen**.

Berechtigungsdetails zu einer Verbindung anzeigen

Beim Anzeigen von Berechtigungsdetails können Sie die Herkunft effektiver Berechtigungen anzeigen.

1. Auf der Registerkarte Domäne, wählen Sie die Ansicht **Verbindungen** aus.
2. Wählen Sie die Verbindung im Navigator aus.
3. Klicken Sie im Inhaltsbereich auf die Ansicht **Berechtigungen**
4. Klicken Sie auf die Registerkarte **Gruppen** oder **Benutzer**.
5. Geben Sie die Filterbedingungen zum Suchen nach Benutzern und Gruppen ein und klicken Sie auf die Schaltfläche **Filtern**.
6. Wählen Sie einen Benutzer oder eine Gruppe aus und klicken Sie auf **Aktionen** > **Berechtigungsdetails anzeigen**.

   Das Dialogfeld **Berechtigungsdetails anzeigen** erscheint. Es enthält alle direkt einem Benutzer oder einer Gruppe zugewiesenen Berechtigungen und alle direkten Berechtigungen, die einer übergeordneten Gruppe zugewiesen werden. Zusätzlich wird bei den Berechtigungsdetails angezeigt, ob dem Benutzer oder der Gruppe die Administratorrolle zugewiesen ist, wodurch die Prüfung von Berechtigungen übergangen wird.
7. Klicken Sie auf **Schließen**
8. Oder klicken Sie auf **Berechtigungen bearbeiten**, um die Berechtigungen sofort zu ändern.

Bearbeiten von Berechtigungen für eine Verbindung

Sie haben die Möglichkeit, direkte Berechtigungen zu einer Verbindung für einen Benutzer oder eine Gruppe zu bearbeiten. Geerbte Berechtigungen oder Ihre eigenen Berechtigungen können Sie nicht widerrufen.

Hinweis: Wenn Sie direkte Berechtigungen für ein Objekt widerrufen, kann der Benutzer oder die Gruppe trotzdem Berechtigungen von einer übergeordneten Gruppe oder einem solchen Objekt erben.

1. Auf der Registerkarte Domäne, wählen Sie die Ansicht **Verbindungen** aus.
2. Wählen Sie die Verbindung im Navigator aus.
3. Klicken Sie im Inhaltsbereich auf die Ansicht **Berechtigungen**
4. Klicken Sie auf die Registerkarte **Gruppen** oder **Benutzer**.
5. Geben Sie die Filterbedingungen zum Suchen nach Benutzern und Gruppen ein und klicken Sie auf die Schaltfläche **Filtern**.
6. Wählen Sie einen Benutzer oder eine Gruppe und klicken Sie auf **Aktionen** > **Direkte Berechtigungen bearbeiten**.

   Das Dialogfeld **Direkte Berechtigungen bearbeiten** wird geöffnet.

7. Wählen Sie, ob Sie Berechtigungen erteilen oder widerrufen möchten.
   - Um eine Berechtigung zu erteilen, wählen Sie **Zulassen**.
   - Löschen Sie **Zulassen**, um eine einzelne Berechtigung zu widerrufen.
   - Mit **Widerrufen** widerrufen Sie alle Berechtigungen.

   Indem Sie auf **Berechtigungsdetails anzeigen** klicken, können Sie überprüfen, ob die Berechtigung direkt zugeordnet oder geerbt wurde.
8. Klicken Sie auf **OK**.

SQL-Datendienst-Berechtigungen

Endbenutzer können über eine JDBC- oder ODBC-Client-Tool eine Verbindung zu einem SQL-Datendienst herstellen. Nach dem Verbindungsaufbau können die Benutzer SQL-Abfragen für virtuelle Tabellen in einem SQL-Datendienst ausführen oder eine virtuelle gespeicherte Prozedur in einem SQL-Datendienst ausführen. Berechtigungen steuern die Zugriffsebene eines Benutzers auf einen SQL-Datendienst.

Berechtigungen lassen sich Benutzern und Gruppen für folgende SQL-Datendienstobjekte zuweisen:

- SQL-Datendienst
- Virtuelle Tabelle
- Virtuelle gespeicherte Prozedur

Wenn Sie einem SQL-Datendienst-Objekt eine Berechtigung zuweisen, erbt der Benutzer oder die Gruppe dieselben Berechtigungen für alle Objekte, die zu diesem SQL-Datendienst-Objekt gehören. Zum Beispiel: Sie weisen einem Benutzer eine Auswahlberechtigung für einen SQL-Datendienst zu. Der Benutzer erbt seine Auswahlberechtigung auf allen virtuellen Tabellen im SQL-Datendienst.

Sie können Berechtigungen für Benutzer und Gruppen für einige SQL-Datendienst-Objekte verweigern. Wenn Sie Berechtigungen verweigern, konfigurieren Sie Ausnahmen für die Berechtigungen, die Benutzer und Gruppen bereits haben. Beispielsweise können Sie keine Berechtigungen für eine Spalte in einer virtuellen Tabelle zuweisen, aber Sie können einem Benutzer verweigern, eine SQL-SELECT-Anweisung auszuführen, die diese Spalte enthält.

Arten von SQL-Datendienst-Berechtigungen

Sie können die folgenden Berechtigungen für Benutzer und Gruppen zuordnen:

- Berechtigung gewähren. Benutzer können Berechtigungen für SQL-Datendienstobjekte mit dem Administrator Tool oder über das *infacmd*-Befehlszeilenprogramm erteilen und entziehen.
- Ausführungsberechtigung. Benutzer können virtuelle gespeicherte Prozeduren im SQL-Datendienst mittels eines JDBC- oder ODBC-Client-Tools ausführen.
- Auswahlberechtigung. Benutzer können SQL-SELECT-Anweisungen auf virtuellen Tabellen im SQL-Datendienst über ein JDBC- oder ODBC-Client-Tool ausführen.

Einige Berechtigungen sind nicht für alle SQL-Datendienstobjekte anwendbar.

Die folgende Tabelle beschreibt die Berechtigungen für jedes SQL-Datendienstobjekt:

Objekt	Berechtigung gewähren	Ausführungsberechtigung	Auswahlberechtigung
SQL-Datendienst	Erteilen und entziehen von Berechtigung auf dem SQL-Datendienst und allen Objekten innerhalb des SQL-Datendienstes.	Alle virtuellen gespeicherten Prozeduren im SQL-Datendienst ausführen.	SQL-SELECT-Anweisungen auf allen virtuellen Tabellen im SQL-Datendienst ausführen.
Virtuelle Tabelle	Erteilen und entziehen der Berechtigung für die virtuelle Tabelle.	-	Ausführen von SQL-SELECT-Anweisungen für die virtuelle Tabelle.
Virtuelle gespeicherte Prozedur	Erteilen und entziehen der Berechtigung auf der virtuellen gespeicherten Prozedur.	Virtuelle gespeicherte Prozedur ausführen.	-

Berechtigungen für den SQL-Datendienst zuweisen

Wenn Sie Berechtigungen für ein SQL-Datendienstobjekt zuweisen, bestimmen Sie die Zugriffsebene des Benutzers oder der Gruppe zu dem Objekt.

1. Wählen Sie die Ansicht **Dienste und Knoten** auf der Registerkarte Domäne.
2. Wählen Sie im Navigator einen Data Integration Service.
3. In der Inhaltsübersicht wählen Sie die Ansicht **Anwendungen**.
4. Wählen Sie das SQL-Datendienstobjekt.
5. Wählen Sie im Fenster Details die Ansicht **Gruppenberechtigungen** oder **Benutzerberechtigungen**.
6. Klicken Sie auf die Schaltfläche **Berechtigung zuweisen**.

   Im Dialogfeld **Berechtigungen zuweisen** stehen alle Benutzer oder Gruppen, die keine Berechtigung für das SQL-Datendienstobjekt haben.
7. Geben Sie die Filterbedingungen zum Suchen nach Benutzern und Gruppen ein und klicken Sie auf die Schaltfläche **Filtern**.
8. Wählen Sie einen Benutzer oder eine Gruppe aus und klicken Sie auf **Weiter**.
9. Für jeden Berechtigungstyp, den Sie zuweisen möchten, wählen Sie **Zulassen**.
10. Klicken Sie auf **Fertig stellen**.

Berechtigungsdetails zu einem SQL-Datendienst anzeigen

Beim Anzeigen von Berechtigungsdetails können Sie den Ursprung effektiver Berechtigungen anzeigen.

1. Wählen Sie die Ansicht **Dienste und Knoten** auf der Registerkarte Domäne.
2. Wählen Sie im Navigator einen Data Integration Service.
3. In der Inhaltsübersicht wählen Sie die Ansicht **Anwendungen**.
4. Wählen Sie das SQL-Datendienstobjekt.
5. Wählen Sie im Fenster Details die Ansicht **Gruppenberechtigungen** oder **Benutzerberechtigungen**.
6. Geben Sie die Filterbedingungen zum Suchen nach Benutzern und Gruppen ein und klicken Sie auf die Schaltfläche **Filtern**.

7. Wählen Sie einen Benutzer oder eine Gruppe aus und klicken Sie auf die Schaltfläche **Berechtigungsdetails anzeigen**.

   Das Dialogfeld **Berechtigungsdetails anzeigen** erscheint. Es enthält alle direkt einem Benutzer oder einer Gruppe zugewiesenen Berechtigungen und alle direkten Berechtigungen, die einer übergeordneten Gruppe zugewiesen wurden, sowie Berechtigungen, die von übergeordneten Objekten geerbt wurden. Zusätzlich wird bei den Berechtigungsdetails angezeigt, ob dem Benutzer oder der Gruppe die Administratorrolle zugewiesen ist, wodurch die Prüfung von Berechtigungen übergangen wird.
8. Klicken Sie auf **Schließen**
9. Oder klicken Sie auf **Berechtigungen bearbeiten**, um die Berechtigungen sofort zu ändern.

Bearbeiten von Berechtigungen für den SQL-Datendienst.

Sie können die direkten Berechtigungen für einen SQL-Datendienst für einen Benutzer oder eine Gruppe bearbeiten. Geerbte Berechtigungen oder Ihre eigenen Berechtigungen können Sie nicht widerrufen.

Hinweis: Wenn Sie direkte Berechtigungen für ein Objekt widerrufen, kann der Benutzer oder die Gruppe trotzdem Berechtigungen von einer übergeordneten Gruppe oder einem solchen Objekt erben.

1. Wählen Sie die Ansicht **Dienste und Knoten** auf der Registerkarte Domäne.
2. Wählen Sie im Navigator einen Data Integration Service.
3. In der Inhaltsübersicht wählen Sie die Ansicht **Anwendungen**.
4. Wählen Sie das SQL-Datendienstobjekt.
5. Wählen Sie im Fenster Details die Ansicht **Gruppenberechtigungen** oder **Benutzerberechtigungen**.
6. Geben Sie die Filterbedingungen zum Suchen nach Benutzern und Gruppen ein und klicken Sie auf die Schaltfläche **Filtern**.
7. Wählen Sie einen Benutzer oder eine Gruppe und klicken Sie auf die Schaltfläche **Direkte Berechtigungen bearbeiten**.

   Das Dialogfeld **Direkte Berechtigungen bearbeiten** wird geöffnet.
8. Wählen Sie, ob Sie Berechtigungen erteilen oder widerrufen möchten.
   - Um eine Berechtigung zu erteilen, wählen Sie **Zulassen**.
   - Löschen Sie **Zulassen**, um eine einzelne Berechtigung zu widerrufen.
   - Mit **Widerrufen** widerrufen Sie alle Berechtigungen.

   Indem Sie auf **Berechtigungsdetails anzeigen** klicken, können Sie überprüfen, ob die Berechtigung direkt zugeordnet oder geerbt wurde.
9. Klicken Sie auf **OK**.

Verweigern von Berechtigungen für einen SQL-Datendienst.

Bei einigen SQL-Datendienstobjekten können Sie Berechtigungen ausdrücklich verweigern. Wenn Sie eine Berechtigung für ein Objekt in einem SQL-Datendienst verweigern, wenden Sie eine Ausnahme der effektiven Berechtigung an.

Verwenden Sie zum Verweigern von Berechtigungen einen der folgenden infacmd-Befehle:

- infacmd sql SetStoredProcedurePermissions. Verweigert die Ausführungs- oder Gewährungsberechtigungen auf der Ebene der gespeicherten Prozeduren.
- infacmd sql SetTablePermissions. Verweigert die Auswahl- und Gewährungsberechtigungen auf der virtuellen Tabellenebene.

- infacmd sql SetColumnPermissions. Verweigert die Auswahlberechtigung auf der Spaltenebene.

Jeder Befehl hat Optionen zum Anwenden (-ap) und Verweigern von Berechtigungen (-dp). Der Befehl SetColumnPermissions enthält keine Option zum Anwenden der Berechtigungen.

Hinweis: Berechtigungen vom Administrator Tool können Sie nicht verweigern.

Der Data Integration Service überprüft die Berechtigungen, bevor er SQL-Abfragen und gespeicherte Prozeduren gegen die virtuelle Datenbank startet. Der Data Integration Service validiert die Berechtigungen für Benutzer oder Gruppen beginnend auf der SQL-Datendienstebene. Wenn Berechtigungen für ein übergeordnetes Objekt in einem SQL-Datendienst gelten, erben die Kind-Objekte die Berechtigung. Der Data Integration Service nimmt eine Prüfung auf verweigerte Berechtigungen auf Spaltenebene durch.

Sicherheit auf Spaltenebene

Ein Administrator kann den Zugriff auf Spalten in einer virtuellen Tabelle eines SQL-Datenobjekts verweigern. Der Administrator kann das Verhalten des Data Integration Services für Abfragen einer Spalte mit begrenztem Zugriff konfigurieren.

Wenn der Benutzer eine Spalte abfragt, für die er keine Berechtigung hat, sind folgende Ergebnisse möglich:

- Die Abfrage gibt anstatt der Daten einen Ersatzwert zurück. Die Abfrage gibt in jeder zurückgegebenen Zeile einen Ersatzwert zurück. Der Ersatzwert ersetzt den Spaltenwert durch die Abfrage. Enthält die Abfrage Filter oder Joins, dann erscheint der Ergebnisersatz in den Ergebnissen.
- Die Abfrage schlägt aufgrund eines Fehlers wegen unzureichender Berechtigung fehl.

Weitere Informationen zum Konfigurieren der Sicherheit für SQL-Datendienste finden Sie im Artikel „Sicherheitskonfiguration für SQL-Datendienste“ der Informatica-Ratgeber-Bibliothek: http://communities.informatica.com/docs/DOC-4507.

Eingeschränkte Spalten

Beim Konfigurieren der Sicherheit auf Spaltenebene legen Sie mit einer Option fest, was geschehen soll, wenn ein Benutzer die eingeschränkte Spalte in einer Abfrage auswählt. Sie können die eingeschränkten Daten durch einen Standardwert ersetzen. Alternativ können Sie die Abfrage fehlschlagen lassen, wenn ein Benutzer die eingeschränkte Spalte auswählt.

Zum Beispiel: Ein Administrator verweigert einem Benutzer den Zugriff auf die Spalte Gehalt in der Tabelle Mitarbeiter. Der Administrator konfiguriert einen Ersatzwert von 100.000 für die Spalte Gehalt. Wenn der Benutzer die Spalte Gehalt in einer SQL-Abfrage wählt, gibt der Data Integration Service in jeder Zeile 100.000 als Gehalt an.

Führen Sie den Befehl infacmd sql UpdateColumnOptions aus, um die Spaltenoptionen zu konfigurieren. Es ist nicht möglich, die Spaltenoptionen im Administrator Tool festzulegen

Wenn Sie den Befehl infacmd sql UpdateColumnOptions ausführen, geben Sie die folgenden Optionen an:

ColumnOptions.DenyWith=*option*

Gibt an, ob der Wert der eingeschränkten Spalte ersetzt werden oder die Abfrage fehlschlagen soll. Wenn Sie den Spaltenwert ersetzen, können Sie zwischen NULL oder einem konstanten Wert wählen. Geben Sie eine der folgenden Optionen an:

- ERROR Die Abfrage schlägt fehl und ein Fehler wird zurückgegeben, wenn eine SQL-Abfrage eine eingeschränkte Spalte auswählt.
- NULL. Gibt NULL-Werte für eine eingeschränkte Spalte in jeder Zeile zurück.

- VALUE. Gibt einen konstanten Wert anstelle der eingeschränkten Spalte in jeder Zeile zurück. Konfigurieren Sie den konstanten Wert in der Option ColumnOptions.InsufficientPermissionValue.

ColumnOptions.InsufficientPermissionValue=*value*

Ersetzt den Wert der eingeschränkten Spalte durch einen konstanten Wert. Standard ist ein leerer String. Wenn der Data Integration Service die Spalte durch einen leeren String ersetzt, die Spalte aber ist eine Zahl oder ein Datum ist, gibt die Abfrage einen Fehler zurück. Wenn Sie einen Wert für die Option DenyWith konfigurieren, ignoriert der Data Integration Service die Option InsufficientPermissionValue.

Um einen Ersatzwert für eine Spalte zu konfigurieren, geben Sie den Befehl mit folgender Syntax ein:

```
infacmd sql UpdateColumnOptions -dn empDomain -sn DISService -un Administrator -pd
Adminpass -sqlds employee_APP.employees_SQL -t Employee -c Salary -o
ColumnOptions.DenyWith=VALUE ColumnOptions.InsufficientPermissionValue=100000
```

Wenn Sie keine der Optionen für eine eingeschränktes Spalte konfigurieren, schlagt die Abfrage standardmäßig nicht fehl. Die Abfrage wird ausgeführt und der Data Integration Service ersetzt den Wert der Spalte durch NULL.

Stufenweise Spaltensicherheit hinzufügen

Sie können mit dem Befehl infacmd sql SetColumnPermissions eine stufenweise Spaltensicherheit einrichten. Es ist nicht möglich, die stufenweise Spaltensicherheit im Administrator Tool einzurichten

Zum Beispiel: Eine Angestelltentabelle enthält Spalten für Vorname, Nachname, Abteilung und Gehalt. Sie können dem Benutzer einen Zugriff auf die Tabelle einrichten, der nur den Zugang auf die Spalte Gehalt verhindert.

Um den Benutzer vom Zugriff auf diese Spalte auszunehmen, deaktivieren Sie den Data Integration Service und geben den Befehl infacmd ähnlich dem nachstehenden ein:

```
infacmd sql SetColumnPermissions -dn empDomain -sn DISService -un Administrator -pd
Adminpass -sqlds employee_APP.employees -t Employee -c Salary gun -Tom -dp SQL_Select
```

Die nachstehenden SQL-Anweisungen geben in der Spalte Gehalt NULL zurück:

```
Select * from Employee
Select LastName, Salary from Employee
```

Das Standardverhalten ist das Zurückgeben von Nullwerten.

Web-Dienstmodul

Die Endbenutzer können Web-Dienst-Anfragen senden und erhalten über den Web-Dienst-Client die Antworten des Web-Dienstes. Mit Berechtigungen wird die Zugriffsebene eines Benutzers auf einen Web-Dienst festgelegt.

Berechtigungen lassen sich Benutzern und Gruppen für folgende Web-Dienst-Objekte zuweisen:

- Web-Dienst
- Web-Dienst-Operation

Wenn Sie einem Web-Dienst-Objekt eine Berechtigung zuweisen, erbt der Benutzer oder die Gruppe dieselben Berechtigungen für alle Objekte, die zu diesem Web-Service-Objekt gehören. Angenommen, Sie weisen einem Benutzer eine Ausführungsberechtigung für einen Web-Dienst zu. Der Benutzer erbt diese Berechtigung dann auch für die Web-Dienst-Operationen in diesem Web-Dienst.

Sie können Berechtigungen für Benutzer und Gruppen für eine Web-Dienst-Operation verweigern. Wenn Sie Berechtigungen verweigern, konfigurieren Sie Ausnahmen für die Berechtigungen, die Benutzer und Gruppen bereits haben. Zum Beispiel: Ein Benutzer hat eine Ausführungsberechtigung für einen Web-Dienst, der drei Operationen zulässt. Sie können den Benutzer daran hindern, eine der Web-Service-Operationen auszuführen, die zu diesem Web-Dienst gehören.

Arten von Web-Dienst-Berechtigungen

Sie können die folgenden Berechtigungen für Benutzer und Gruppen zuordnen:

- Berechtigung gewähren Benutzer können die Berechtigungen für die Web-Dienstobjekte mit dem Administrator Tool oder über das Befehlszeilenprogramm *infacmd* verwalten.
- Ausführungsberechtigung. Benutzer können Web-Dienstanfragen verschicken und erhalten Web-Dienstantworten.

Die folgende Tabelle beschreibt die Berechtigungen für die einzelnen Web-Dienstobjekte:

Objekt	Berechtigung gewähren	Ausführungsberechtigung
Web Dienst	Erteilen und entziehen der Berechtigung für den Web-Dienst und alle Web-Dienstoperationen innerhalb des Web-Diensts.	Verschicken von Web-Dienstanfragen und Empfangen von Web-Dienstantworten von allen Web-Dienstoperationen innerhalb des Web-Diensts.
Web-Dienst-Operation	Erteilen, entziehen und verweigern der Berechtigung für Web-Dienstoperation.	Verschicken von Web-Dienstanfragen und Empfangen von Web-Dienstantworten von Web-Dienstoperationen.

Berechtigungen für einen Web-Dienst zuweisen

Wenn Sie Berechtigungen für ein Web-Dienstobjekt zuweisen, legen Sie fest, auf welcher Ebene der Benutzer oder die Gruppe Zugriff zum Objekt hat.

1. Wählen Sie die Ansicht **Dienste und Knoten** auf der Registerkarte Domäne.
2. Wählen Sie im Navigator einen Data Integration Service.
3. In der Inhaltsübersicht wählen Sie die Ansicht **Anwendungen**.
4. Wählen Sie das Web-Dienstobjekt.
5. Wählen Sie im Fenster Details die Ansicht **Gruppenberechtigungen** oder **Benutzerberechtigungen**.
6. Klicken Sie auf die Schaltfläche **Berechtigung zuweisen**.

   Im Dialogfeld **Berechtigungen zuweisen** stehen alle Benutzer oder Gruppen, die keine Berechtigung für das SQL-Datendienstobjekt haben.
7. Geben Sie die Filterbedingungen zum Suchen nach Benutzern und Gruppen ein und klicken Sie auf die Schaltfläche **Filtern**.
8. Wählen Sie einen Benutzer oder eine Gruppe aus und klicken Sie auf **Weiter**.
9. Für jeden Berechtigungstyp, den Sie zuweisen möchten, wählen Sie **Zulassen**.
10. Klicken Sie auf **Fertig stellen**.

Berechtigungsdetails zu einem Web-Dienst anzeigen

Beim Anzeigen von Berechtigungsdetails können Sie den Ursprung effektiver Berechtigungen anzeigen.

1. Wählen Sie die Ansicht **Dienste und Knoten** auf der Registerkarte Domäne.
2. Wählen Sie im Navigator einen Data Integration Service.
3. In der Inhaltsübersicht wählen Sie die Ansicht **Anwendungen**.
4. Wählen Sie das Web-Dienstobjekt.
5. Wählen Sie im Fenster Details die Ansicht **Gruppenberechtigungen** oder **Benutzerberechtigungen**.
6. Geben Sie die Filterbedingungen zum Suchen nach Benutzern und Gruppen ein und klicken Sie auf die Schaltfläche **Filtern**.
7. Wählen Sie einen Benutzer oder eine Gruppe aus und klicken Sie auf die Schaltfläche **Berechtigungsdetails anzeigen**.

   Das Dialogfeld **Berechtigungsdetails anzeigen** erscheint. Es enthält alle direkt einem Benutzer oder einer Gruppe zugewiesenen Berechtigungen und alle direkten Berechtigungen, die einer übergeordneten Gruppe zugewiesen wurden, sowie Berechtigungen, die von übergeordneten Objekten geerbt wurden. Zusätzlich wird bei den Berechtigungsdetails angezeigt, ob dem Benutzer oder der Gruppe die Administratorrolle zugewiesen ist, wodurch die Prüfung von Berechtigungen übergangen wird.
8. Klicken Sie auf **Schließen**
9. Oder klicken Sie auf **Berechtigungen bearbeiten**, um die Berechtigungen sofort zu ändern.

Bearbeiten von Berechtigungen für einen Web-Dienst

Sie können direkte Berechtigungen eines Benutzers oder einer Gruppe für einen Web-Dienst bearbeiten. Bei der Bearbeitung von Berechtigungen eines Benutzers oder einer Gruppe können Sie objektbezogene Berechtigungen verweigern. Geerbte Berechtigungen oder Ihre eigenen Berechtigungen können Sie nicht widerrufen.

Hinweis: Wenn Sie direkte Berechtigungen für ein Objekt widerrufen, kann der Benutzer oder die Gruppe trotzdem Berechtigungen von einer übergeordneten Gruppe oder einem solchen Objekt erben.

1. Wählen Sie die Ansicht **Dienste und Knoten** auf der Registerkarte Domäne.
2. Wählen Sie im Navigator einen Data Integration Service.
3. In der Inhaltsübersicht wählen Sie die Ansicht **Anwendungen**.
4. Wählen Sie das Web-Dienstobjekt.
5. Im Fenster Details wählen Sie die Ansicht **Gruppenberechtigungen** oder **Benutzerberechtigungen**.
6. Geben Sie die Filterbedingungen zum Suchen nach Benutzern und Gruppen ein und klicken Sie auf die Schaltfläche **Filtern**.
7. Wählen Sie einen Benutzer oder eine Gruppe und klicken Sie auf die Schaltfläche **Direkte Berechtigungen bearbeiten**.

   Das Dialogfeld **Direkte Berechtigungen bearbeiten** wird geöffnet.
8. Wählen Sie, ob Sie Berechtigungen erteilen oder widerrufen möchten.
   - Um eine Berechtigung zu erteilen, wählen Sie **Zulassen**.
   - Mit **Verweigern** verweigern Sie eine Berechtigung für eine Web-Dienstobjekt.
   - Löschen Sie **Zulassen**, um eine einzelne Berechtigung zu widerrufen.
   - Mit **Widerrufen** widerrufen Sie alle Berechtigungen.

Indem Sie auf **Berechtigungsdetails anzeigen** klicken, können Sie überprüfen, ob die Berechtigung direkt zugeordnet oder geerbt wurde.

9. Klicken Sie auf **OK**.

KAPITEL 10

Auditberichte

Dieses Kapitel umfasst die folgenden Themen:

Auditberichte - Übersicht

Verwenden Sie die Auditberichte, um Informationen über Benutzer und Gruppen in der Informatica-Domäne und ihnen zugewiesene Berechtigungen anzuzeigen.

Sie können die folgenden Auditberichte generieren:

Persönliche Benutzerinformationen

Zeigt Informationen über die Benutzerkonten in der Domäne einschließlich des Benutzerstatus an. Sie können die Benutzer oder Gruppen auswählen, für die Sie den Bericht generieren möchten.

Benutzergruppen-Zuordnung

Zeigt Informationen zu Benutzern und den Gruppen an, zu denen sie gehören. Sie können die Benutzer oder Gruppen auswählen, für die Sie den Bericht generieren möchten.

Berechtigungen

Zeigt Informationen über Berechtigungen an, die Benutzern und Gruppen in der Domäne zugewiesen sind. Sie können die Benutzer oder Gruppen auswählen, für die Sie den Bericht generieren möchten.

Rollen

Zeigt Informationen über die Rollen an, die Benutzern und Gruppen in der Domäne zugewiesen sind. Sie können die Rollen auswählen, für die Sie den Bericht generieren möchten.

Domänenobjektberechtigungen

Zeigt Informationen über die Domänenobjekte an, für die Benutzer und Gruppen über eine Berechtigung verfügen. Sie können die Benutzer oder Gruppen auswählen, für die Sie den Bericht generieren möchten.

Sie können die Auditberichte in verschiedenen Formaten, einschließlich CSV-, Text- bzw. PDF-Dateien, generieren. Sie können den Bericht auch auf dem Bildschirm anzeigen.

Sie können die Auditberichte aus dem Administrator-Tool oder über die Befehlszeile generieren. Führen Sie zum Ausführen der Auditberichte über die Befehlszeile das Befehlszeilenprogramm „infacmd“ aus.

Persönliche Benutzerinformationen

Der Bericht zu den persönlichen Benutzerinformationen zeigt die Kontaktinformationen und den Status von Benutzerkonten in der Domäne an.

Wenn Sie den Bericht für Gruppen ausführen, ordnet der Bericht die Liste von Benutzern nach Gruppen an und zeigt den Gruppennamen und die Sicherheitsdomäne für jede Gruppe an. Der Bericht zeigt die geschachtelten Gruppen separat an.

Der Bericht zu den persönlichen Benutzerinformationen zeigt die folgenden Informationen an:

Anmeldename

Anmeldename für das Benutzerkonto.

Vollständiger Name

Vollständiger Name für das Benutzerkonto.

Sicherheitsdomäne

Sicherheitsdomäne, zu der der Benutzer gehört.

Beschreibung

Beschreibung des Benutzerkontos.

E-Mail-ID

E-Mail-Adresse des Benutzerkontos.

Telefon

Telefonnummer des Benutzerkontos.

Konto gesperrt

Gibt an, ob das Konto gesperrt ist. Der Bericht zeigt „Ja“ an, wenn das Konto gesperrt ist, und „Nein“ an, wenn das Konto nicht gesperrt ist.

Konto deaktiviert

Gibt an, ob das Konto deaktiviert ist. Der Bericht zeigt „Ja“ an, wenn das Konto deaktiviert ist, und „Nein“ an, wenn das Konto aktiviert ist.

Benutzergruppen-Zuordnung

Der Bericht zur Benutzergruppen-Zuordnung zeigt Informationen über die Benutzer und deren verbundenen Gruppen an.

Wenn Sie den Bericht für Benutzer ausführen, zeigt der Bericht die Liste der Benutzer und Gruppen an, zu denen sie gehören.

Der Bericht zur Benutzergruppen-Zuordnung zeigt die folgenden Informationen an:

Anmeldename

Anmeldename für das Benutzerkonto.

Vollständiger Name

Vollständiger Name für das Benutzerkonto.

Sicherheitsdomäne

Sicherheitsdomäne, zu der das Benutzerkonto gehört.

Gruppenname

Name der Gruppe, zu der der Benutzer gehört.

Gruppenpfad

Wenn es sich bei der Gruppe um eine einzelne Gruppe handelt, zeigt der Gruppenpfad den Gruppennamen an. Wenn es sich bei der Gruppe um eine geschachtelte Gruppe handelt, zeigt der Gruppenpfad die Position der Gruppe in der Hierarchie der geschachtelten Gruppen an.

Gruppensicherheitsdomäne

Sicherheitsdomäne für die Gruppe, zu der der Benutzer gehört.

Wenn Sie den Bericht für Gruppen ausführen, ordnet der Bericht die Liste von Benutzern nach Gruppen an und zeigt den Gruppennamen und die Sicherheitsdomäne für jede Gruppe an. Der Bericht zeigt die geschachtelten Gruppen separat an. Der Bericht zeigt für jede Gruppe die Liste von Benutzern und untergeordneten Gruppen an, die zur Gruppe gehören.

Der Bericht zur Benutzergruppen-Zuordnung zeigt die folgenden Informationen für die Benutzer an, die zur Gruppe gehören:

Anmeldename

Anmeldename für das Benutzerkonto.

Vollständiger Name

Vollständiger Name für das Benutzerkonto.

Sicherheitsdomäne

Sicherheitsdomäne, zu der das Benutzerkonto gehört.

Der Bericht zur Benutzergruppen-Zuordnung zeigt die folgenden Informationen für die untergeordneten Gruppen an, die zur Gruppe gehören:

Gruppenname

Name der Gruppe.

Sicherheitsdomäne

Sicherheitsdomäne, zu der die Gruppe gehört.

Gruppenpfad

Wenn es sich bei der Gruppe um eine einzelne Gruppe handelt, zeigt der Gruppenpfad den Gruppennamen an. Wenn es sich bei der Gruppe um eine geschachtelte Gruppe handelt, zeigt der Gruppenpfad die Position der Gruppe in der Hierarchie der geschachtelten Gruppen an.

Berechtigungen

Der Bericht zu Berechtigungen zeigt die Benutzer und Gruppen sowie die Berechtigungen an, die zu Benutzern und Gruppen zugewiesen sind.

Wenn Sie den Bericht für Benutzer ausführen, zeigt der Bericht die Liste der Benutzer und Berechtigungen an, die jedem Benutzer zugewiesen sind. Wenn Sie den Bericht für Gruppen ausführen, zeigt der Bericht die Liste der Gruppen und Berechtigungen an, die jeder Gruppe zugewiesen sind.

Der Bericht zu den Berechtigungen zeigt die folgenden Informationen an:

Berechtigungsname

Name der Berechtigung.

Berechtigungspfad

Die Hierarchie der Berechtigungsgruppe, die die Berechtigung enthält.

Objektname

Name des Objekts, für das die Berechtigung zulässig ist.

Objekttyp

Typ des Objekts, für das die Berechtigung zulässig ist.

Rollenzuordnung

Der Bericht zur Rollenzuordnung zeigt eine Liste von Rollen sowie Benutzern und Gruppen an, zu denen die Rollen zugewiesen sind.

Der Bericht zur Rollenzuordnung zeigt die folgenden Informationen an:

Anmeldename

Anmeldename für das Benutzerkonto, dem die Rolle zugewiesen ist. Wird für die Liste von Benutzern angezeigt.

Vollständiger Name

Vollständiger Name für das Benutzerkonto, dem die Rolle zugewiesen ist. Wird für die Liste von Benutzern angezeigt.

Gruppenname

Name der Gruppe, der die Rolle zugewiesen ist. Wird für die Liste von Gruppen angezeigt.

Sicherheitsdomäne

Sicherheitsdomäne, zu der der Benutzer oder die Gruppe gehört.

Objektname

Name des Objekts, auf dem der Satz von Berechtigungen in der Rolle zulässig ist.

Objekttyp

Typ des Objekts, auf dem der Satz von Berechtigungen in der Rolle zulässig ist.

Domänenobjektberechtigung

Der Bericht zur Domänenobjektberechtigung zeigt die Benutzer und Gruppen sowie Objekte an, für die die Benutzer und Gruppen über eine Berechtigung verfügen.

Wenn Sie den Bericht für Benutzer ausführen, zeigt der Bericht die Liste der Benutzer und Objekte an, für die die Benutzer über Berechtigungen verfügen. Wenn Sie den Bericht für Gruppen ausführen, zeigt der Bericht die Liste der Gruppen und Objekte an, für die die Gruppen über Berechtigungen verfügen.

Der Bericht zur Domänenobjektberechtigung zeigt die folgenden Informationen an:

Objektname

Name des Objekts, für das der Benutzer oder die Gruppe über eine Berechtigung verfügt.

Objekttyp

Typ des Objekts, für das der Benutzer oder die Gruppe über eine Berechtigung verfügt.

Objektpfad

Speicherort des Objekts im Repository.

Auswählen von Benutzern für einen Auditbericht

Sie können einen Auditbericht für mehrere Benutzer generieren.

1. Klicken Sie im Administrator-Tool auf **Sicherheit** > **Auditberichte**.
2. Wählen Sie aus der Liste **Berichtstyp auswählen** den Typ des Auditberichts aus, den Sie ausführen möchten.
3. Wählen Sie aus der Liste **Bericht generieren für Benutzer** aus und klicken Sie auf **Los**.

   Das Dialogfeld **Benutzer auswählen** wird angezeigt. Standardmäßig ist das Symbol **Benutzer** ausgewählt und die Liste aller verfügbaren Benutzer wird angezeigt. Die Liste zeigt den vollständigen Namen des Benutzers und die Sicherheitsdomäne an, zu der der Benutzer gehört.
4. Wählen Sie aus der Liste **Verfügbare Benutzer** die Benutzer aus, für die Sie den Bericht ausführen möchten.

   Mithilfe der Umschalt- oder Strg-Taste können Sie mehrere Benutzer auswählen.
5. Um Benutzer nach der Gruppe auszuwählen, klicken Sie auf das Symbol **Gruppen**.

   Die Liste **Verfügbare Gruppen** zeigt alle Gruppen in der Domäne an und die Liste **Mitglieder** zeigt die Benutzer an, die Mitglieder der Gruppen sind. Wählen Sie aus der Liste **Mitglieder** die Benutzer aus, für die Sie den Bericht ausführen möchten. Sie können Benutzer aus mehreren Gruppen auswählen.
6. Klicken Sie auf **Hinzufügen**.

   Klicken Sie zum Ausführen des Berichts für alle Benutzer auf das Symbol **Benutzer** und anschließend auf **Alle hinzufügen**, ohne einen Benutzer auszuwählen.

   Um den Bericht für alle Benutzer in einer Gruppe auszuführen, klicken Sie auf das Symbol **Gruppen**. Wählen Sie eine Gruppe aus und klicken Sie auf **Alle hinzufügen**, ohne einen Benutzer aus der Liste **Mitglieder** auszuwählen.

   Die ausgewählten Benutzer wurden in die Liste **Ausgewählte Benutzer** verschoben.
7. Wählen Sie aus der Liste **Berichtausgabeformat** das Format aus, in dem Sie den Bericht sehen möchten.

Der Bericht wird standardmäßig auf dem Bildschirm angezeigt.
Sie können einen Auditbericht auch in einem der folgenden Formate anzeigen:

- Text. Generiert den Auditbericht als Textdatei mit in Spalten aufgelisteten Werten.
- CSV. Generiert den Auditbericht als Textdatei mit durch Kommas getrennten Werten.
- PDF. Generiert den Auditbericht im PDF-Format. Sie müssen Acrobat Reader zum Anzeigen des Berichts installieren.

8. Klicken Sie auf **Bericht generieren**.

Auswählen von Gruppen für einen Auditbericht

Sie können Auditberichte für mehrere Gruppen ausführen.

1. Klicken Sie im Administrator-Tool auf **Sicherheit** > **Auditberichte**.
2. Wählen Sie aus der Liste **Berichtstyp auswählen** den Typ des Auditberichts aus, den Sie ausführen möchten.
3. Wählen Sie aus der Liste **Bericht generieren für Gruppen** aus und klicken Sie auf **Los**.

   Das Dialogfeld **Gruppen auswählen** wird angezeigt. Die Liste von Gruppen wird nach der Sicherheitsdomäne organisiert.
4. Wählen Sie aus der Liste **Verfügbare Gruppen** die Gruppen aus, für die Sie den Bericht ausführen möchten.

   Mithilfe der Umschalt- oder Strg-Taste können Sie mehrere Gruppen auswählen.
5. Klicken Sie auf **Hinzufügen**.

   Wählen Sie zum Ausführen des Berichts für alle Gruppen keine Gruppe aus und klicken Sie auf **Alle hinzufügen**.

   Die ausgewählten Gruppen wurden in die Liste **Ausgewählte Gruppen** verschoben.
6. Wählen Sie aus der Liste **Berichtausgabeformat** das Format aus, in dem Sie den Bericht sehen möchten.

   Standardmäßig werden die Berichte auf dem Bildschirm angezeigt.
   Sie können einen Auditbericht auch in einem der folgenden Formate ausführen:

   - Text. Generiert den Auditbericht als Textdatei mit in Spalten aufgelisteten Werten.
   - CSV. Generiert den Auditbericht als Textdatei mit durch Kommas getrennten Werten.
   - PDF. Generiert den Auditbericht im PDF-Format. Sie müssen Acrobat Reader zum Anzeigen des Berichts installieren.
7. Klicken Sie auf **Bericht generieren**.

Auswählen von Rollen für einen Auditbericht

Beim Ausführen des Berichts zur Rollenzuordnung müssen Sie die Rollen auswählen, für die Sie den Bericht ausführen möchten.

1. Klicken Sie im Administrator-Tool auf **Sicherheit** > **Auditberichte**.

2. Wählen Sie aus der Liste **Berichtstyp auswählen** den Bericht **Rollenzuordnung** aus.
3. Wählen Sie aus der Liste **Bericht generieren für Rollen** aus und klicken Sie auf **Los**.

   Das Dialogfeld **Rollen auswählen** wird angezeigt. Die Liste der systemdefinierten Rollen wird getrennt von der Liste benutzerdefinierter Rollen angezeigt.
4. Wählen Sie aus der Liste **Verfügbare Rollen** die Rollen aus, für die Sie den Bericht ausführen möchten.

   Mithilfe der Umschalt- oder Strg-Taste können Sie mehrere Rollen auswählen.
5. Klicken Sie auf **Hinzufügen**.

   Wählen Sie zum Ausführen des Berichts für alle Rollen keine Rolle aus und klicken Sie auf **Alle hinzufügen**.

   Die ausgewählten Rollen wurden in die Liste **Ausgewählte Rollen** verschoben.
6. Wählen Sie aus der Liste **Berichtausgabeformat** das Format aus, in dem Sie den Bericht sehen möchten.

   Standardmäßig werden die Berichte auf dem Bildschirm angezeigt.
   Sie können einen Auditbericht auch in einem der folgenden Formate ausführen:
   - Text. Generiert den Auditbericht als Textdatei mit in Spalten aufgelisteten Werten.
   - CSV. Generiert den Auditbericht als Textdatei mit durch Kommas getrennten Werten.
   - PDF. Generiert den Auditbericht im PDF-Format. Sie müssen Acrobat Reader zum Anzeigen des Berichts installieren.
7. Klicken Sie auf **Bericht generieren**.

ANHANG A

Benutzerdefinierte Rollen

Dieser Anhang umfasst die folgenden Themen:

PowerCenter Repository Service - Benutzerdefinierte Rollen

Die folgende Tabelle enthält die die Standardberechtigungen, die der benutzerdefinierten Rolle "PowerCenter - Verbindungsadministrator" zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Tools	Workflow Manager öffnen
Globale Objekte	Verbindungen erstellen

Die folgende Tabelle enthält die die Standardberechtigungen, die der benutzerdefinierten Rolle "PowerCenter - Entwickler" zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Tools	- Designer öffnen - Workflow Manager öffnen - Workflow Monitor öffnen
Designobjekte	- Erstellen, Bearbeiten und Löschen - Versionen verwalten

Berechtigungsgruppe	Name der Berechtigung
Quellen und Targets	- Erstellen, Bearbeiten und Löschen - Versionen verwalten
Laufzeitobjekte	- Erstellen, Bearbeiten und Löschen - Ausführen - Versionen verwalten - Überwachen

Die folgende Tabelle enthält die die Standardberechtigungen, die der benutzerdefinierten Rolle "PowerCenter - Operator" zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Tools	Workflow Monitor öffnen
Laufzeitobjekte	- Ausführen - Ausführung verwalten - Überwachen

Die folgende Tabelle enthält die die Standardberechtigungen, die der benutzerdefinierten Rolle "PowerCenter - Repository-Ordneradministrator" zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Tools	Zugriff auf Repository Manager
Ordner	- Kopieren - Erstellen - Versionen verwalten
Globale Objekte	- Bereitstellungsgruppen verwalten - Bereitstellungsgruppen werden ausgeführt - Beschriftungen erstellen - Berechtigung zum Erstellen von Anfragen

Benutzerdefinierte Rollen für den Metadata Manager-Dienst

Zu den benutzerdefinierten Rollen für den Metadata Manager-Dienst gehören die Rollen „Metadata Manager - Erweiterter Benutzer“, „Metadata Manager - Standardbenutzer“ und „Metadata Manager - Fortgeschrittener Benutzer“.

Die folgende Tabelle enthält die die Standardberechtigungen, die der benutzerdefinierten Rolle "Metadata Manager - Erweiterter Benutzer" zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Katalog	- Verknüpfungen gemeinsam nutzen - Herkunft anzeigen - Zugehörige Kataloge anzeigen - Berichte anzeigen - Profilergebnisse anzeigen - Katalog anzeigen - Beziehungen anzeigen - Verwalten von Beziehungen - Kommentare anzeigen - Kommentare posten - Kommentare löschen - Links anzeigen - Links verwalten - Glossar anzeigen - Objekte verwalten
Laden	- Ressource anzeigen - Ressource laden - Zeitpläne verwalten - Metadaten bereinigen - Ressource verwalten
Modell	- Modell anzeigen - Modell verwalten - Modelle exportieren/importieren
Sicherheit	Katalogberechtigungen verwalten

Die folgende Tabelle enthält die die Standardberechtigungen, die der benutzerdefinierten Rolle "Metadata Manager - Standardbenutzer" zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Katalog	- Herkunft anzeigen - Zugehörige Kataloge anzeigen - Katalog anzeigen - Beziehungen anzeigen - Kommentare anzeigen - Links anzeigen
Modell	Modell anzeigen

Die folgende Tabelle enthält die die Standardberechtigungen, die der benutzerdefinierten Rolle "Metadata Manager - Fortgeschrittener Benutzer" zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Katalog	- Herkunft anzeigen - Zugehörige Kataloge anzeigen - Berichte anzeigen - Profilergebnisse anzeigen - Katalog anzeigen - Beziehungen anzeigen - Kommentare anzeigen - Kommentare posten - Kommentare löschen - Links anzeigen - Links verwalten - Glossar anzeigen
Laden	- Ressource anzeigen - Ressource laden
Modell	Modell anzeigen

Benutzerdefinierte Rollen für den Reporting Service

Die folgende Tabelle enthält die die Standardberechtigungen, die der benutzerdefinierte Rolle "Reporting Service - Erweiterte Verbraucher" zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Administration	- Schema pflegen - XML-Dateien exportieren/importieren - Benutzerzugriff verwalten - Zeitplan und Tasks einrichten - Systemeigenschaften verwalten - Abfragegrenzen einrichten - Echtzeit-Nachrichtenströme konfigurieren
Alarme	- Alarme erhalten - Echtzeitalarme erstellen - Zustelloptionen einrichten

Berechtigungsgruppe	Name der Berechtigung
Kommunikation	- Drucken - E-Mail-Objektverknüpfungen - E-Mail-Objektinhalte - Exportieren - Export nach Excel oder CSV - Export nach Pivot-Tabellen - Diskussionen anzeigen - Diskussionen hinzufügen - Diskussionen verwalten - Feedback geben
Inhaltsverzeichnis	- Auf Inhaltsverzeichnis zugreifen - Erweiterte Suche öffnen - Inhaltsverzeichnis verwalten - Fortgeschrittene Suche verwalten
Dashboard	- Dashboards anzeigen - Persönliche Dashboards verwalten
Indikatoren	- Mit Indikatoren interagieren - Echtzeitindikatoren erstellen - Kontinuierliche, automatische Echtzeit-Indikatoraktualisierungen erhalten
Konten verwalten	Persönliche Einstellungen verwalten
Berichte	- Berichte anzeigen - Berichte analysieren - Mit Daten interagieren - Beliebigen Drill ausführen - Filtersätze erstellen - Benutzerdefinierte Metrik fortführen - Abfrage anzeigen - Lifecycle-Metadata anzeigen - Berichten erstellen und löschen - Auf grundlegende Berichtserstellung zugreifen - Auf erweiterte Berichtserstellung zugreifen - Berichtskopien speichern - Berichte bearbeiten

Die folgende Tabelle enthält die die Standardberechtigungen, die der benutzerdefinierte Rolle "Reporting Service - Erweiterter Provider" zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Administration	Schema pflegen
Alarme	- Alarme erhalten - Echtzeitalarme erstellen - Zustelloptionen einrichten
Kommunikation	- Drucken - E-Mail-Objektverknüpfungen - E-Mail-Objektinhalte - Exportieren - Export nach Excel oder CSV - Export nach Pivot-Tabellen - Diskussionen anzeigen - Diskussionen hinzufügen - Diskussionen verwalten - Feedback geben
Inhaltsverzeichnis	- Auf Inhaltsverzeichnis zugreifen - Erweiterte Suche öffnen - Inhaltsverzeichnis verwalten - Fortgeschrittene Suche verwalten
Dashboards	- Dashboards anzeigen - Persönliche Dashboards verwalten - Dashboards erstellen, bearbeiten und löschen - Auf grundlegende Dashboardserstellung zugreifen - Auf erweiterte Dashboardserstellung zugreifen
Indikatoren	- Mit Indikatoren interagieren - Echtzeitindikatoren erstellen - Kontinuierliche, automatische Echtzeit-Indikatoraktualisierungen erhalten

Berechtigungsgruppe	Name der Berechtigung
Konten verwalten	Persönliche Einstellungen verwalten
Berichte	- Berichte anzeigen - Berichte analysieren - Mit Daten interagieren - Beliebigen Drill ausführen - Filtersätze erstellen - Benutzerdefinierte Metrik fortführen - Abfrage anzeigen - Lifecycle-Metadata anzeigen - Berichten erstellen und löschen - Auf grundlegende Berichtserstellung zugreifen - Auf erweiterte Berichtserstellung zugreifen - Berichtskopien speichern - Berichte bearbeiten

Die folgende Tabelle enthält die die Standardberechtigungen, die der benutzerdefinierte Rolle "Reporting Service - Standardverbraucher" zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Alarme	- Alarme erhalten - Zustelloptionen einrichten
Kommunikation	- Drucken - E-Mail-Objektverknüpfungen - Exportieren - Diskussionen anzeigen - Diskussionen hinzufügen - Feedback geben
Inhaltsverzeichnis	Auf Inhaltsverzeichnis zugreifen
Dashboards	Dashboards anzeigen
Konto verwalten	Persönliche Einstellungen verwalten
Berichte	- Berichte anzeigen - Berichte analysieren

Die folgende Tabelle enthält die die Standardberechtigungen, die der benutzerdefinierte Rolle "Reporting Service - Standardprovider" zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Administration	Schema pflegen
Alarme	- Alarme erhalten - Echtzeitalarme erstellen - Zustelloptionen einrichten
Kommunikation	- Drucken - E-Mail-Objektverknüpfungen - E-Mail-Objektinhalte - Exportieren - Export nach Excel oder CSV - Export nach Pivot-Tabellen - Diskussionen anzeigen - Diskussionen hinzufügen - Diskussionen verwalten - Feedback geben
Inhaltsverzeichnis	- Auf Inhaltsverzeichnis zugreifen - Erweiterte Suche öffnen - Inhaltsverzeichnis verwalten - Fortgeschrittene Suche verwalten
Dashboards	- Dashboards anzeigen - Persönliche Dashboards verwalten - Dashboards erstellen, bearbeiten und löschen - Auf grundlegende Dashboarderstellung zugreifen
Indikatoren	- Mit Indikatoren interagieren - Echtzeitindikatoren erstellen - Kontinuierliche, automatische Echtzeit-Indikatoraktualisierungen erhalten

Berechtigungsgruppe	Name der Berechtigung
Konten verwalten	Persönliche Einstellungen verwalten
Berichte	- Berichte anzeigen - Berichte analysieren - Mit Daten interagieren - Beliebigen Drill ausführen - Filtersätze erstellen - Benutzerdefinierte Metrik fortführen - Abfrage anzeigen - Lifecycle-Metadata anzeigen - Berichten erstellen und löschen - Auf grundlegende Berichtserstellung zugreifen - Auf erweiterte Berichtserstellung zugreifen - Berichtskopien speichern - Berichte bearbeiten

Die folgende Tabelle enthält die die Standardberechtigungen, die der benutzerdefinierte Rolle "Reporting Service - Fortgeschrittene Verbraucher" zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Alarme	- Alarme erhalten - Zustelloptionen einrichten
Kommunikation	- Drucken - E-Mail-Objektverknüpfungen - Exportieren - Export nach Excel oder CSV - Export nach Pivot-Tabellen - Diskussionen anzeigen - Diskussionen hinzufügen - Diskussionen verwalten - Feedback geben
Inhaltsverzeichnis	Auf Inhaltsverzeichnis zugreifen
Dashboards	- Dashboards anzeigen - Persönliche Dashboards verwalten
Indikatoren	- Mit Indikatoren interagieren - Kontinuierliche, automatische Echtzeit-Indikatoraktualisierungen erhalten

Berechtigungsgruppe	Name der Berechtigung
Konten verwalten	Persönliche Einstellungen verwalten
Berichte	- Berichte anzeigen - Berichte analysieren - Mit Daten interagieren - Lifecycle-Metadata anzeigen - Berichtskopien speichern

Die folgende Tabelle enthält die die Standardberechtigungen, die der benutzerdefinierte Rolle "Reporting Service - Verbraucher mit Lesezugriff" zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Berichte	Berichte anzeigen

Die folgende Tabelle enthält die die Standardberechtigungen, die der benutzerdefinierte Rolle "Reporting Service - Schemadesigner" zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Administration	- Schema pflegen - Zeitplan und Tasks einrichten - Echtzeit-Nachrichtenströme konfigurieren
Alarme	- Alarme erhalten - Echtzeitalarme erstellen - Zustelloptionen einrichten
Kommunikation	- Drucken - E-Mail-Objektverknüpfungen - E-Mail-Objektinhalte - Exportieren - Export nach Excel oder CSV - Export nach Pivot-Tabellen - Diskussionen anzeigen - Diskussionen hinzufügen - Diskussionen verwalten - Feedback geben
Inhaltsverzeichnis	- Auf Inhaltsverzeichnis zugreifen - Erweiterte Suche öffnen - Inhaltsverzeichnis verwalten - Fortgeschrittene Suche verwalten

Berechtigungsgruppe	Name der Berechtigung
Dashboards	- Dashboards anzeigen - Persönliche Dashboards verwalten - Dashboards erstellen, bearbeiten und löschen
Indikatoren	- Mit Indikatoren interagieren - Echtzeitindikatoren erstellen - Kontinuierliche, automatische Echtzeit-Indikatoraktualisierungen erhalten
Konten verwalten	Persönliche Einstellungen verwalten
Berichte	- Berichte anzeigen - Berichte analysieren - Mit Daten interagieren - Beliebigen Drill ausführen - Filtersätze erstellen - Benutzerdefinierte Metrik fortführen - Abfrage anzeigen - Lifecycle-Metadata anzeigen - Berichten erstellen und löschen - Auf grundlegende Berichtserstellung zugreifen - Auf erweiterte Berichtserstellung zugreifen - Berichtskopien speichern - Berichte bearbeiten

Benutzerdefinierte Rollen für den Test Data Manager-Dienst

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Testdaten-Administrator“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Projekte	Projekt prüfen
Verwaltung	- Verbindungen anzeigen - Verbindungen verwalten

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Testdaten-Entwickler“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Richtlinien	- Richtlinien anzeigen - Richtlinien verwalten
Regeln	- Maskierungsregeln anzeigen - Maskierungsregeln verwalten - Generierungsregeln anzeigen
Datendomänen	- Datendomänen anzeigen - Datendomänen verwalten
Projekte	Projekt prüfen

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Testdaten-Projekt-DBA“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Projekte	- Projekt anzeigen - Projekt ausführen - Projekt überwachen - Projekt prüfen
Verwaltung	- Verbindungen anzeigen - Verbindungen verwalten

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Testdaten-Projektentwickler“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Richtlinien	Richtlinien anzeigen
Regeln	- Maskierungsregeln anzeigen - Generierungsregeln anzeigen
Datendomänen	Datendomänen anzeigen
Projekte	- Projekt anzeigen - Projekt ermitteln - Projekt ausführen - Projekt überwachen - Projekt prüfen - Metadaten importieren
Datenmaskierung	- Datenmaskierung anzeigen - Datenmaskierung verwalten
Datenteilmenge	- Data Subset anzeigen - Data Subset verwalten

Berechtigungsgruppe	Name der Berechtigung
Datengenerierung	- Datengenerierung anzeigen - Datengenerierung verwalten
Verwaltung	- Verbindungen anzeigen - Verbindungen verwalten

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Testdaten-Projekteigentümer“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Richtlinien	Richtlinien anzeigen
Regeln	- Maskierungsregeln anzeigen - Generierungsregeln anzeigen
Datendomänen	Datendomänen anzeigen
Projekte	- Projekt anzeigen - Projekt verwalten - Projekt ermitteln - Projekt ausführen - Projekt überwachen - Projekt prüfen - Metadaten importieren
Datenmaskierung	- Datenmaskierung anzeigen - Datenmaskierung verwalten
Datenteilmenge	- Data Subset anzeigen - Data Subset verwalten
Datengenerierung	- Datengenerierung anzeigen - Datengenerierung verwalten
Verwaltung	- Verbindungen anzeigen - Verbindungen verwalten

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Testdaten-Risikomanager“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Richtlinien	Richtlinien anzeigen
Regeln	- Maskierungsregeln anzeigen - Generierungsregeln anzeigen
Datendomänen	Datendomänen anzeigen
Projekte	Projekt prüfen

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Testdaten-Spezialist“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Richtlinien	Richtlinien anzeigen
Regeln	- Maskierungsregeln anzeigen - Maskierungsregeln verwalten - Generierungsregeln anzeigen - Generierungsregeln verwalten
Datendomänen	- Datendomänen anzeigen - Datendomänen verwalten
Projekte	- Projekt verwalten - Projekt anzeigen - Projekt ermitteln - Projekt ausführen - Projekt überwachen - Projekt prüfen - Metadaten importieren
Datenmaskierung	- Datenmaskierung anzeigen - Datenmaskierung verwalten
Datenteilmenge	- Data Subset anzeigen - Data Subset verwalten
Datengenerierung	- Datengenerierung anzeigen - Datengenerierung verwalten
Verwaltung	- Verbindungen anzeigen - Verbindungen verwalten

Hinweis: Wenn Ihre TDM-Einrichtung Informatica Services 9.6.1 verwendet oder wenn Sie auf Informatica Services 9.6.1 HotFix 1 aktualisiert haben, kann ein Benutzer mit der Rolle „Testdaten-Spezialist“ Datengenerierungsregeln weder erstellen noch löschen. Die Rolle enthält nicht die Berechtigung zum Verwalten der Datengenerierung. Damit Benutzer mit dieser Rolle Datengenerierungsregeln erstellen und löschen können, müssen Sie die Rolle manuell bearbeiten. Melden Sie sich am Administrator-Tool an und bearbeiten Sie die benutzerdefinierte Rolle des TDM-Diensts, um die Berechtigung zum Verwalten von Generierungsregeln aus der Berechtigungsgruppe „Regeln“ einzubeziehen.

Benutzerdefinierte Rolle für den Analyst-Dienst

Der Business Glossary-Verbraucher für den Analyst-Dienst ist eine benutzerdefinierte Rolle für den Analyst-Dienst.

Die folgende Tabelle listet die standardmäßige Berechtigung auf, die der benutzerdefinierten Rolle des Business Glossary-Verbrauchers für den Analyst-Dienst zugewiesen ist:

Berechtigungsgruppe	Name der Berechtigung
Zugriff auf Workspace	Glossar-Workspace

ANHANG B

Standardliste der Chiffre-Suites

Standardmäßig verwendet die Informatica-Domäne die folgenden Chiffre-Suites für sichere Kommunikation innerhalb der Domäne sowie für sichere Clientverbindungen:

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256

INDEX

C

D

E

G

I

K

L

M

N

O

P

Q

R

S

T

U

V

W