



Informatica®
10.5.9

Handbuch für Sicherheit

© Copyright Informatica LLC 2013, 2025

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

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

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

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

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

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

Die in dieser Dokumentation enthaltenen Informationen können jederzeit ohne vorherige Ankündigung geändert werden. Wenn Sie Probleme in dieser Dokumentation finden, melden Sie sie uns unter infa_documentation@informatica.com.

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

Publikationsdatum: 2025-10-21

Inhalt

Einleitung	11
Informatica-Ressourcen.	11
Informatica Network.	11
Informatica-Wissensdatenbank.	11
Informatica-Dokumentation.	12
Informatica-Produktverfügbarkeitsmatrizen.	12
Informatica Velocity.	12
Informatica Marketplace.	12
Informatica – Weltweiter Kundensupport.	12
 Kapitel 1: Einführung in die Informatica-Sicherheit.....	13
Übersicht über die Informatica-Sicherheit.	13
Infrastruktur-Sicherheit.	14
Authentifizierung.	14
Sichere Domänenkommunikation.	15
Sicherer Datenspeicher.	16
Operationssicherheit.	16
Domänenkonfigurations-Repository.	17
Sicherheitsdomäne.	17
 Kapitel 2: Benutzerauthentifizierung.....	19
Benutzerauthentifizierung - Übersicht.	19
Native Benutzerauthentifizierung.	20
LDAP-Benutzerauthentifizierung.	21
Kerberos-Authentifizierung.	21
SAML-Authentifizierung.	22
SAML-Authentifizierung für Informatica-Webanwendungen.	22
SAML-Authentifizierung für Informatica Developer.	22
 Kapitel 3: LDAP-Authentifizierung.....	24
Übersicht.	24
LDAP-Sicherheitsdomänen.	25
Synchronisierung des Benutzerkontos.	25
LDAP-Verzeichnisdienste.	25
Azure Active Directory für eine sichere LDAP-Authentifizierung.	26
Vorbereiten des Imports von Active Directory-Benutzerkonten.	27
Erstellen einer LDAP-Konfiguration.	27
Erstellen der LDAP-Konfiguration und Konfigurieren der LDAP-Serververbindung.	28
Konfigurieren der Sicherheitsdomäne.	30
Konfigurieren des Synchronisationszeitplans.	31

Geschachtelte Gruppen im LDAP-Verzeichnisdienst verwenden.	32
Ein selbstsigniertes SSL-Zertifikat verwenden.	32
Löschen einer LDAP-Konfiguration.	33

Kapitel 4: Kerberos-Authentifizierung..... 34

Überblick über Kerberos.	34
Funktionsweise von Kerberos in einer Informatica-Domäne.	35
Bereichsübergreifende Kerberos-Authentifizierung.	37
Umwandeln einer Domäne mit einer Kerberos-Konfiguration für Einzelbereiche in eine Domäne mit bereichsübergreifender Kerberos-Konfiguration.	37
Vorbereiten der Aktivierung der Kerberos-Authentifizierung.	39
Bestimmen der Kerberos-Dienstprinzipalebene.	39
Konfigurieren der Kerberos-Konfigurationsdatei.	39
Erstellen der Kerberos-Prinzipalkonten in Active Directory.	43
Generieren der Formate für Dienstprinzipalnamen und Keytab-Dateinamen.	44
Generieren der Keytab-Dateien.	49
Aktivieren der Kerberos-Authentifizierung.	53
Aktivieren der Kerberos-Authentifizierung in der Domäne.	53
Aktualisieren der Knoten in der Domäne.	56
Aktivieren von Kerberos auf Informatica-Knoten.	58
Kopieren der Keytab-Dateien auf die Informatica-Knoten.	59
Aktivieren der Kerberos-Authentifizierung für Informatica-Clients.	60
Aktivieren von Kerberos für die Hadoop-Integration.	60
Aktivieren von Benutzerkonten für die Verwendung von Kerberos-Authentifizierung.	61
Importieren von Benutzerkonten aus Active Directory in LDAP-Sicherheitsdomänen.	61
Migrieren von nativen Benutzerrechten und -berechtigungen zur Kerberos-Sicherheitsdomäne.	64
Kerberos-Delegierung.	66
Arten der Kerberos-Delegierung.	66
Service for User (S4U)-Erweiterung.	66
Aktivieren der ressourcenbasierten eingeschränkten Delegierung mit S4U2Self.	67
Aktivieren der vollständigen Delegierung für die Kerberos-Prinzipalbenutzerkonten in Active Directory.	67
Wechseln von der vollständigen Delegierung zur eingeschränkten Delegierung.	68

Kapitel 5: SAML-Authentifizierung für Informatica-Webanwendungen..... 69

SAML-Authentifizierung - Übersicht.	69
Default Keystore and Truststore Directory.	70
Unterstützte Identitätsanbieter.	71
SAML-Authentifizierungsprozess.	71
Aktivieren von SAML-Authentifizierung in einer Domäne.	72
Erstellen einer LDAP-Konfiguration für den Identitäts-Provider oder LDAP-Speicher.	72
Exportieren des Assertionssignierzertifikats.	73
Importieren des Zertifikats in den für SAML-Authentifizierung verwendeten Truststore.	73

Konfigurieren des Identitäts-Providers.	73
Hinzufügen von Informatica-Webanwendungs-URLs zum Identitäts-Provider.	74
Einrichten der SAML-Authentifizierung in der Domäne.	74
Aktivieren der SAML-Authentifizierung auf den Knoten.	74
Verbesserte Authentifizierungssicherheit.	75
Anforderungssignierung.	76
Signierte Antwort.	77
Verschlüsselte Assertion.	77
Konfigurieren von Webanwendungen zur Verwendung verschiedener Identitäts-Provider.	78
Vorbereiten der Verwendung eines Identitäts-Providers.	79
Konfigurieren von Informatica Administrator zur Verwendung eines Identitäts-Providers.	79
Konfigurieren einer Informatica-Webanwendung.	81

Kapitel 6: Domänensicherheit. 83

Domänensicherheit - Übersicht.	83
Secure Communication Within the Domain.	84
Sichere Kommunikation für Dienste und den Dienstmanager.	85
Sichere Domänenkonfigurations-Repository-Datenbank.	91
Sichere PowerCenter-Repository-Datenbank.	94
Sichere Modellrepository-Datenbank.	95
Sichere Kommunikation für Arbeitsabläufe und Sitzungen.	96
Sichere Verbindungen zu einem Webanwendungsdienst.	96
Anforderungen für sichere Verbindungen zu Webanwendungsdiensten.	97
Aktivieren sicherer Verbindungen zum Administrator-Tool.	97
Informatica-Webanwendungsdienste.	98
Chiffre-Suites für die Informatica-Domäne.	100
Erstellen von Listen mit Chiffre-Suites.	101
TLS 1.3 aktivieren	103
Konfigurieren der Informatica-Domäne anhand einer neuen Gültigkeitsliste mit Chiffre-Suites	103
Sichere Quellen und Ziele.	104
Datenintegrationsdienst-Quellen und -Ziele.	104
PowerCenter-Quellen und -Ziele.	105
Secure Data Storage.	106
Sicheres Verzeichnis unter UNIX.	106
Ändern des Verschlüsselungsschlüssels über die Befehlszeile.	107
Anwendungsdienste und Ports.	110

Kapitel 7: Sicherheitsverwaltung in Informatica Administrator. 114

Verwenden von Informatica Administrator - Übersicht.	114
Benutzersicherheit.	115
Encryption.	115
Authentifizierung.	116
Autorisierung.	116

Registerkarte Sicherheit.	117
Der Suchbereich.	117
Der Sicherheits-Navigator.	118
Gruppen.	118
Benutzer.	119
Rollen.	119
Betriebssystemprofile.	120
LDAP-Konfiguration.	120
Kontoverwaltung.	120
Auditberichte.	121
Passwortverwaltung.	121
Ändern Ihres Passwortes.. . . .	122
Domänensicherheitsmanagement.	122
Sicherheitsverwaltung für Benutzer.	123
Kapitel 8: Benutzer und Gruppen.....	124
Benutzer und Gruppen - Übersicht.	124
Standardgruppen.	125
Administratorgruppe.	125
Gruppe „Jeder“.	125
Operatorgruppe.	126
Das Konzept der Benutzerkonten.	126
Standardadministrator.	126
Domänenadministrator.	126
Anwendungs-Client-Administrator.	127
Benutzer.	128
Benutzer verwalten.	128
Erstellen nativer Benutzer.	128
Allgemeine Eigenschaften der nativen Benutzer bearbeiten.	129
Zuweisen von nativen Benutzern zu nativen Gruppen.	129
Zuweisen von LDAP-Benutzern zu nativen Gruppen.	130
Aktivieren und Deaktivieren von Benutzerkonten.	130
Native Benutzer löschen.	131
LDAP-Benutzer.	131
Entsperren eines Benutzerkontos.	131
Vergrößern des Systemspeichers für eine Vielzahl von Benutzern.	132
Anzeigen von Benutzeraktivität.	133
Gruppen verwalten.	137
Hinzufügen einer nativen Gruppe.	137
Eigenschaften einer nativen Gruppe bearbeiten.	137
Eine native Gruppe in eine andere native Gruppe verschieben.	138
Eine native Gruppe löschen.	138
LDAP-Gruppen.	138

Managing operating system profiles.	138
Eigenschaften des Betriebssystemprofils für den PowerCenter-Integrationsdienst	139
Eigenschaften des Betriebssystemprofils für den Datenintegrationsdienst.	141
Eigenschaften des Betriebssystemprofils für den Metadaten-Zugriffsdienst.	143
Betriebssystemprofil erstellen.	143
Bearbeiten eines Betriebssystemprofils.	145
Zuweisen eines Standardbetriebssystemprofils zu einem Benutzer oder einer Gruppe.	145
Löschen eines Betriebssystemprofils	146
Working with Operating System Profiles in a Secure Domain.	146
Arbeiten mit Betriebssystemprofilen in einer Domäne mit Kerberos-Authentifizierung.	147
Kontosperre.	148
Konfigurieren der Kontosperre.	148
Regeln und Richtlinien für die Kontosperre.	149
Kapitel 9: Berechtigungen und Rollen.	150
Berechtigungen.	150
Berechtigungsgruppen.	151
Rollen.	152
Domänenberechtigungen.	152
Berechtigungsgruppe Sicherheitsverwaltung.	152
Berechtigungsgruppe „Domänenverwaltung“.	153
Überwachen-Berechtigungsgruppe.	158
Berechtigungsgruppe „Tools“.	159
Berechtigungsgruppe „Cloud-Verwaltung“.	160
Berechtigungen für den Analyst-Dienst.	160
Berechtigungen für den Content-Management-Dienst.	162
Datenintegrationsdienst-Berechtigungen.	162
Berechtigung für den Massenerfassungsdienst.	163
Metadata Manager Service-Berechtigungen.	163
Katalogberechtigungsgruppe.	164
Berechtigungsgruppe „Laden“.	165
Modell-Berechtigungsgruppe.	167
Sicherheitsberechtigungsgruppe.	167
Berechtigungen für den Modellrepository-Dienst.	168
PowerCenter Repository Service-Berechtigungen.	169
Tools-Berechtigungsgruppe.	170
Ordnerberechtigungsgruppe.	170
Designobjekt-Berechtigungsgruppe.	172
Quell- und Target-Berechtigungsgruppe.	174
Laufzeitobjekte-Berechtigungsgruppe.	176
Berechtigungsgruppe für globale Objekte.	180
Berechtigungen des PowerExchange Listener Service.	183
PowerExchange Logger Service-Berechtigungen.	183

Berechtigungen des Scheduler-Diensts.	184
Berechtigungen für Test Data Manager-Dienst.	185
Berechtigungsgruppe „Verwaltung“.	185
Berechtigungsgruppe für Verbindungen.	185
Datendomänen-Berechtigungsgruppe.	186
Berechtigungsgruppe für Datenmaskierung.	187
Data Subset-Berechtigungsgruppe.	187
Richtlinien-Berechtigungsgruppe.	187
Berechtigungsgruppe „Projekte“.	188
Regel-Berechtigungsgruppe.	188
Berechtigungsgruppe für Datengenerierung.	188
Verwalten von Rollen.	189
Systemdefinierte Rollen.	189
Benutzerdefinierte Rollen.	190
Benutzern und Gruppen Berechtigungen und Rollen zuweisen.	192
Geerbte Berechtigungen.	193
Einem Benutzer oder einer Gruppe Berechtigungen und Rollen über die Navigation zuweisen.	193
Benutzer mit Berechtigungen für einen Dienst anzeigen.	194
Fehlerbehebung bei Berechtigungen und Rollen.	194
Kapitel 10: Berechtigungen.	197
Berechtigungen - Übersicht.	197
Arten von Berechtigungen.	198
Berechtigungssuchfilter.	199
Domänenobjektberechtigungen.	199
Berechtigungen per Domänenobjekt.	200
Berechtigungen per Benutzern oder Gruppen.	202
Betriebssystemprofil-Berechtigungen.	202
Verbindungsberechtigungen.	204
Berechtigungstypen für Verbindungen.	204
Standardverbindungsberechtigungen.	204
Berechtigungen für eine Verbindung zuweisen.	205
Berechtigungsdetails zu einer Verbindung anzeigen.	205
Bearbeiten von Berechtigungen für eine Verbindung.	206
Berechtigungen für die Cluster-Konfiguration.	206
Anwendungs- und Anwendungsobjektberechtigungen.	207
Typen von Anwendungs- und Anwendungsobjektberechtigungen.	207
Zuweisen von Berechtigungen zu einer Anwendung oder einem Anwendungsobjekt.	207
Anzeigen von Berechtigungsdetails für eine Anwendung oder ein Anwendungsobjekt.	208
Bearbeiten von Berechtigungen für eine Anwendung oder ein Anwendungsobjekt.	208
Verweigern von Berechtigungen für eine Anwendung oder ein Anwendungsobjekt.	209
SQL-Datendienst-Berechtigungen.	209
Arten von SQL-Datendienst-Berechtigungen.	209

Berechtigungen für den SQL-Datendienst zuweisen.	210
Berechtigungsdetails zu einem SQL-Datendienst anzeigen.	210
Bearbeiten von Berechtigungen für den SQL-Datendienst.	211
Verweigern von Berechtigungen für einen SQL-Datendienst.	211
Sicherheit auf Spaltenebene.	212
Web-Dienstmodul.	213
Arten von Web-Dienst-Berechtigungen.	214
Berechtigungen für einen Web-Dienst zuweisen.	215
Berechtigungsdetails zu einem Web-Dienst anzeigen.	215
Bearbeiten von Berechtigungen für einen Web-Dienst.	215

Kapitel 11: Auditberichte. 217

Auditberichte - Übersicht.	217
Persönliche Benutzerinformationen.	218
Benutzergruppen-Zuordnung.	218
Berechtigungen.	220
Rollenzuordnung.	220
Domänenobjektberechtigung.	221
Auswählen von Benutzern für einen Auditbericht.	221
Auswählen von Gruppen für einen Auditbericht	222
Auswählen von Rollen für einen Auditbericht.	222

Anhang A: Befehlszeilenberechtigungen. 224

infacmd as Befehle.	224
infacmd cluster-Befehle.	225
infacmd dis-Befehle.	226
infacmd dp-Befehle.	228
infacmd es-Befehle.	228
infacmd ipc Befehlsprogramme.	228
infacmd isp-Befehle.	228
infacmd mas-Befehle.	238
infacmd mi-Befehle.	239
infacmd mrs Befehlsprogramme.	239
infacmd ms-Befehle.	241
infacmd tools-Befehle.	242
infacmd ps Befehlsprogramme.	242
infacmd pwx-Befehle.	243
infacmd rms-Befehle.	244
infacmd rtm Befehlsprogramme.	245
infacmd sch-Befehle.	245
infacmd sql - Befehle.	246
infacmd wfs-Befehle.	247
pmcmd-Befehle.	247

pmrep Befehlsprogramme.	250
Anhang B: Benutzerdefinierte Rollen.	256
Benutzerdefinierte Rolle für den Analyst-Dienst.	256
Benutzerdefinierte Rollen für den Metadata Manager-Dienst.	257
Benutzerdefinierte Rolle für den Operator.	259
PowerCenter-Repository-Dienst - Benutzerdefinierte Rollen.	260
Benutzerdefinierte Rollen für den Test Data Manager.	261
Index.	265

Einleitung

Das *Informatica-Sicherheitshandbuch* enthält Informationen zum Aktivieren von Sicherheit in einer Informatica-Domäne. Machen Sie sich mit der Konfiguration und Verwaltung verschiedener Authentifizierungsprotokolle vertraut, einschließlich LDAP (Lightweight Directory Access Protocol), Kerberos und SAML (Security Assertion Markup Language). Sie erhalten Informationen zum Verwalten von Benutzern und Gruppen sowie zum Verwenden von Berechtigungen, Rechten und Rollen zum Verwalten der Benutzersicherheit.

Informatica-Ressourcen

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

Informatica Network

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

Als Mitglied des Informatica Network haben Sie die folgenden Optionen:

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

Informatica-Wissensdatenbank

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

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

Informatica-Dokumentation

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

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

Informatica-Produktverfügbarkeitsmatrizen

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

Informatica Velocity

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

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

Informatica Marketplace

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

Informatica – Weltweiter Kundensupport

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

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

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

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

KAPITEL 1

Einführung in die Informatica-Sicherheit

Dieses Kapitel umfasst die folgenden Themen:

- [Übersicht über die Informatica-Sicherheit, 13](#)
- [Infrastruktur-Sicherheit, 14](#)
- [Operationssicherheit, 16](#)
- [Domänenkonfigurations-Repository, 17](#)
- [Sicherheitsdomäne, 17](#)

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 Repositories, 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.

SAML-basiertes Single Sign-On

Bei SAML (Security Assertion Markup Language) handelt es sich um ein XML-basiertes Datenformat für den Austausch von Authentifizierungs- und Autorisierungsinformationen zwischen einem Dienstanbieter und einem Identitäts-Provider. Sie können SAML-basiertes Single Sign-On für folgende Webanwendungen konfigurieren: Administrator Tool, Analyst Tool und Monitoring Tool.

In einer Informatica-Domäne fungiert die Informatica-Webanwendung als Dienstanbieter und Microsoft Active Directory Federation Services (AD FS) als Identitäts-Provider. Die Konten und Anmeldeinformationen für Benutzer der Informatica-Webanwendung werden in Microsoft Active Directory gespeichert. Sie importieren Konten aus Active Directory in eine Sicherheitsdomäne innerhalb der Informatica-Domäne. Sie müssen die Benutzerkonten in der Sicherheitsdomäne in regelmäßigen Abständen mit den Benutzerkonten im Active Directory-Verzeichnisdienst synchronisieren.

Beachten Sie, dass SAML-basiertes Single Sign-On in einer für die Verwendung von Kerberos-Authentifizierung konfigurierten Informatica-Domäne nicht aktiviert werden kann.

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 verschlüsseln 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

Sie können das Java-Keytool-Dienstprogramm zur Schlüssel- und Zertifikatsverwaltung zum Erstellen eines SSL-Zertifikats oder eines CSR (Certificate Signing Request) sowie von Schlüsselspeicherdateien und Truststore-Dateien im JKS-Format verwenden.

Das Keytool-Dienstprogramm ist im folgenden Verzeichnis auf Domänenknoten verfügbar:

```
<Informatica installation directory>\java\bin
```

Wenn die Domänenknoten auf AIX ausgeführt werden, können Sie das bereitgestellte Keytool mit dem IBM JDK zum Erstellen eines SSL-Zertifikats oder eines CSR (Certificate Signing Request) sowie von Schlüsselspeicherdateien und Truststore-Dateien verwenden.

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 `_infalInternalNamespace`. Die Sicherheitsdomäne `_infalInternalNamespace` enthält das Standard-Administrator-Benutzerkonto, das Sie während der Installation erstellen. Nach der Installation können Sie Benutzer nicht zur Sicherheitsdomäne `_infalInternalNamespace` 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, 19](#)
- [Native Benutzerauthentifizierung, 20](#)
- [LDAP-Benutzerauthentifizierung, 21](#)
- [Kerberos-Authentifizierung, 21](#)
- [SAML-Authentifizierung, 22](#)

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
- SAML-basiertes (Security Assertion Markup Language) Single Sign-On

Native Benutzerkonten werden in der Informatica-Domäne gespeichert und können nur innerhalb der Informatica-Domäne verwendet werden.

LDAP- und Kerberos-Benutzerkonten werden in einem LDAP-Verzeichnisdienst gespeichert und von Anwendungen innerhalb des Unternehmens gemeinsam verwendet.

SAML-basiertes Single Sign-On authentifiziert Benutzer anhand von Kontoanmeldedaten, die in Microsoft Active Directory gespeichert sind. Konten werden aus Active Directory in eine Sicherheitsdomäne innerhalb der Informatica-Domäne importiert.

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-Schlüsselverteilungszentrum (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.

Sie können SAML-basiertes Single Sign-On für Informatica-Webanwendungen vor oder nach der Installation aktivieren. Sie müssen jedoch alle erforderlichen Einrichtungsaufgaben abschließen, bevor SAML-basiertes Single Sign-On aktiviert werden kann. SAML-basiertes Single Sign-On kann in einer für die Verwendung von Kerberos-Authentifizierung konfigurierten Informatica-Domäne nicht aktiviert werden kann.

Wenn sich die Informatica-Domäne lokal und nicht auf einer AWS EC2-Instanz befindet, können Sie das EMRFS-Authentifizierungsprotokoll nicht in Integration mit Amazon EMR verwenden.

Sie können das Token für Benutzeranmeldedaten mit dem eindeutigen Site-Schlüssel verschlüsseln. Um das Token für Benutzeranmeldedaten zu verschlüsseln, legen Sie die Umgebungsvariable `infaEnableAdvancedEncryptionSchemeForCredential` auf `True` fest. Bei der nativen und der LDAP-Benutzerauthentifizierung wird nach erfolgreicher Benutzerauthentifizierung das verschlüsselte Anmeldedatentoken anstelle des Benutzerpassworts verwendet.

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 eine Informatica-Domäne konfigurieren, um Benutzern in einem LDAP-Verzeichnisdienst die Anmeldung bei Informatica-Client-Anwendungen zu ermöglichen. Sie können mehrere LDAP-Konfigurationen für eine Domäne erstellen, wobei mit jeder Konfiguration eine Verbindung zu einem anderen LDAP-Server hergestellt wird. Eine Domäne kann 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.

Sie können eine Informatica-Domäne zur Verwendung von bereichsübergreifender Kerberos-Authentifizierung konfigurieren. Mit der bereichsübergreifenden Kerberos-Authentifizierung können sich Informatica-Clients, die zu einem Kerberos-Bereich gehören, bei Knoten und Anwendungsdiensten authentifizieren, die zu einem anderen Kerberos-Bereich gehören.

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.

SAML-Authentifizierung

Sie können eine Informatica-Domäne so konfigurieren, dass Benutzer die SAML-Authentifizierung (Security Assertion Markup Language) zum Anmelden bei den folgenden Webanwendungen verwenden können: Administrator Tool, Analyst Tool, Massenerfassungstool, Metadaten-Manager und Monitoring Tool. Sie können eine Informatica-Domäne auch für die Verwendung von SAML-Authentifizierung mit Informatica Developer (dem Developer Tool) konfigurieren.

Bei SAML (Security Assertion Markup Language) handelt es sich um ein XML-basiertes Datenformat für den Austausch von Authentifizierungs- und Autorisierungsinformationen zwischen einem Dienstanbieter und einem Identitäts-Provider.

SAML-Authentifizierung für Informatica-Webanwendungen

In einer Informatica-Domäne fungiert die Informatica-Webanwendung als Dienstanbieter. Microsoft Active Directory Federation Services (ADFS) dient als Identitäts-Provider, der Webanwendungsbenutzer mit dem Active Directory-Identitätsspeicher Ihres Unternehmens authentifiziert.

Damit die Informatica-Domäne SAML-basiertes Single Sign-On verwenden kann, müssen Sie eine LDAP-Sicherheitsdomäne für Benutzerkonten der Informatica-Webanwendung erstellen und die Benutzer dann aus Active Directory in die Domäne importieren. Sie können das Administrator Tool verwenden, um die Verbindung zum Active Directory-Server einzurichten, und Benutzer dann in die Sicherheitsdomäne importieren.

Wenn sich ein Benutzer an einer Informatica-Webanwendung anmeldet, sendet die Anwendung eine SAML-Authentifizierungsanfrage an ADFS. ADFS authentifiziert die Anmeldedaten des Benutzers anhand der Benutzerkontendaten in Active Directory und gibt dann ein SAML-Assertionstoken mit sicherheitsrelevanten Informationen über den Benutzer an die Webanwendung zurück.

Sie konfigurieren ADFS zur Ausgabe von SAML-Token, die zum Authentifizieren von Benutzern der Informatica-Webanwendung dienen. Sie müssen auch das Assertionssignaturzertifikat des Identitäts-Providers aus ADFS exportieren und das Zertifikat anschließend in die Truststore-Standarddatei von Informatica auf allen Gateway-Knoten in der Domäne importieren.

SAML-Authentifizierung für Informatica Developer

Sie können SAML-Authentifizierung in Informatica Developer (dem Developer Tool) aktivieren.

Aktivieren Sie zur Verwendung von SAML-Authentifizierung das folgende Flag in der Datei „developerCore.ini“:

```
-DsamlAuthenticationEnabled=true
```

Sie finden die Datei „developerCore.ini“ in folgendem Verzeichnis: <Informatica-Installationsverzeichnis>\clients\DeveloperClient

Sie müssen auch das Assertionssignaturzertifikat des Identitäts-Providers aus dem SAML-Provider exportieren und dann das Zertifikat in die Truststore-Standarddatei von Informatica im Developer Tool importieren.

SAML-Authentifizierungsmodi

Sie können einen Benutzer in einer SAML-fähigen Domäne in einem der folgenden Modi authentifizieren:

Benutzername und Passwort

Verwendet die Anmeldeinformationen des Benutzers.

Fügen Sie der Datei „developerCore.ini“ folgende Eigenschaft hinzu:

```
-DkerberosLoginType=TYPE_USER_PWD
```

Schlüsseltabelle

Verwendet die Schlüsseltabelle, die für den Benutzer im SAML-Provider generiert wurde. Wählen Sie den SAML-konfigurierten Namespace aus, wenn Sie das Developer Tool mit dem Modellrepository verbinden.

Fügen Sie der Datei „developerCore.ini“ folgende Eigenschaften hinzu:

```
-DkerberosLoginType=TYPE_KEYTAB
```

```
-DkerberosAuthSPN=<SPN value generated from the SAML provider for the user>
```

```
-DkerberosAuthKeytab=<Location of the keytab file generated from the SAML provider  
for the user>
```

Angemeldete Benutzer

Verwendet die Anmeldeinformationen des Benutzers, um sich bei dem Computer anzumelden, auf dem das Developer Tool installiert ist. Wählen Sie den SAML-konfigurierten Namespace aus, wenn Sie das Developer Tool mit dem Modellrepository verbinden.

Fügen Sie der Datei „developerCore.ini“ folgende Eigenschaft hinzu:

```
-DkerberosLoginType=TYPE_LOGGED_IN_USER
```

KAPITEL 3

LDAP-Authentifizierung

Dieses Kapitel umfasst die folgenden Themen:

- [Übersicht, 24](#)
- [LDAP-Sicherheitsdomänen, 25](#)
- [Synchronisierung des Benutzerkontos, 25](#)
- [LDAP-Verzeichnisdienste, 25](#)
- [Azure Active Directory für eine sichere LDAP-Authentifizierung, 26](#)
- [Erstellen einer LDAP-Konfiguration, 27](#)
- [Löschen einer LDAP-Konfiguration, 33](#)

Übersicht

Sie können eine Informatica-Domäne konfigurieren, damit sich Benutzer, die aus einem oder mehreren LDAP-Verzeichnisdiensten importiert wurden, bei Informatica-Knoten, -Diensten und -Anwendungs-Clients wie Informatica Developer und Informatica Analyst anmelden können.

Ein LDAP-Verzeichnisdienst speichert die Benutzernamen und Passwörter für die Konten. Die Verwendung der LDAP-Authentifizierung ermöglicht es Ihnen, die Anmeldeinformationen für alle Ihre Informatica-Benutzer in einem einzigen Identitätsspeicher zu konsolidieren, was das Erstellen und Aktualisieren von Kontoanmeldeinformationen vereinfacht.

Sie können die native Authentifizierung und die LDAP-Authentifizierung zusammen in einer Informatica-Domäne verwenden. Der Dienstmanager, der auf dem Master-Gateway-Knoten innerhalb der Domäne ausgeführt wird, authentifiziert Benutzer basierend auf der Sicherheitsdomäne, zu der die Benutzer gehören. Wenn ein Benutzer zur standardmäßigen nativen Sicherheitsdomäne gehört, authentifiziert der Dienstmanager den Benutzer anhand der Kontoinformationen im Domänenkonfigurations-Repository. Wenn der Benutzer zu einer LDAP-Sicherheitsdomäne gehört, übergibt der Dienstmanager die Benutzeranmeldedaten zur Authentifizierung an den LDAP-Server.

LDAP-Sicherheitsdomänen

Eine LDAP-Sicherheitsdomäne enthält Benutzer und Gruppen, die aus einem LDAP-Verzeichnisdienst importiert werden. Sie können innerhalb einer Informatica-Domäne mehrere LDAP-Sicherheitsdomänen definieren. Sie können dann Konten aus LDAP-Verzeichnisdiensten in die Sicherheitsdomänen importieren.

Sie müssen eine LDAP-Sicherheitsdomäne erstellen, wenn Sie eine Informatica-Domäne zur Verwendung der Kerberos-Authentifizierung konfigurieren. 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.

Wenn Sie eine LDAP-Sicherheitsdomäne erstellen, konfigurieren Sie Suchbasen und Filter, die den Satz von LDAP-Benutzerkonten und -Gruppen definieren, die in die Sicherheitsdomäne aufgenommen werden sollen. Der Dienstmanager verwendet die Konfiguration der Sicherheitsdomäne, um Benutzer und Gruppen in der Sicherheitsdomäne in Benutzer und Gruppen im LDAP-Verzeichnisdienst zu importieren bzw. mit diesen zu synchronisieren.

Der Dienstmanager verwendet beim Importieren oder Synchronisieren von Benutzern und Gruppen innerhalb einer LDAP-Sicherheitsdomäne die folgenden Kriterien:

- Der Dienstmanager verwendet die Benutzersuchbasen und Filter zum Importieren von Benutzerkonten.
- Der Dienstmanager verwendet die Gruppensuchbasen und Filter zum Importieren von Gruppen.
- Der Dienstmanager importiert die Gruppen, die im Gruppenfilter enthalten sind, und die Benutzerkonten, die im Benutzerfilter enthalten sind.

Synchronisierung des Benutzerkontos

Der Dienstmanager aktualisiert die Sicherheitsdomäne mit den Benutzern und Gruppen in einem LDAP-Verzeichnisdienst anhand eines Zeitplans. Sie können den Synchronisationszeitplan festlegen, wenn Sie die LDAP-Authentifizierung konfigurieren.

Der Dienstmanager führt während der Synchronisierung die folgenden Schritte aus:

- Es ruft eine aktualisierte Liste der Benutzer und Gruppen aus dem LDAP-Verzeichnisdienst ab. Dabei verwendet er die Suchbasis und Filter, die Sie für die Sicherheitsdomäne konfiguriert haben.
- Er aktualisiert die Liste der LDAP-Benutzer und -Gruppen in der Sicherheitsdomäne. Wenn ein LDAP-Benutzer in der Sicherheitsdomäne im LDAP-Verzeichnisdienst gelöscht wurde, überträgt der Dienstmanager die Eigentümerschaft der Benutzerobjekte an das Domänenadministratorkonto.

LDAP-Verzeichnisdienste

Sie können Benutzerkonten aus LDAP-Verzeichnisdiensten in Informatica-Sicherheitsdomänen importieren.

Sie können Benutzer aus den folgenden LDAP-Verzeichnisdiensten importieren:

- IBM Tivoli-Verzeichnisserver
- Microsoft Active Directory
- Microsoft Azure Active Directory

- Novell eDirectory
- OpenLDAP
- Oracle Directory Server (ODSEE)
- Oracle Unified Directory (OUD)
- Sun Java System-Verzeichnisserver

Hinweis: Wenn Sie Kerberos-Authentifizierung verwenden, können ausschließlich Benutzer aus Microsoft Active Directory importiert werden.

Der Dienstmanager benötigt eine bestimmte eindeutige ID (UID, Unique ID) zur Angabe von Benutzern in jedem LDAP-Verzeichnisdienst. In der folgenden Tabelle wird die Standard-UID für jeden LDAP-Verzeichnisdienst aufgelistet:

LDAP-Verzeichnisdienst	UID
IBM Tivoli-Verzeichnisserver	uid
Microsoft Active Directory	sAMAccountName
Microsoft Azure Active Directory	UserPrincipalName
Novell eDirectory	uid
OpenLDAP	uid
Oracle Directory Server (ODSEE)	uid
Oracle Unified Directory (OUD)	uid
Sun Java System-Verzeichnisserver	uid

Azure Active Directory für eine sichere LDAP-Authentifizierung

Sie können Benutzer von einem Azure Active Directory (Azure AD) in eine LDAP-Sicherheitsdomäne importieren.

Die Azure Active Directory-Domänendienste bieten eine sichere öffentliche LDAP-IP-Adresse für den Import von Benutzerkonten von Azure Active Directory in eine LDAP-Sicherheitsdomäne. Benutzer, die Sie importieren, können sich mit ihren LDAP-Anmeldeinformationen bei Informatica-Knoten, -Dienstern und -Anwendungen anmelden, die auf virtuellen Maschinen in einer von Azure Active Directory verwalteten Domäne ausgeführt werden.

Unterstützte Versionen von Active Directory finden Sie in der Produktverfügbarkeitsmatrix auf Informatica Network: <https://network.informatica.com/community/informatica-network/product-availability-matrices>.

Sie müssen die Authentifizierung per Secure Lightweight Directory Access Protocol (sicheres LDAP) in Azure Active Directory Domain Services aktivieren, um die Informatica-Benutzer zu authentifizieren.

Sie können die folgenden Artikel in der Informatica-Ratgeber-Bibliothek lesen, um eine End-to-End-Ansicht des Prozesses zur Verwendung der LDAP-Authentifizierung mit Active Directory zu erhalten:

- [Enabling SAML Authentication with Active Directory Federation Services in Informatica 10.4.0](#)
- [Enabling SAML Authentication with Azure Active Directory for Web Applications](#)

Vorbereiten des Imports von Active Directory-Benutzerkonten

Führen Sie die folgenden Schritte aus, um den Import von Benutzerkonten aus Azure Active Directory in eine Informatica-Domäne vorzubereiten:

1. Vergewissern Sie sich, dass Port 636, der sichere LDAP-Port von Azure Active Directory, über Ihre Firewall zugänglich ist.
2. Aktivieren Sie die sichere LDAP-Authentifizierung in den Azure Active Directory-Domänendiensten.
Mit dem Azure-Portal können Sie die sichere LDAP-Authentifizierung in den Azure Active Directory-Domänendiensten verwenden. Informationen über das Konfigurieren des sicheren LDAP in den Azure Active Directory-Domänendiensten finden Sie unter folgendem Link:
<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-admin-guide-configure-secure-ldap>
3. Stellen Sie beim Konfigurieren des sicheren LDAP-Zertifikats in Azure Active Directory Domain Services sicher, dass der Subjektnamen auf dem Zertifikat der vollqualifizierte Domänenname (FQDN) von Azure Active Directory ist.
4. Konvertieren Sie das sichere LDAP-Zertifikat vom PFX- in das PEM-Format. Java erfordert, dass das Zertifikat im PEM-Format vorliegt.
5. Importieren Sie die Zertifikate, die von allen Domänenknoten verwendet werden, in die Java-TrustStore-Datei `cacerts`, die sich auf einem einzelnen Gateway-Knoten in der Domäne in folgendem Verzeichnis befindet:

```
<Informatica-Installationsverzeichnis>/java/jre/lib/security/
```
6. Kopieren Sie die Datei `cacerts`, die die importierten Zertifikate enthält, auf jedem anderen Gateway-Knoten in der Domäne in dasselbe Verzeichnis.
7. Fügen Sie die öffentliche IP-Adresse und den vollqualifizierten Domännennamen (FQDN) des Azure Active Directory zur Datei „`/etc/hosts`“ auf jedem Gateway-Knoten in der Domäne hinzu. Verwenden Sie das folgende Format:

```
<Host-IP-Adresse des Azure Active Directory> ldaps.<FQDN des Azure Active Directory>
```

Erstellen einer LDAP-Konfiguration

Sie können eine oder mehrere LDAP-Konfigurationen erstellen, damit aus LDAP-Verzeichnisdiensten importierte Benutzerkonten oder -gruppen sich mit einer Informatica-Domäne authentifizieren können.

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

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 zuordnen, um die Konten anhand ihrer Rollen in der Informatica-Domäne zu verwalten.

Sie können das Administrator Tool nicht verwenden, um Benutzer und Gruppen in einer LDAP-Sicherheitsdomäne zu erstellen, zu bearbeiten oder zu löschen. Sie müssen Änderungen an LDAP-Benutzern und -Gruppen im LDAP-Verzeichnisdienst vornehmen und die LDAP-Sicherheitsdomäne anschließend mit dem LDAP-Verzeichnisdienst synchronisieren.

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

Führen Sie zum Erstellen einer LDAP-Konfiguration die folgenden Schritte aus:

1. Konfigurieren Sie die Verbindung zum LDAP-Server, der den Verzeichnisdienst enthält, aus dem Sie Benutzerkonten und -gruppen importieren möchten.
2. Erstellen Sie eine LDAP-Sicherheitsdomäne für jeden Satz von Benutzerkonten und -gruppen, die Sie aus dem LDAP-Verzeichnisdienst importieren möchten.
3. Richten Sie einen Zeitplan für den Dienstmanager ein, um die LDAP-Sicherheitsdomänen mit neuen oder geänderten Benutzern und Gruppen im LDAP-Verzeichnisdienst zu aktualisieren.

Erstellen der LDAP-Konfiguration und Konfigurieren der LDAP-Serververbindung

Erstellen Sie die LDAP-Konfiguration und konfigurieren Sie die Verbindung zum LDAP-Server, der den Verzeichnisdienst enthält, aus dem Sie die Benutzerkonten 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 SSL auf dem LDAP-Server verwendet wird, müssen Sie das Zertifikat, das von jedem Domänenknoten verwendet wird, auf einer Gateway-Knotendomäne in die Truststore-Datei `cacerts` importieren. Sie kopieren dann die Datei `cacerts` mit den importierten Zertifikaten in dasselbe Verzeichnis auf jedem Knoten in der Domäne. Weitere Informationen hierzu finden Sie unter [“Ein selbstsigniertes SSL-Zertifikat verwenden” auf Seite 32](#).

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 die Registerkarte **LDAP-Konfiguration**.
3. Klicken Sie auf das Menü **Aktionen** und wählen Sie **LDAP-Konfiguration erstellen** aus.
4. Klicken Sie im Dialogfeld **LDAP-Konfiguration erstellen** auf die Registerkarte **LDAP-Konnektivität**.
5. Konfigurieren Sie die Verbindungseigenschaften für den LDAP-Server.

Möglicherweise müssen Sie den LDAP-Administrator konsultieren, um die benötigten Informationen für die Verbindung zum LDAP-Server zu erhalten.

Die folgende Tabelle beschreibt die LDAP-Konfigurationseigenschaften:

Eigenschaft	Beschreibung
Name der LDAP-Konfiguration	Name der LDAP-Konfiguration.
Servename	Hostname oder IP-Adresse des Computers, auf dem der LDAP-Verzeichnisdienst gehostet wird.
Port	Listenerport für den LDAP-Server. Dies ist die Portnummer für die Kommunikation mit dem LDAP-Verzeichnisdienst. In der Regel weist der LDAP-Server die Portnummer 389 auf. Wenn der LDAP-Server SSL nutzt, ist die Portnummer 636. Die maximale Portnummer ist 65535.
LDAP-Verzeichnisdienst	Typ des LDAP-Verzeichnisdiensts. 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 allgemeinen Namen (Common Name, CN), einer Organisation (Organization, O) und einem Land (Country, 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. Um eine Verbindung zu Azure Active Directory herzustellen, geben Sie den Namen des Benutzerprinzips (UPN) für den Prinzipal-Benutzer an.
Passwort	Passwort für den Prinzipal-Benutzer. Für anonyme Anmeldung leer lassen.
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.
Ohne Beachtung der Groß-/Kleinschreibung	Gibt an, dass der Dienstmanager bei der Zuweisung von Benutzern zu Gruppen die Groß- und Kleinschreibung bei DN-Attributen ignorieren muss.
Gruppenmitgliedschaft sattribut	Name des Attributs, das 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 <i>member</i> oder <i>memberof</i> .
Maximale Größe	Maximale Anzahl an Benutzerkonten zum Importieren in eine Sicherheitsdomäne. Beispiel: Wenn der Wert auf 100 gesetzt ist, können Sie maximal 100 Benutzerkonten in die Sicherheitsdomäne importieren. Wenn die Anzahl der zu importierenden Benutzer 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 importieren müssen. Standardwert ist „1000“.

- Klicken Sie auf **Verbindung testen**, um sicherzustellen, dass die Verbindung zum LDAP-Server gültig ist.
- Klicken Sie zum Speichern der LDAP-Konfiguration auf **OK**.

Konfigurieren der Sicherheitsdomäne

Erstellen Sie eine LDAP-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.

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. Beachten Sie, dass im Gegensatz zu nativen Benutzernamen bei LDAP-Benutzernamen zwischen Groß- und Kleinschreibung unterschieden wird.

Der Service Manager verwendet die Benutzersuchbasen und Filter zum Importieren von Benutzern und die Gruppensuchbasen zum Importieren von Gruppen. Der Dienstmanager verwendet die Filter, um Gruppen und die Liste der zu jeder Gruppe gehörenden Benutzer zu importieren.

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 dann **LDAP-Konfiguration** aus.
3. Klicken Sie im Dialogfeld **LDAP-Konfiguration** auf die Registerkarte **Sicherheitsdomänen**.
4. Klicken Sie auf **Hinzufügen**.

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

Eigenschaft	Beschreibung
Sicherheitsdomäne	Name der LDAP-Sicherheitsdomäne. Der Name unterliegt nicht der Groß-/ Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die Zeichenfolge darf maximal 128 Zeichen umfassen und keines der 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. Bei der Suche wird ein Objekt im Verzeichnis anhand des Pfads im Distinguished Name des Objekts gefunden. Beispiel: In Microsoft Active Directory könnte der Distinguished Name des Benutzers cn=UserName,ou=OrganizationalUnit,dc=DomainName lauten, wobei die Reihe der durch dc=DomainName benannten relativen Distinguished Names die DNS-Domäne des Objekts kennzeichnet.

Eigenschaft	Beschreibung
Benutzerfilter	<p>Eine LDAP-Abfragezeichenfolge, mit der die Kriterien für die Suche nach Benutzern im Verzeichnisdienst festgelegt wird. Der Filter kann Attributtypen, Assertionswerte und Abgleichkriterien angeben.</p> <p>Beispiel: <code>(objectclass=*)</code> sucht nach allen Objekten. <code>(&(objectClass=user)(!(cn=susan)))</code> sucht nach allen Benutzerobjekten mit Ausnahme von „susan“.</p> <p>Weitere Informationen zu Suchfiltern finden Sie in der Dokumentation für den LDAP-Verzeichnisdienst.</p>
Gruppensuchbasis	Distinguished Name (DN) des Eintrags, der als Ausgangspunkt für die Suche nach Gruppennamen im LDAP-Verzeichnisdienst dient.
Gruppenfilter	Eine LDAP-Abfragezeichenfolge, mit der die Kriterien für die Suche nach Gruppen im Verzeichnisdienst festgelegt wird.

- 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.
- 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.
- Klicken Sie zum Speichern der Sicherheitsdomäne auf **OK**.

Konfigurieren des Synchronisationszeitplans

Sie können einen Tagesplan für den Dienstmanager einrichten, um die LDAP-Sicherheitsdomänen mit neuen oder geänderten Benutzern und Gruppen im LDAP-Verzeichnisdienst zu aktualisieren.

Wenn der Dienstmanager die LDAP-Sicherheitsdomänen mit dem LDAP-Verzeichnisdienst synchronisiert, importiert er alle Benutzer, die mit den Benutzerfiltereinstellungen übereinstimmen, vom LDAP-Verzeichnisdienst in die Sicherheitsdomäne. Der Service Manager importiert dann alle Gruppen, die den Gruppenfiltereinstellungen entsprechen, und ordnet die Benutzer den entsprechenden Gruppen zu. Der Dienstmanager löscht auch alle Benutzer oder Gruppen, die nicht im LDAP-Verzeichnisdienst gefunden wurden, aus der Sicherheitsdomäne.

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 korrekt ist, planen Sie, wann der Dienstmanager die LDAP-Sicherheitsdomänen mit dem LDAP-Verzeichnisdienst synchronisiert. Der Dienstmanager synchronisiert die LDAP-Sicherheitsdomänen mit dem LDAP-Verzeichnisdienst jeden Tag zu den von Ihnen festgelegten Zeiten.

Um sicherzustellen, dass die Synchronisierung erfolgreich ist, beachten Sie die folgenden Empfehlungen, bevor Sie den Synchronisationszeitplan einrichten:

Vergewissern Sie sich, dass die Datei „/etc/hosts“ einen Eintrag für den LDAP-Server enthält.

Stellen Sie sicher, dass die Datei `/etc/hosts` auf jedem Gateway-Knoten in der Domäne einen Eintrag mit dem Hostnamen und der IP-Adresse des LDAP-Servers enthält. Wenn der Dienstmanager den Hostnamen für den LDAP-Server nicht auflösen kann, kann die Synchronisierung fehlschlagen.

Aktivieren Sie das Paging in LDAP, wenn Sie mehr als 100 Benutzer oder Gruppen synchronisieren.

Aktivieren Sie das Paging auf dem LDAP-Verzeichnisdienst, bevor Sie mehr als 100 Benutzer oder Gruppen synchronisieren. Wenn Sie das Paging für den LDAP-Verzeichnisdienst nicht aktivieren, kann die Synchronisierung fehlschlagen.

Synchronisieren Sie Sicherheitsdomänen in Zeiten, in denen die meisten Benutzer nicht bei Informatica-Anwendungen angemeldet sind.

Während der Synchronisation sperrt der Service Manager jedes Benutzerkonto, das er synchronisiert. Benutzer sind möglicherweise nicht in der Lage, sich während der Synchronisierung bei den Informatica-Anwendungs-Clients anzumelden. Benutzer, die sich während des Startens der Synchronisierung bei einem Anwendungs-Client angemeldet haben, können bestimmte Aufgaben möglicherweise nicht ausführen.

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.
5. Um die Benutzer und Gruppen in den LDAP-Sicherheitsdomänen sofort mit den Benutzern und Gruppen im LDAP-Verzeichnisdienst zu synchronisieren, klicken Sie auf **Jetzt synchronisieren**.
6. Klicken Sie zum Speichern des Synchronisationszeitplans auf **OK**.

Hinweis: Warten Sie, bis der Dienstmanager mit dem LDAP-Verzeichnisdienst synchronisiert wurde, bevor Sie die Informatica-Domäne neu starten, um zu vermeiden, dass die Synchronisationszeiten verloren gehen, die Sie im Zeitplan festgelegt haben.

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.

Um eine Verbindung zu einem LDAP-Server herzustellen, der ein SSL-Zertifikat verwendet, importieren Sie mit dem Java-Keytool-Schlüssel- und Zertifikatsverwaltungsdienstprogramm die Zertifikate, die von allen Domänenknoten verwendet werden, auf einem einzelnen Gateway-Knoten in der Domäne in die Java-TrustStore-Datei `cacerts`. Kopieren Sie dann die KeyStore-Datei `cacerts` mit den importierten Zertifikaten in die anderen Knoten in der Domäne.

Die Truststore-Datei `cacerts` befindet sich auf allen Knoten in folgendem Verzeichnis:

```
<Informatica installation directory>\java\jre\lib\security
```

Das Keytool-Dienstprogramm ist in folgendem Verzeichnis auf allen Knoten verfügbar:

```
<Informatica installation directory>\java\bin
```

Starten Sie den Knoten neu, nachdem Sie das Zertifikat importiert haben.

Löschen einer LDAP-Konfiguration

Sie können eine LDAP-Konfiguration und die zugehörigen Sicherheitsdomänen löschen, um Benutzern dauerhaft den Zugriff auf die Domäne zu verweigern.

Um eine LDAP-Konfiguration zu löschen, müssen zuerst die mit der LDAP-Konfiguration verknüpften Sicherheitsdomänen gelöscht werden. Der Dienstmanager löscht alle Benutzerkonten und -gruppen in allen gelöschten LDAP-Sicherheitsdomänen aus der Domänenkonfigurationsdatenbank.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Sicherheit**.
2. Klicken Sie auf die Registerkarte **LDAP-Konfiguration**.
3. Klicken Sie auf die Registerkarte **Sicherheitsdomänen** und dann auf die Schaltfläche **Bearbeiten**.
4. Wählen Sie eine Sicherheitsdomäne im Dialogfeld **LDAP-Konfiguration bearbeiten** aus und klicken Sie dann auf **Löschen**.
5. Wählen Sie die zu löschende LDAP-Konfiguration im Navigator der LDAP-Konfiguration aus.
6. Klicken Sie auf das Menü **Aktionen** und wählen Sie dann **LDAP-Konfiguration löschen** aus.
7. Klicken Sie auf **OK**, um den Vorgang zum Löschen der LDAP-Konfiguration zu bestätigen.

KAPITEL 4

Kerberos-Authentifizierung

Dieses Kapitel umfasst die folgenden Themen:

- [Überblick über Kerberos, 34](#)
- [Funktionsweise von Kerberos in einer Informatica-Domäne, 35](#)
- [Bereichsübergreifende Kerberos-Authentifizierung, 37](#)
- [Vorbereiten der Aktivierung der Kerberos-Authentifizierung, 39](#)
- [Aktivieren der Kerberos-Authentifizierung, 53](#)
- [Aktivieren von Kerberos auf Informatica-Knoten, 58](#)
- [Aktivieren von Kerberos für die Hadoop-Integration, 60](#)
- [Aktivieren von Benutzerkonten für die Verwendung von Kerberos-Authentifizierung, 61](#)
- [Kerberos-Delegierung, 66](#)

Überblick über Kerberos

Kerberos ist ein Authentifizierungsprotokoll für Computernetzwerke, mit dem Informatica-Clients, -Knoten und -Dienste, die über ein Netzwerk miteinander kommunizieren, eine sichere Verbindung untereinander herstellen können.

Durch Kerberos-Authentifizierung entfallen native Informatica-Konten, und es ist nicht mehr erforderlich, dass die Domäne Benutzeranmeldedaten an einen LDAP-Server weitergibt. Nachdem Sie Kerberos-Authentifizierung in einer Domäne aktiviert haben, verwenden Informatica-Clients die Kerberos-Tickets, die während des Windows-Authentifizierungsprozesses erstellt wurden, um sich bei den in der Domäne ausgeführten Informatica-Diensten anzumelden.

Sie können Kerberos-Authentifizierung in einer Domäne aktivieren, die auf einem Windows-Netzwerk ausgeführt wird. Das Netzwerk muss Microsoft Active Directory-Domänendienste (AD DS) als Kerberos-Prinzipaldatenbank verwenden.

Um Kerberos-Authentifizierung in einer Informatica-Domäne zu aktivieren, führen Sie die folgenden Schritte aus:

Bereiten Sie die Aktivierung der Kerberos-Authentifizierung vor.

Sie müssen mehrere Aufgaben ausführen, bevor Sie die Kerberos-Authentifizierung aktivieren. Zu den Aufgaben, die Sie ausführen müssen, zählen die Folgenden:

- Erstellen Sie die Kerberos-Konfigurationsdatei.
- Erstellen Sie Konten für Kerberos-Prinzipalbenutzer in Active Directory.

- Generieren Sie die Formate für den Dienstprinzipalnamen (SPN) und Keytab.
- Erstellen Sie die Keytab-Dateien, die zum Authentifizieren von Benutzern und Diensten im Netzwerk verwendet werden.

Aktivieren Sie Kerberos-Authentifizierung in der Informatica-Domäne.

Sie können Kerberos-Authentifizierung in einer Informatica-Domäne während oder nach der Installation der Informatica-Dienste aktivieren. Wenn Sie Kerberos-Authentifizierung nicht während der Installation aktivieren, können Sie die Informatica-Befehlszeilenprogramme verwenden, um die Domäne zur Verwendung von Kerberos-Authentifizierung zu konfigurieren.

Aktivieren Sie Kerberos-Authentifizierung auf Informatica-Knoten und Clienthosts.

Nachdem Sie Kerberos in der Domäne aktiviert haben, kopieren Sie die Kerberos-Konfigurationsdatei auf jeden Knoten in der Domäne und auf jeden Informatica-Clienthost. Außerdem konfigurieren Sie die Webbrowser für den Zugriff auf Informatica-Webanwendungen.

Aktivieren Sie Informatica-Benutzer für die Verwendung von Kerberos-Authentifizierung.

Nachdem Sie Kerberos-Authentifizierung aktiviert haben, importieren Sie Informatica-Benutzer aus Active Directory in eine LDAP-Sicherheitsdomäne, die die Kerberos-Benutzerkonten enthält. Sie müssen auch die Gruppen, Rollen, Rechte und Berechtigungen der nativen Benutzerkonten auf die Benutzerkonten in der LDAP-Sicherheitsdomäne migrieren.

Funktionsweise von Kerberos in einer Informatica-Domäne

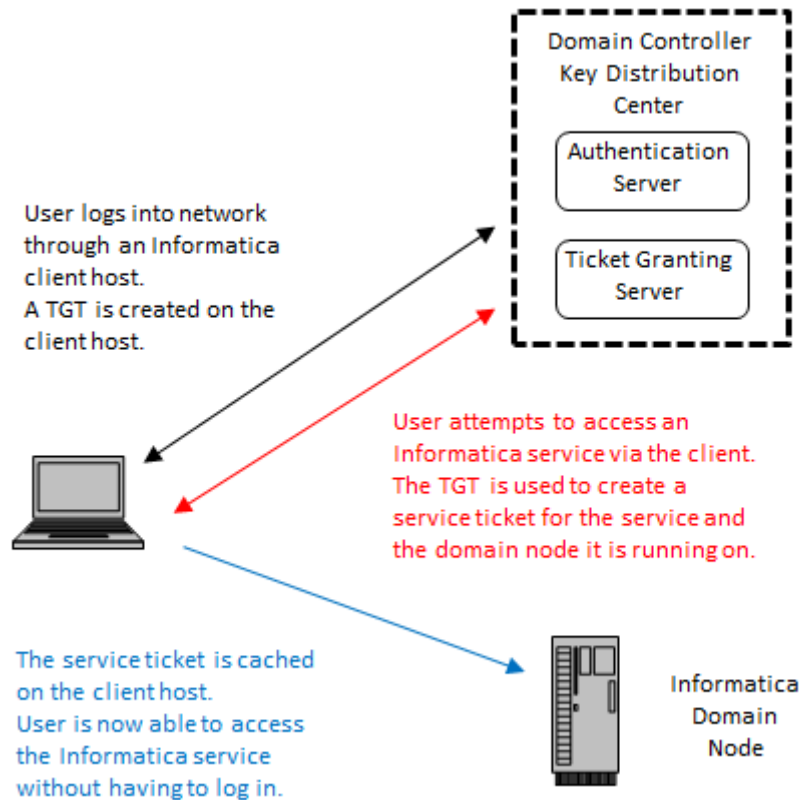
In einer Domäne, die zur Verwendung der Kerberos-Authentifizierung konfiguriert ist, authentifizieren sich die Informatica-Clients bei Knoten und Anwendungsdiensten innerhalb der Domäne, ohne Passwörter zu benötigen.

In einer Domäne mit Kerberos-Authentifizierung handelt es sich bei den innerhalb der Domäne ausgeführten Diensten, wie z. B. Knotenprozessen, Dienstanwendungsprozessen und Informatica-Anwendungsdiensten, um Kerberos-*Prinzipale*. Die vom Kerberos-Bereich verwendete Active Directory-Prinzipaldatenbank enthält ein Benutzerkonto für jeden Prinzipal.

Das Kerberos-Authentifizierungsprotokoll verwendet *keytabs*, um Informatica-Clients bei Diensten zu authentifizieren, die innerhalb der Domäne ausgeführt werden. Die Keytab-Datei für einen Prinzipal wird auf dem Knoten gespeichert, auf dem der Dienst ausgeführt wird. Die Keytab-Datei enthält den *Dienstprinzipalnamen (SPN, Service Principal Name)*, der den Dienst innerhalb des Kerberos-Bereichs identifiziert, sowie den Schlüssel, der dem SPN in Active Directory zugewiesen ist.

Wenn das KDC ein Dienstticket an einen Client ausgibt, verschlüsselt es das Ticket mit dem Schlüssel, der dem SPN zugewiesen ist. Der angeforderte Dienst verwendet den Schlüssel zum Entschlüsseln des Diensttickets.

Die folgende Abbildung zeigt den grundlegenden Ablauf für Kerberos-Authentifizierung:



Der folgende Überblick beschreibt den grundlegenden Ablauf für Kerberos-Authentifizierung:

1. Ein Informatica-Clientbenutzer meldet sich bei einem Netzwerkcomputer an, der einen Informatica-Client hostet.
2. Die Anmeldeanforderung wird an den *Authentifizierungsserver*, eine Komponente des *Kerberos-Schlüsselverteilungscenters (Key Distribution Center, KDC)*, weitergeleitet. Das KDC ist ein Netzwerkdienst mit Zugriff auf Benutzerkonteninformationen, der auf jedem Domänencontroller innerhalb der Active Directory-Domäne ausgeführt wird.
3. Der Authentifizierungsserver verifiziert, dass der Benutzer in der Prinzipaldatenbank vorhanden ist, und erstellt dann einen Kerberos-Token, der als *Ticket-Granting-Ticket (TGT)* bezeichnet wird, auf dem Computer des Benutzers.
4. Der Benutzer versucht, auf einen Prozess oder Dienst innerhalb der Informatica-Domäne über einen Informatica-Client zuzugreifen.
5. Informatica und die Kerberos-Bibliotheken verwenden das TGT, um ein *Dienstticket* und einen *Sitzungsschlüssel* für den angeforderten Dienst bei einem *Ticket-Granting-Server* anzufordern, der ebenfalls innerhalb des KDC ausgeführt wird.

Wenn der Benutzer beispielsweise auf einen Modellrepository-Dienst vom Informatica Developer-Client zugreift, fordert das TGT ein Dienstticket für den Knoten an, auf dem der angeforderte Dienst ausgeführt wird. Das TGT fordert auch ein Dienstticket für den Modellrepository-Dienst an.

6. Kerberos verwendet das Dienstticket, um den Client bei dem angeforderten Dienst zu authentifizieren. Das Dienstticket wird auf dem Computer zwischengespeichert, den der Informatica-Client hostet, was es dem Client ermöglicht, das Ticket zu verwenden, solange es gültig ist. Wenn der Benutzer den Informatica-Client herunterfährt und dann neu startet, verwendet der Client das gleiche Ticket wieder, um auf Prozesse und Dienste innerhalb der Informatica-Domäne zuzugreifen.

Bereichsübergreifende Kerberos-Authentifizierung

Sie können eine Informatica-Domäne zur Verwendung der bereichsübergreifenden Kerberos-Authentifizierung konfigurieren. Mit der bereichsübergreifenden Kerberos-Authentifizierung können sich Informatica-Clients, die zu einem Kerberos-Bereich gehören, bei Knoten und Anwendungsdiensten authentifizieren, die zu einem anderen Kerberos-Bereich gehören.

Wenn Sie eine Domäne zur Verwendung der bereichsübergreifenden Kerberos-Authentifizierung konfigurieren, fügen Sie der Kerberos-Konfigurationsdatei Eigenschaften für jeden Kerberos-Bereich hinzu. Darüber hinaus schließen Sie den Namen jedes Kerberos-Bereichs ein, wenn Sie `infasetup`-Befehle zum Aktivieren der Kerberos-Authentifizierung in der Domäne und auf Domänenknoten ausführen.

Die Active Directory-Server, die von der Domäne für die bereichsübergreifende Kerberos-Authentifizierung verwendet werden, müssen zur selben Active Directory-Gesamtstruktur gehören. Bei einer Active Directory-Gesamtstruktur handelt es sich um eine Gruppe von Active Directory-Domänen, die einen allgemeinen globalen Katalog, ein Verzeichnisschema, eine logische Struktur und Verzeichniskonfiguration gemeinsam nutzen. Sie stellen eine Verbindung zum globalen Katalog her, um Benutzer aus den Active Directory-Servern in LDAP-Sicherheitsdomänen zu importieren.

Zur Verwendung der bereichsübergreifenden Kerberos-Authentifizierung muss eine bidirektionale Vertrauensstellung zwischen den Active Directory-Servern in der Gesamtstruktur aktiviert werden.

Umwandeln einer Domäne mit einer Kerberos-Konfiguration für Einzelbereiche in eine Domäne mit bereichsübergreifender Kerberos-Konfiguration

Sie können eine Informatica-Domäne, die einen einzelnen Kerberos-Bereich zur Authentifizierung von Benutzern verwendet, in eine Domäne mit bereichsübergreifender Kerberos-Authentifizierung umwandeln.

Sie müssen die Domäne auf Version 10.2 HotFix 2 aktualisieren, bevor Sie die Domäne in eine Domäne mit bereichsübergreifender Kerberos-Authentifizierung umwandeln.

Darüber hinaus müssen Sie Benutzer- und Gruppenkonten aus dem globalen Active Directory-Katalog in eine LDAP-Sicherheitsdomäne importieren. Wenn Sie Konten importieren, werden vorhandene Konten in der LDAP-Sicherheitsdomäne, die das Namensattribut „samAccount“ verwenden, gelöscht und durch neue Konten mit dem Namensattribut „user principal“ ersetzt.

Benutzer melden sich bei Informatica-Clients mit dem vollqualifizierten Benutzerprinzipalnamen an, der folgendes Format aufweist:

```
<user name>@<KERBEROS REALM NAME>
```

Nachdem Sie die Benutzer- und Gruppenkonten importiert haben, weisen Sie den Konten Rechte, Rollen und Berechtigungen zu.

1. Aktualisieren Sie die Domäne auf Version 10.2 HotFix 2.

2. Fügen Sie die notwendigen Eigenschaften für jeden Kerberos-Bereich zur Kerberos-Konfigurationsdatei hinzu.

Legen Sie die Eigenschaften für jeden Bereich in der Konfigurationsdatei `krb5.conf` auf allen Knoten in der Domäne fest. Starten Sie die Domäne neu, nachdem Sie die Datei auf allen Knoten in der Domäne aktualisiert haben.

Weitere Informationen zum Konfigurieren der Konfigurationsdatei `krb5.conf` für die bereichsübergreifende Kerberos-Authentifizierung finden Sie unter ["Konfigurieren der Kerberos-Konfigurationsdatei" auf Seite 39](#).

3. Kopieren Sie die aktualisierte Datei `krb5.conf` in folgendes Verzeichnis auf jedem Computer, der einen Informatica-Client hostet:

```
<Informatica-Installationsverzeichnis>\clients\shared\security
```

4. Führen Sie die `infasetup`-Befehle „`UpdateGatewayNode`“ und „`UpdateWorkerNode`“ auf den Domänenknoten aus.

Geben Sie den Namen jedes Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird, als Wert für die Optionen „`-srn`“ und „`-urn`“, getrennt durch ein Komma, an.

Weitere Informationen zum Ausführen der `infasetup`-Befehle finden Sie im Abschnitt „`infasetup`-Befehlsreferenz“ in der *Informatica 10.2 HotFix 2-Befehlsreferenz*.

5. Führen Sie den Befehl „`UpdateKerberosConfig`“ auf einem Gateway-Knoten innerhalb der Domäne aus.

Geben Sie den Namen jedes Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird, als Wert für die Optionen „`-srn`“ und „`-urn`“, getrennt durch ein Komma, an.

6. Führen Sie den Befehl „`UpdateKerberosAdminUser`“ auf einem Gateway-Knoten innerhalb der Domäne aus.

Geben Sie den vollqualifizierten Benutzerprinzipalnamen für das Benutzerkonto des Domänenadministrators an.

7. Importieren Sie Benutzer- und Gruppenkonten in LDAP-Sicherheitsdomänen.

Stellen Sie eine Verbindung zum globalen Active Directory-Katalog her. Beim Herstellen einer Verbindung zum globalen Katalog importieren Sie Benutzer aus dem Active Directory-Server, der von allen Kerberos-Bereichen verwendet wird.

Weitere Informationen zum Herstellen einer Verbindung zum globalen Katalog und Importieren von Konten finden Sie unter ["Importieren von Benutzerkonten aus Active Directory in LDAP-Sicherheitsdomänen" auf Seite 61](#).

8. Weisen Sie den Benutzer- und Gruppenkonten, die Sie in eine LDAP-Sicherheitsdomäne importiert haben, Rechte, Rollen und Berechtigungen zu.

Weitere Informationen zum Zuweisen von Rechten und Rollen finden Sie unter [Kapitel 9, "Berechtigungen und Rollen" auf Seite 150](#).

Weitere Informationen zum Zuweisen von Berechtigungen finden Sie unter [Kapitel 10, "Berechtigungen" auf Seite 197](#).

Vorbereiten der Aktivierung der Kerberos-Authentifizierung

Sie müssen mehrere Aufgaben ausführen, um die Aktivierung der Kerberos-Authentifizierung in einer Informatica-Domäne vorzubereiten. Die Verfahren, die Sie für die einzelnen Aufgaben befolgen, hängen von der Dienstprinzipalebene ab, auf der Sie Kerberos aktivieren.

Hinweis: Sie können Kerberos-Authentifizierung in einer Domäne nach der Aktivierung nicht mehr deaktivieren. Es ist auch nicht möglich, die Dienstprinzipalebene zwischen der Knotenebene und der Prozessebene umzuschalten.

Bestimmen der Kerberos-Dienstprinzipalebene

Wenn Sie die Aktivierung der Kerberos-Authentifizierung vorbereiten, müssen Sie die erforderliche Dienstprinzipalebene bestimmen. Die erforderliche Dienstprinzipalebene bestimmt die Verfahren, die Sie zum Vorbereiten der Aktivierung der Kerberos-Authentifizierung in der Domäne befolgen müssen.

Sie können Kerberos-Authentifizierung auf einer der folgenden Ebenen aktivieren:

Knotenebene

Wenn Sie die Domäne zu Test- oder Entwicklungszwecken verwenden und die Domäne keine hohe Sicherheitsstufe erfordert, können Sie Kerberos auf Knotenebene aktivieren. Sie können einen einzelnen Dienstprinzipalnamen und eine einzelne Keytab-Datei für den Knoten und für alle Prozesse und Dienste verwenden, die auf dem Knoten ausgeführt werden. Sie müssen auch einen SPN und eine Keytab-Datei für die auf dem Knoten ausgeführten HTTP-Prozesse erstellen.

Prozessebene

Wenn die Domäne zur Produktion verwendet wird und eine hohe Sicherheitsstufe erfordert, können Sie den Dienstprinzipal auf Prozessebene festlegen. Sie erstellen einen eindeutigen SPN und eine eigene Keytab-Datei für jeden Knoten und für jeden Prozess auf dem Knoten. Sie müssen auch einen SPN und eine Keytab-Datei für die auf dem Knoten ausgeführten HTTP-Prozesse erstellen.

Auf Prozessebene aktiviertes Kerberos bietet die höchste Sicherheitsstufe, kann aber schwer zu verwalten sein, wenn die Informatica-Domäne viele Knoten oder Dienste enthält. In diesem Szenario haben Sie die Möglichkeit, Kerberos auf Knotenebene zu aktivieren.

Konfigurieren der Kerberos-Konfigurationsdatei

Legen Sie die Eigenschaften fest, die von Informatica für die Kerberos-Konfigurationsdatei gefordert werden, und kopieren Sie die Datei dann auf jeden Knoten in der Informatica-Domäne.

Kerberos speichert Konfigurationsinformationen in einer Datei mit der Bezeichnung *krb5.conf*: Sie müssen die Eigenschaften in der Konfigurationsdatei „krb5.conf“ festlegen und die Datei anschließend auf jeden Knoten in der Informatica-Domäne kopieren.

Wenn in der Domäne die bereichsübergreifende Kerberos-Authentifizierung verwendet wird, geben Sie die notwendigen Eigenschaften für jeden Kerberos-Bereich ein.

1. Konfigurieren Sie die folgenden Eigenschaften der Kerberos-Bibliothek im Abschnitt *libdefaults* der Datei.

In der folgenden Tabelle werden die einzugebenden Eigenschaften beschrieben:

Eigenschaft	Beschreibung
default_realm	Name des Kerberos-Bereichs, zu dem die Informatica-Domänendienste gehören. Der Bereichsname muss aus Großbuchstaben bestehen. Wird in der Domäne ein einzelner Kerberos-Bereich für die Authentifizierung verwendet, müssen der Name des Dienstbereichs und der Name des Benutzerbereichs identisch sein.
forwardable	Ermöglicht es einem Dienst, Client-Benutzeranmeldedaten an einen anderen Dienst zu delegieren. Für die Informatica-Domäne müssen Anwendungsdienste die Client-Benutzeranmeldedaten bei anderen Diensten authentifizieren. Setzen Sie den Wert auf „true“.
default_tkt_enctypes	Verschlüsselungstypen für den Sitzungsschlüssel, der in den Ticket-Granting-Tickets (TGT) enthalten ist. Legen Sie diese Eigenschaft nur fest, wenn Sitzungsschlüssel spezifische Verschlüsselungstypen verwenden müssen. Vergewissern Sie sich, dass das Key Distribution Center (KDC) von Kerberos den angegebenen Verschlüsselungstyp unterstützt. Legen Sie diese Eigenschaft nicht fest, um zuzulassen, dass das Kerberos-Protokoll den zu verwendenden Verschlüsselungstyp auswählt. Wenn die Knotenhosts oder die Informatica-Clienthosts 256-Bit-Verschlüsselung verwenden, installieren Sie die Unlimited Strength JCE-Richtliniendateien (Java Cryptography Extension) auf allen Knotenhosts und Informatica-Clienthosts, um Authentifizierungsprobleme zu vermeiden.
rdns	Bestimmt, ob Reverse Name Lookup zusätzlich zu Forward Name Lookup verwendet wird, um Hostnamen für die Verwendung in Dienstprinzipalnamen zu kanonisieren. Setzen Sie den Wert auf „false“.
renew_lifetime	Die verlängerbare Standardlebensdauer für anfängliche Ticketanfragen.
ticket_lifetime	Die Standardlebensdauer für anfängliche Ticketanfragen.
udp_preference_limit	Legt das Protokoll fest, das Kerberos beim Senden einer Meldung an das KDC verwendet. Legen Sie den Wert auf 1 fest, um das TCP-Protokoll zu verwenden, wenn in der Domäne immer wieder Kerberos-Authentifizierungsfehler auftreten.
dns_lookup_kdc	Gibt an, ob der Kerberos-Client die KDCs und andere Server für einen Bereich, falls diese nicht in den Informationen für den Bereich aufgeführt sind, mithilfe von DNS-SRV-Datensätzen sucht. Anhand von SRV-Datensätzen ermittelt DNS Computer, die bestimmte Dienste hosten. Erforderlich, wenn die Domäne Kerberos-fähig ist. Erfordert die Festlegung der Bereichseigenschaft „admin_server“. Setzen Sie den Wert auf „true“.
dns_lookup_realm	Gibt an, ob der Kerberos-Client den Kerberos-Bereich eines Hosts mithilfe von DNS-TXT-Datensätzen bestimmt. Anhand von TXT-Datensätzen verknüpft DNS beliebigen Text, beispielsweise visuell lesbare Informationen zu einem Server, Netzwerk, Datencenter oder anderen Buchhaltungsinformationen, mit einem Hostnamen oder anderen Namen. Erforderlich, wenn die Domäne Kerberos-fähig ist. Setzen Sie den Wert auf „true“.

- Definieren Sie die einzelnen Kerberos-Bereiche im Abschnitt *realms* der Datei.

Das folgende Beispiel zeigt den Eintrag für einen Kerberos-Bereich mit dem Namen COMPANY.COM:

```
[realms]
COMPANY.COM = {...}
```

3. Geben Sie die folgenden Bereichseigenschaften in Klammern für jeden Kerberos-Bereich im Abschnitt *realms* der Datei ein.

In der folgenden Tabelle werden die einzugebenden Eigenschaften beschrieben:

Eigenschaft	Beschreibung
admin_server	Der Name oder die IP-Adresse des Kerberos-Verwaltungsserverhosts. Sie können eine optionale Portnummer einschließen, die durch einen Doppelpunkt vom Hostnamen getrennt wird. Der Standardwert ist 749. Erforderlich, wenn Sie „dns_lookup_kdc“ im Abschnitt <i>libdefaults</i> konfigurieren.
kdc	Der Name oder die IP-Adresse eines Hosts, der das Key Distribution Center (KDC) für den Bereich ausführt. Sie können eine optionale Portnummer einschließen, die durch einen Doppelpunkt vom Hostnamen getrennt wird. Der Standardwert ist 88.

Das folgende Beispiel zeigt die Einträge für jeden Kerberos-Bereich in einer bereichsübergreifenden Kerberos-Konfiguration:

```
[realms]
COMPANY.COM = {
  admin_server = KDC01.COMPANY.COM:749
  kdc = KDC01.COMPANY.COM:88
}
EAST.COMPANY.COM = {
  kdc = 10.75.141.193
  admin_server = 10.75.141.193
}
WEST.COMPANY.COM = {
  kdc = 10.78.140.111
  admin_server = 10.78.140.111
}
```

4. Ordnen Sie im Abschnitt *domain_realms* den Domänen- oder Hostnamen einem Kerberos-Bereichsnamen zu. Der Domänenname weist als Präfix einen Punkt (.) auf.

Das folgende Beispiel zeigt die Parameter für den Hadoop-Bereich „domain_realm“, wenn die Informatica-Domäne die Kerberos-Authentifizierung nicht verwendet:

```
[domain_realm]
.hadoop_realm.com = HADOOP-REALM
hadoop_realm.com = HADOOP-REALM
```

Das folgende Beispiel zeigt die Parameter für den Hadoop-Bereich „domain_realm“, wenn die Informatica-Domäne die Kerberos-Authentifizierung verwendet:

```
[domain_realm]
.infa_ad_realm.com = INFA-AD-REALM
infa_ad_realm.com = INFA-AD-REALM
.hadoop_realm.com = HADOOP-REALM
hadoop_realm.com = HADOOP-REALM
```

5. Kopieren Sie die Datei `krb5.conf` in die folgenden Verzeichnisse auf dem Computer, auf dem der Datenintegrationsdienst gehostet wird:

- <Informatica-Installationsverzeichnis>/services/shared/security
- <Informatica-Installationsverzeichnis>/java/jre/lib/security/

Das folgende Beispiel zeigt den Inhalt einer Kerberos-Konfigurationsdatei mit den notwendigen Eigenschaften für eine Kerberos-Konfiguration für Einzelbereiche:

```
[libdefaults]
default_realm = COMPANY.COM
forwardable = true
rdns = false
renew_lifetime = 7d
ticket_lifetime = 24h
udp_preference_limit = 1
dns_lookup_kdc = true
dns_lookup_realm = true

[realms]
COMPANY.COM = {
admin_server = KDC01.COMPANY.COM:749
kdc = KDC01.COMPANY.COM:88
}

[domain_realm]
.company.com = COMPANY.COM
company.com = COMPANY.COM
```

Das folgende Beispiel zeigt den Inhalt einer Kerberos-Konfigurationsdatei mit den notwendigen Eigenschaften für eine bereichsübergreifende Kerberos-Konfiguration:

```
[libdefaults]
default_realm = COMPANY.COM
forwardable = true
rdns = false
renew_lifetime = 7d
ticket_lifetime = 24h
udp_preference_limit = 1
dns_lookup_kdc = true
dns_lookup_realm = true

[realms]
COMPANY.COM = {
admin_server = KDC01.COMPANY.COM:749
kdc = KDC01.COMPANY.COM:88
}
EAST.COMPANY.COM = {
kdc = 10.75.141.193
admin_server = 10.75.141.193
}
WEST.COMPANY.COM = {
kdc = 10.78.140.111
admin_server = 10.78.140.111
}

[domain_realm]
.company.com = COMPANY.COM
company.com = COMPANY.COM
.east.company.com = EAST.COMPANY.COM
east.company.com = EAST.COMPANY.COM
.west.company.com = WEST.COMPANY.COM
west.company.com = WEST.COMPANY.COM
```

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

Erstellen der Kerberos-Prinzipalkonten in Active Directory

Erstellen Sie die LDAP-Benutzerkonten für die Kerberos-Prinzipale in Active Directory. Ein Kerberos-Prinzipal ist ein Prozess, Dienst oder Benutzer innerhalb des Kerberos-Bereichs.

Wenn Sie die Eigenschaft „default_tkt_enctypes“ in der Konfigurationsdatei „krb5.conf“ auf die 128-Bit- oder 256-Bit-AES-Verschlüsselungstypen festlegen, konfigurieren Sie jedes Konto für die Verwendung des entsprechenden Verschlüsselungstyps in Active Directory.

Welche Konten erstellt werden, hängt davon ab, ob Sie Kerberos auf Knotenebene oder auf Prozessebene aktivieren.

Hinweis: Kontonamen können maximal 20 Zeichen umfassen.

Auf Knotenebene erforderliche Konten

Erstellen Sie die LDAP-Benutzerkonten, die zur Aktivierung der Kerberos-Authentifizierung auf Knotenebene erforderlich sind, in Active Directory.

Erstellen Sie die folgenden Kerberos-Prinzipalkonten in Active Directory, wenn Sie Kerberos auf Knotenebene aktivieren:

Knotenprozesse

Erstellen Sie ein Konto für jeden Knoten, der in der Domäne ausgeführt wird.

HTTP-Prozess

Erstellen Sie ein Konto für die Informatica-Webanwendungen, die auf einem Knoten in der Domäne ausgeführt werden. Zu den Webanwendungen, die auf einem Knoten ausgeführt werden können, gehören beispielsweise das Administrator Tool, Informatica Analyst und Catalog Administrator. Erstellen Sie ein einzelnes Konto, das von allen auf dem Knoten ausgeführten Webanwendungen gemeinsam genutzt wird.

Distinguished Name (DN) des Bind-Benutzers

Erstellen Sie ein LDAP-Bind-Benutzerkonto, das Sie zum Synchronisieren der LDAP-Sicherheitsdomäne, welche die Kerberos-Benutzerkonten enthält, mit Active Directory verwenden.

Auf Prozessebene erforderliche Konten

Erstellen Sie die LDAP-Benutzerkonten, die zur Aktivierung der Kerberos-Authentifizierung auf Prozessebene erforderlich sind, in Active Directory.

Erstellen Sie die folgenden Kerberos-Prinzipalkonten in Active Directory, wenn Sie Kerberos auf Prozessebene aktivieren:

Knotenprozesse

Erstellen Sie ein Konto für jeden Knoten, der in der Domäne ausgeführt wird.

HTTP-Prozesse

Erstellen Sie ein Konto für die Informatica-Webanwendungen, die auf einem Knoten in der Domäne ausgeführt werden. Zu den Webanwendungen, die auf einem Knoten ausgeführt werden können, zählen beispielsweise Informatica Analyst und Catalog Administrator. Erstellen Sie ein einzelnes Konto, das von allen auf dem Knoten ausgeführten Webanwendungen gemeinsam genutzt wird.

Informatica Administrator-Dienst

Erstellen Sie ein Konto für das Administrator Tool auf jedem Gateway-Knoten in der Domäne.

Informatica-Anwendungsdienste

Erstellen Sie ein Konto für jeden Informatica-Anwendungsdienst, der auf den einzelnen Knoten in der Domäne ausgeführt wird.

Distinguished Name (DN) des Bind-Benutzers

Erstellen Sie ein LDAP-Benutzerkonto, das Sie zum Synchronisieren der LDAP-Sicherheitsdomäne, welche die Kerberos-Benutzerkonten enthält, mit Active Directory verwenden.

Generieren der Formate für Dienstprinzipalnamen und Keytab-Dateinamen

Verwenden Sie das Dienstprogramm SPN-Formatgenerator von Informatica für Kerberos, um die Formate für den Dienstprinzipalnamen (SPN) und den Keytab-Dateinamen zu generieren, die für die Verwendung der Kerberos-Authentifizierung erforderlich sind. Das Dienstprogramm SPN-Formatgenerator für Kerberos generiert eine Textdatei mit dem Namen „SPNKeytabFormat.txt“, die das korrekte Format für die SPNs und die Keytab-Dateinamen enthält.

Welche SPN- und Keytab-Dateinamensformate generiert werden, hängt davon ab, ob Sie Kerberos auf Knotenebene oder auf Prozessebene aktivieren.

Generieren der Formate für Dienstprinzipalnamen und Keytab-Dateinamen auf Knotenebene

Generieren Sie die Formate für die SPNs und die Keytab-Dateinamen, die zum Aktivieren der Kerberos-Authentifizierung auf Knotenebene erforderlich sind.

Die Informatica-Domäne erfordert SPNs und Keytab-Dateien für die folgenden Prozesse, wenn Sie Kerberos-Authentifizierung auf Knotenebene aktivieren:

Knotenprozesse

Informatica erfordert einen SPN und eine Keytab-Datei für jeden Knoten in der Domäne. Kerberos verwendet den gleichen Dienstprinzipalnamen und Keytab zum Authentifizieren der Informatica-Anwendungsdienste, die auf dem Knoten ausgeführt werden.

HTTP-Prozesse

Informatica erfordert einen SPN und eine Keytab-Datei für die Webanwendungen, die auf den einzelnen Knoten in der Domäne ausgeführt werden. Zu den Webanwendungen, die auf einem Knoten ausgeführt werden können, gehören beispielsweise das Administrator Tool, Informatica Analyst und Catalog Administrator. Kerberos verwendet den gleichen Dienstprinzipalnamen zum Authentifizieren aller Webanwendungen, die auf dem Knoten ausgeführt werden.

1. Gehen Sie auf einem Windows Informatica-Knotenhost zu dem Verzeichnis, das die Batchdatei „SPNFormatGenerator.bat“ enthält:

```
<Informatica-Installationsverzeichnis>\tools\Kerberos
```

Navigieren Sie auf einem UNIX Informatica-Knotenhost zu dem Verzeichnis, das die Shell-Datei „SPNFormatGenerator.sh“ enthält:

```
<Informatica-Installationsverzeichnis>/tools/Kerberos
```

2. Führen Sie „SPNFormatGenerator.bat“ bzw. „SPNFormatGenerator.sh“ aus.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie **Knotenebene** aus.
5. Klicken Sie auf **Weiter**.

6. Geben Sie die erforderlichen Eigenschaften zum Generieren der SPN- und Keytab-Dateiformate ein.
In der folgenden Tabelle werden die Eigenschaften beschrieben:

Eingabeaufforderung	Beschreibung
Domänenname	Name der Informatica-Domäne. Der Name darf maximal 128 Zeichen umfassen und muss im 7-Bit-ASCII-Format vorliegen. Er darf weder Leerzeichen noch die folgenden Zeichen enthalten: ` % * + ; " ? , < > \ /
Dienstbereichsname	Name des Kerberos-Bereichs. Der Bereichsname muss aus Großbuchstaben bestehen.
Knotenname	Name des Informatica-Knotens
Hostname des Knotens	Vollqualifizierter Name des Knotenhosts. Der Hostname des Knotens darf keine Unterstriche (_) enthalten. Hinweis: Verwenden Sie nicht <i>localhost</i> . Der Hostname muss den Host eindeutig kennzeichnen.

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

Die folgende Abbildung zeigt die Einträge für mehrere Knoten in der InfaDomain-Domäne im Dienstprogramm „SPN-Formatgenerator“:

Informatica Kerberos SPN Format Generator

Authentication Parameters - Kerberos Authentication - Step 3 of 4

Specify the domain and Kerberos authentication parameters.

Domain name: InfaDomain

Service realm name: COMPANY.COM

Node name: node01

Node host name: JS001DEV

+Node -Node

Node name: node02

Node host name: JS005DEV

< Previous Next > Cancel

8. Klicken Sie auf **Weiter**.

Das Dienstprogramm „SPN-Formatgenerator“ zeigt den Pfad und Namen der Datei an, die die Liste der Dienstprinzipalnamen und Keytab-Dateinamen enthält.

9. Klicken Sie auf **Fertig**, um das Dienstprogramm „SPN-Formatgenerator“ zu beenden.

Generieren der Formate für Dienstprinzipalnamen und Keytab-Dateinamen auf Prozessebene

Generieren Sie die Formate für die SPNs und die Keytab-Dateinamen, die zum Aktivieren der Kerberos-Authentifizierung auf Prozessebene erforderlich sind.

Die Informatica-Domäne erfordert SPNs und Keytab-Dateien für die folgenden Prozesse und Dienste, wenn Sie Kerberos-Authentifizierung auf Prozessebene aktivieren:

Knotenprozesse

Informatica erfordert einen SPN und eine Keytab-Datei für jeden Knoten in der Domäne.

Informatica Administrator

Informatica erfordert einen SPN und eine Keytab-Datei für das Administrator Tool für jeden Gateway-Knoten in der Domäne.

HTTP-Prozesse

Informatica erfordert einen SPN und eine Keytab-Datei für die Webanwendungen, die auf einem Knoten in der Domäne ausgeführt werden. Zu den Webanwendungen, die auf einem Knoten ausgeführt werden können, zählen beispielsweise Informatica Analyst und Catalog Administrator.

Informatica-Anwendungsdienstprozesse

Informatica erfordert einen SPN und eine Keytab-Datei für jeden Informatica-Anwendungsdienst, der auf den einzelnen Knoten in der Domäne ausgeführt wird.

1. Gehen Sie auf einem Windows Informatica-Knotenhost zu dem Verzeichnis, das die Batchdatei „SPNFormatGenerator.bat“ enthält:

```
<Informatica-Installationsverzeichnis>\tools\Kerberos
```

Navigieren Sie auf einem UNIX Informatica-Knotenhost zu dem Verzeichnis, das die Shell-Datei „SPNFormatGenerator.sh“ enthält:

```
<Informatica-Installationsverzeichnis>/tools/Kerberos
```

2. Führen Sie „SPNFormatGenerator.bat“ bzw. „SPNFormatGenerator.sh“ aus.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie **Prozessebene** aus.
5. Klicken Sie auf **Weiter**.
6. Geben Sie die erforderlichen Eigenschaften zum Generieren der SPN- und Keytab-Dateiformate ein.

In der folgenden Tabelle werden die Eigenschaften beschrieben:

Eingabeaufforderung	Beschreibung
Domänenname	Name der Informatica-Domäne. Der Name darf maximal 128 Zeichen umfassen und muss im 7-Bit-ASCII-Format vorliegen. Er darf weder Leerzeichen noch die folgenden Zeichen enthalten: ` % * + ; " ? , < > \ /
Dienstbereichsname	Name des Kerberos-Bereichs. Der Bereichsname muss aus Großbuchstaben bestehen.

Eingabeaufforderung	Beschreibung
Knotenname	Name des Informatica-Knotens
Hostname des Knotens	Vollqualifizierter Name oder die IP-Adresse des Knotenhosts. Der Hostname des Knotens darf keine Unterstriche (_) enthalten. Hinweis: Verwenden Sie nicht <i>localhost</i> . Der Hostname muss den Host eindeutig kennzeichnen.

- Um das SPN-Format für einen Informatica-Anwendungsdienst zu generieren, der auf einem Knoten ausgeführt wird, klicken Sie nach Eingabe der Knotendetails auf **Dienst**.
Geben Sie den Namen des Informatica-Anwendungsdiensts ein, wie im Administrator Tool gezeigt. Führen Sie diesen Schritt für jeden Informatica-Anwendungsdienst aus, der auf den einzelnen Knoten in der Domäne ausgeführt wird.
- Zum Generieren des SPN-Formats für einen zusätzlichen Knoten klicken Sie auf **+Knoten**, und geben Sie den Knotennamen und Hostnamen an.

Die folgende Abbildung zeigt die Einträge für mehrere Knoten und Anwendungsdienste, die in der InfaDomain-Domäne im Dienstprogramm „SPN-Formatgenerator“ ausgeführt werden:

Informatica Kerberos SPN Format Generator

Authentication Parameters - Kerberos Authentication - Step 3 of 4

Specify the domain and Kerberos authentication parameters.

Domain name: InfaDomain

Service realm name: COMPANY.COM

Node name: node01

Node host name: JS001DEV

Service on node: MRS_dev

Service on node: DIS_dev

Node name: node02

Node host name: JS005DEV

Service on node: CMS_dev

+Node +Service -Node

< Previous Next > Cancel

- Klicken Sie auf **Weiter**.
Das Dienstprogramm „SPN-Formatgenerator“ zeigt den Pfad und Namen der Datei an, die die Liste der Dienstprinzipalnamen und Keytab-Dateinamen enthält.
- Klicken Sie auf **Fertig**, um das Dienstprogramm „SPN-Formatgenerator“ zu beenden.

Überprüfen der Textdatei der Formate für Dienstprinzipalnamen und Keytab-Dateinamen

Nachdem Sie die Datei „SPNKeytabFormat.txt“ generiert haben, können Sie die Datei überprüfen.

Sie verwenden die Informationen in der Datei zum Generieren der Keytab-Dateien und zum Zuordnen jedes SPN zum entsprechenden Prinzipalbenutzerkonto in Active Directory.

Die Datei „SPNKeytabFormat.txt“ enthält die folgenden Informationen:

Entitätsname

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

Dienstprinzipalname

Format für den SPN. Beim SPN wird die Groß- und Kleinschreibung beachtet.

Hinweis: Wenn Sie eine aus mehreren Kerberos-Domänennamen bestehende Zeichenfolge eingeben oder ein Sternchen vor einem Bereichssuffix einfügen, um alle Bereiche mit diesem Suffix zu berücksichtigen, ist der Bereichsname im SPN-Format nicht enthalten.

In der folgenden Tabelle werden die SPN-Formate beschrieben:

Keytab-Typ	SPN-Format
NODE_SPN	isp/<Knotenname>/<Domänename>@<BEREICHNAME>
NODE_AC_SPN	_AdminConsole/<Knotenname>/<Domänename>@<BEREICHNAME>
NODE_HTTP_SPN	HTTP/<Knoten-Hostname>@<BEREICHNAME> 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	<Anwendungsdienstname>/<Knotenname>/<Domänename>@<BEREICHNAME>

Keytab-Dateiname

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

Die folgende Tabelle beschreibt die Formate für Keytab-Dateinamen:

Keytab-Typ	Keytab-Dateiname
NODE_SPN	<Knotenname>.keytab
NODE_AC_SPN	_AdminConsole.keytab
NODE_HTTP_SPN	webapp_http.keytab
SERVICE_PROCESS_SPN	<Anwendungsdienstname>.keytab

Dienstprinzipale auf der Knotenebene

Die folgende Abbildung 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@COMPANY.COM	node01.keytab	NODE_SPN
node01	HTTP/US001DEV.company.com@COMPANY.COM	webapp_http.keytab	NODE_HTTP_SPN
node02	isp/node02/Infadomain@COMPANY.COM	node02.keytab	NODE_SPN
node02	HTTP/US005DEV.company.com@COMPANY.COM	webapp_http.keytab	NODE_HTTP_SPN

Dienstprinzipale auf der Prozessebene

Die folgende Abbildung 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@COMPANY.COM	node01.keytab	NODE_SPN
node01	_AdminConsole/node01/Infadomain@COMPANY.COM	_AdminConsole.keytab	NODE_AC_SPN
node01	HTTP/US001DEV.company.com@COMPANY.COM	webapp_http.keytab	NODE_HTTP_SPN
node02	isp/node02/Infadomain@COMPANY.COM	node02.keytab	NODE_SPN
node02	_AdminConsole/node02/Infadomain@COMPANY.COM	_AdminConsole.keytab	NODE_AC_SPN
node02	HTTP/US005DEV.company.com@COMPANY.COM	webapp_http.keytab	NODE_HTTP_SPN
MRS_dev:node01	MRS_dev/node01/Infadomain@COMPANY.COM	MRS_dev.keytab	SERVICE_PROCESS_SPN
DIS_dev:node01	DIS_dev/node01/Infadomain@COMPANY.COM	DIS_dev.keytab	SERVICE_PROCESS_SPN
CAT_dev:node02	CAT_dev/node02/Infadomain@COMPANY.COM	CAT_dev.keytab	SERVICE_PROCESS_SPN

Generieren der Keytab-Dateien

Generieren Sie die Keytab-Dateien, die zum Authentifizieren der Informatica-Benutzer und -Dienste verwendet werden.

Sie verwenden das Dienstprogramm „ktpass“ von Microsoft Windows Server, um eine Keytab-Datei für jedes Benutzerkonto zu generieren, das Sie in Active Directory erstellt haben. Sie müssen die Keytab-Dateien auf einem Mitgliedsserver oder einem Domänencontroller innerhalb der Active Directory-Domäne generieren. Sie können Keytab-Dateien nicht auf einem Workstation-Betriebssystem wie Microsoft Windows 7 generieren.

Um „ktpass“ zum Generieren einer Keytab-Datei zu verwenden, führen Sie den folgenden Befehl aus:

```
ktpass.exe -out <keytab filename> -princ <service principal name> -mapuser <user account> [-pass <user account password>] -crypto <key types> -ptype <principal type> [-target <realm name>]
```

In der folgenden Tabelle werden die Befehlsoptionen beschrieben:

Option	Beschreibung
-out	Der Dateiname der zu generierenden Kerberos-Keytab-Datei, der in der Spalte KEY_TAB_NAME in der Datei „SPNKeytabFormat.txt“ angezeigt wird.
-princ	Der Dienstprinzipalname, der in der Spalte SPN in der Datei „SPNKeytabFormat.txt“ angezeigt wird. Wenn in der Domäne die bereichsübergreifende Kerberos-Authentifizierung verwendet wird, muss der Dienstprinzipalname in allen Kerberos-Bereichen eindeutig sein.
-mapuser	Das Active Directory-Benutzerkonto, das dem SPN zugeordnet wird. Der Kontoname kann maximal 20 Zeichen umfassen.
-pass	Das in Active Directory festgelegte Passwort für das Active Directory-Benutzerkonto, falls zutreffend.
-crypto	Gibt die in der Keytab-Datei generierten Schlüsseltypen an. Legen Sie „Alle“ fest, um alle unterstützten Verschlüsselungstypen zu verwenden.

Option	Beschreibung
-ptype	Der Prinzipaltyp. Legen Sie ihn auf KRB5_NT_PRINCIPAL fest.
-target	Der Name des Bereichs, zu dem der Active Directory-Server gehört. Schließen Sie diese Option ein, wenn der folgende Fehler beim Ausführen des Dienstprogramms auftritt: DsCrackNames hat 0x2 im Namen zurückgegeben

Welche Keytab-Dateien generiert werden, hängt davon ab, ob Sie Kerberos auf Knotenebene oder auf Prozessebene aktivieren.

Generieren der Keytab-Dateien auf Knotenebene

Wenn Sie „ktpass“ zum Generieren der Keytab-Dateien auf Knotenebene ausführen, ordnen Sie jedem Kerberos-Prinzipalbenutzerkonto den entsprechenden SPN in Active Directory zu.

Die folgende Tabelle zeigt die Zuordnung zwischen den Kerberos-Prinzipalbenutzerkonten und den SPNs anhand der Beispieldatei „SPNKeytabFormat.txt“:

Benutzerkonto	Keytab-Typ	Dienstprinzipalname
nodeuser01	NODE_SPN	isp/node01/InfaDomain/COMPANY.COM
httpuser01	NODE_HTTP_SPN	HTTP/US001DEV.company.com@COMPANY.COM
nodeuser02	NODE_SPN	isp/node02/InfaDomain/COMPANY.COM
httpuser02	NODE_HTTP_SPN	HTTP/US005DEV.company.com@COMPANY.COM

Sie erstellen auch eine Keytab für das LDAP-Bind-Benutzerkonto, das während der LDAP-Synchronisierung für den Zugriff auf und das Durchsuchen von Active Directory verwendet wird.

1. Erstellen Sie eine Keytab-Datei für das Kerberos-Prinzipalbenutzerkonto, das Sie für jeden Knoten in Active Directory erstellt haben.

Kopieren Sie den Keytab-Dateinamen aus der Spalte `KEY_TAB_NAME` in der Datei „SPNKeytabFormat.txt“.

Kopieren Sie den Dienstprinzipalnamen aus der Spalte `SPN` in der Datei „SPNKeytabFormat.txt“.

Im folgenden Beispiel wird eine Keytab-Datei für ein Kerberos-Prinzipalbenutzerkonto mit dem Namen „nodeuser0“ erstellt:

```
ktpass.exe -out node01.keytab -princ isp/node01/InfaDomain/COMPANY.COM -mapuser
nodeuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
```

2. Erstellen Sie eine Keytab-Datei für jedes in Active Directory erstellte Kerberos-Prinzipalbenutzerkonto des HTTP-Prozesses.

Wenn in der Domäne bereichsübergreifende Kerberos-Authentifizierung verwendet wird, kann das Prinzipalbenutzerkonto in einem von der Domäne verwendeten Kerberos-Bereich vorhanden sein.

Kopieren Sie den Namen der Keytab-Datei aus der Spalte `KEY_TAB_NAME` in der Datei „SPNKeytabFormat.txt“. Kopieren Sie den Dienstprinzipalnamen aus der Spalte `SPN` in der Datei „SPNKeytabFormat.txt“.

Im folgenden Beispiel wird eine Keytab-Datei für ein Kerberos-Prinzipalbenutzerkonto mit dem Namen „httpuser01“ erstellt:

```
ktpass.exe -out webapp_http.keytab -princ HTTP/US001DEV.company.com@COMPANY.COM -mapuser
httpuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
```

- Erstellen Sie eine Keytab-Datei für das LDAP-Bind-Benutzerkonto, das während der LDAP-Synchronisierung für den Zugriff auf und das Durchsuchen von Active Directory verwendet wird.
Strukturieren Sie den Wert für die Option „-princ“ als <principal name>@<KERBEROS REALM>. Schließen Sie den Namen der LDAP-Konfiguration für den Active Directory-Server in den Namen der Keytab-Datei ein. Verwenden Sie für den Namen der Keytab-Datei folgende Struktur: <Active Directory LDAP configuration_name>.keytab.

Im folgenden Beispiel wird eine Keytab-Datei für ein Dienstprinzipalbenutzerkonto mit dem Namen „ldapuser“ erstellt.

```
ktpass.exe -out ActiveDirectoryServer1.keytab -princ ldapuser@COMPANY.COM -mapuser
ldapuser -crypto all -ptype KRB5_NT_PRINCIPAL
```

Generieren der Keytab-Dateien auf Prozessebene

Wenn Sie „ktpass“ zum Generieren der Keytab-Dateien auf Prozessebene ausführen, ordnen Sie jedem Kerberos-Prinzipalbenutzerkonto den entsprechenden SPN in Active Directory zu.

Die folgende Tabelle zeigt die Zuordnung zwischen den Kerberos-Prinzipalbenutzerkonten und den SPNs anhand der Beispieldatei „SPNKeytabFormat.txt“:

Benutzerkonto	Keytab-Typ	Dienstprinzipalname
nodeuser01	NODE_SPN	isp/node01/Infadomain/COMPANY.COM
admintooluser01	NODE_AC_SPN	_AdminConsole/node01/Infadomain@COMPANY.COM
httpuser01	NODE_HTTP_SPN	HTTP/US001DEV.company.com@COMPANY.COM
MRSdevuser01	SERVICE_PROCESS_SPN	MRS_dev/node01/Infadomain@COMPANY.COM
DISdevuser01	SERVICE_PROCESS_SPN	DIS_dev/node01/Infadomain@COMPANY.COM
nodeuser02	NODE_SPN	isp/node02/Infadomain/COMPANY.COM
admintooluser02	NODE_AC_SPN	_AdminConsole/node02/Infadomain@COMPANY.COM
httpuser02	NODE_HTTP_SPN	HTTP/US005DEV.company.com@COMPANY.COM
CATdevuser01	SERVICE_PROCESS_SPN	CAT_dev/node02/Infadomain@COMPANY.COM

Sie erstellen auch eine Keytab für das LDAP-Bind-Benutzerkonto, das während der LDAP-Synchronisierung für den Zugriff auf und das Durchsuchen von Active Directory verwendet wird.

- Erstellen Sie eine Keytab-Datei für das Kerberos-Prinzipalbenutzerkonto, das Sie für jeden Knoten in Active Directory erstellt haben.

Kopieren Sie den Dateinamen aus der Spalte KEY_TAB_NAME in die Datei „SPNKeytabFormat.txt“. Kopieren Sie den Dienstprinzipalnamen aus der Spalte SPN in der Datei „SPNKeytabFormat.txt“.

Im folgenden Beispiel wird eine Keytab-Datei für ein Kerberos-Prinzipalbenutzerkonto mit dem Namen „nodeuser01“ erstellt:

```
ktpass.exe -out node01.keytab -princ isp/node01/Infadomain/COMPANY.COM -mapuser
nodeuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
```

2. Erstellen Sie eine Keytab-Datei für jedes erstellte Kerberos-Prinzipalbenutzerkonto des HTTP-Prozesses.

Wenn in der Domäne bereichsübergreifende Kerberos-Authentifizierung verwendet wird, kann das Prinzipalbenutzerkonto in einem von der Domäne verwendeten Kerberos-Bereich vorhanden sein.

Kopieren Sie den Dateinamen aus der Spalte `KEY_TAB_NAME` in die Datei „SPNKeytabFormat.txt“. Kopieren Sie den Dienstprinzipalnamen aus der Spalte `SPN` in der Datei „SPNKeytabFormat.txt“.

Im folgenden Beispiel wird eine Keytab-Datei für ein Kerberos-Prinzipalbenutzerkonto mit dem Namen „httpuser01“ erstellt:

```
ktpass.exe -out webapp_http.keytab -princ HTTP/US001DEV.company.com@COMPANY.COM -mapuser httpuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
```

3. Erstellen Sie eine Keytab-Datei für jedes erstellte Kerberos-Prinzipalbenutzerkonto im Administrator Tool.

Kopieren Sie den Dateinamen aus der Spalte `KEY_TAB_NAME` in die Datei „SPNKeytabFormat.txt“. Kopieren Sie den Dienstprinzipalnamen aus der Spalte `SPN` in der Datei „SPNKeytabFormat.txt“.

Im folgenden Beispiel wird eine Keytab-Datei für ein Kerberos-Prinzipalbenutzerkonto mit dem Namen „admintooluser01“ erstellt:

```
ktpass.exe -out _AdminConsole.keytab -princ _AdminConsole/node01/InfraDomain@COMPANY.COM -mapuser admintooluser01 -crypto all -ptype KRB5_NT_PRINCIPAL
```

4. Erstellen Sie eine Keytab-Datei für jedes erstellte Kerberos-Prinzipalbenutzerkonto im Informatica-Anwendungsdienst.

Kopieren Sie den Dateinamen aus der Spalte `KEY_TAB_NAME` in die Datei „SPNKeytabFormat.txt“. Kopieren Sie den Dienstprinzipalnamen aus der Spalte `SPN` in der Datei „SPNKeytabFormat.txt“.

Im folgenden Beispiel wird eine Keytab-Datei für ein Kerberos-Dienstprinzipalbenutzerkonto mit dem Namen „MRSdevuser01“ erstellt:

```
ktpass.exe -out MRS_dev.keytab -princ HTTP/US001DEV.company.com@COMPANY.COM -mapuser MRSdevuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
```

5. Erstellen Sie eine Keytab-Datei für das LDAP-Bind-Benutzerkonto, das während der LDAP-Synchronisierung für den Zugriff auf und das Durchsuchen von Active Directory verwendet wird.

Strukturieren Sie den Wert für die Option „-princ“ als <principal name>@<KERBEROS REALM>. Nehmen Sie den Namen der LDAP-Konfiguration für den Active Directory-Server in den Namen der Keytab-Datei auf. Verwenden Sie für den Namen der Keytab-Datei folgende Struktur: <Active Directory LDAP configuration_name>.keytab.

Im folgenden Beispiel wird eine Keytab-Datei für ein Dienstprinzipalbenutzerkonto mit dem Namen „ldapuser“ erstellt.

```
ktpass.exe -out ActiveDirectoryServer1.keytab -princ ldapuser@COMPANY.COM -mapuser ldapuser -crypto all -ptype KRB5_NT_PRINCIPAL
```

Überprüfen der Dienstprinzipalnamen und Keytab-Dateien

Sie können Kerberos-Dienstprogramme verwenden, um zu überprüfen, ob die SPNs und die Keytab-Dateien gültig sind. Mit den Dienstprogrammen können Sie außerdem den Status des Kerberos-Schlüsselverteilungszentrums (KDC) ermitteln.

Sie können Kerberos-Dienstprogramme wie *kinit* und *klist* verwenden, um die SPNs und die Keytab-Dateien anzuzeigen und zu überprüfen. Stellen Sie zum Verwenden der Dienstprogramme sicher, dass die Umgebungsvariable `KRB5_CONFIG` den Pfad und den Dateinamen der Kerberos-Konfigurationsdatei enthält. 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:

kinit

Sie können das Dienstprogramm *kinit* verwenden, um ein Ticket-Granting-Ticket (TGT) vom KDC anzufordern und zu überprüfen, dass eine Keytab-Datei zum Einrichten einer Kerberos-Verbindung verwendet werden kann. Wenn die Keytab und der angegebene SPN gültig sind, ruft der Befehl ein Ticket ab und speichert das Ticket im angegebenen Zwischenspeicher.

Das Dienstprogramm „kinit“ ist in folgendem Verzeichnis auf einem Informatica-Knoten verfügbar:

```
<Informatica-Installationsverzeichnis>\java\jre\bin
```

Führen Sie zum Anfordern eines Ticket-Granting-Tickets für einen SPN den folgenden Befehl aus:

```
kinit -c <cache name> -k -t <Keytab-Dateiname> <Dienstprinzipalname>
```

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

```
Cache: \temp\krb Using principal: isp/node01/Infadomain/COMPANY.COM Using keytab: node01.keytab Authenticated to Kerberos v5
```

klist

Sie können das Dienstprogramm *klist* zum Auflisten der Kerberos-Prinzipale und Schlüssel in einer Keytab-Datei verwenden. 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-Dateiname>
```

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

```
Keytab name: FILE:node01.keytab KVNO Timestamp Principal ----
----- 3 12/31/16 19:00:00 MRS_dev/
node01/Infadomain@COMPANY.COM 3 12/31/16 19:00:00 MRS_dev/node01/
Infadomain@COMPANY.COM 3 12/31/16 19:00:00 MRS_dev/node01/Infadomain@COMPANY.COM 3
12/31/16 19:00:00 MRS_dev/node01/Infadomain@COMPANY.COM
```

Aktivieren der Kerberos-Authentifizierung

Sie können Kerberos-Authentifizierung in einer Informatica-Domäne während oder nach der Installation der Informatica-Dienste aktivieren.

Wenn Sie die Kerberos-Authentifizierung während der Installation nicht aktivieren, führen Sie die Schritte in diesem Abschnitt aus, um Informatica-Befehlszeilenprogramme zur Aktivierung der Kerberos-Authentifizierung zu verwenden, nachdem Sie die Dienste installiert haben.

Aktivieren der Kerberos-Authentifizierung in der Domäne

Aktivieren Sie Kerberos auf einem Gateway-Knoten innerhalb der Domäne.

Führen Sie den `infasetup`-Befehl „`switchToKerberosMode`“ auf einem Gateway-Knoten innerhalb der Domäne aus, um die Authentifizierung in die Kerberos-Netzwerkauthentifizierung zu ändern.

1. Fahren Sie die Domäne und alle Informatica-Dienste herunter. Fahren Sie die Dienste in der nachstehenden Reihenfolge herunter:
 - Metadata Manager-Dienst
 - PowerCenter®-Integrationsdienst

- PowerCenter®-Repository-Dienst
 - Content-Management-Dienst
 - Analyst-Dienst
 - Datenintegrationsdienst
 - Modellrepository-Dienst
2. Wechseln Sie an der Eingabeaufforderung auf einem Gateway-Knoten zu dem Verzeichnis, in dem sich die ausführbare infasetup-Datei befindet:

```
<Informatica-Installationsverzeichnis>\isp\bin
```

3. Führen Sie den folgenden Befehl aus:

```
infasetup switchToKerberosMode -ad <administrator name> -srn <Kerberos realm names> -  
urn <Kerberos realm names> -spnSL <service principal level>
```

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

Option	Argument	Beschreibung
-administratorName -ad	user_name	<p>Benutzername für das Domänenadministrator-Konto, das beim Konfigurieren der Kerberos-Authentifizierung erstellt wird. Geben Sie den Namen eines Kontos an, das in Active Directory vorhanden ist.</p> <p>Nachdem Sie die Kerberos-Authentifizierung konfiguriert haben, wird dieser Benutzer in die Sicherheitsdomäne <i>_infaInternalNamespace</i> aufgenommen, die vom Befehl erstellt wird.</p> <p>Wenn in der Domäne ein einzelner Kerberos-Bereich zum Authentifizieren der Benutzer verwendet wird, geben Sie den Namen „samAccount“ des Kontos an, das als Administratorkonto verwendet werden soll.</p> <p>Wenn in der Domäne die bereichsübergreifende Kerberos-Authentifizierung verwendet wird, geben Sie den vollqualifizierten Benutzerprinzipalnamen einschließlich des Bereichsnamens für das Konto an, das als Administratorkonto verwendet werden soll. Beispiel: sysadmin@COMPANY.COM</p>
-ServiceRealmName -srn	Kerberos_realm_name	<p>Name des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird. Der Bereichsname muss in Großbuchstaben angegeben werden und unterliegt der Groß-/Kleinschreibung.</p> <p>Zum Konfigurieren der bereichsübergreifenden Kerberos-Authentifizierung geben Sie den Namen des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird, getrennt durch Kommas ein. Beispiel: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM</p> <p>Verwenden Sie ein Sternchen als Platzhalterzeichen vor dem Bereichsnamen, um alle Bereiche mit diesem Namen einzuschließen. Beispiel: *EAST.COMPANY.COM</p>

Option	Argument	Beschreibung
-UserRealmName -urn	Kerberos_realm_name	<p>Name des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird. Der Bereichsname muss in Großbuchstaben angegeben werden und unterliegt der Groß-/Kleinschreibung.</p> <p>Zum Konfigurieren der bereichsübergreifenden Kerberos-Authentifizierung geben Sie den Namen des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird, getrennt durch Kommas ein. Beispiel:</p> <p>COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM</p> <p>Verwenden Sie ein Sternchen als Platzhalterzeichen vor dem Bereichsnamen, um alle Bereiche mit diesem Namen einzuschließen. Beispiel:</p> <p>*EAST.COMPANY.COM</p>
-SPNShareLevel -spnSL	NODE PROCESS	<p>Dienstprinzipalebene für die Domäne.</p> <p>Legen Sie NODE fest, um Kerberos auf Knotenebene zu aktivieren.</p> <p>Legen Sie PROCESS fest, um Kerberos auf Prozessebene zu aktivieren.</p>

Im folgenden Beispiel wird die Domänenauthentifizierung in Kerberos geändert, wobei das sysadmin-Benutzerkonto in einer Domäne, die einen einzelnen Kerberos-Bereich zum Authentifizieren von Benutzern verwendet, als Administratorkonto festgelegt wird:

```
infasetup switchToKerberosMode -ad sysadmin -srn COMPANY.COM -urn COMPANY.COM -spnSL
NODE
```

Im folgenden Beispiel wird die Domänenauthentifizierung in Kerberos geändert, wobei das sysadmin-Benutzerkonto in einer Domäne, die bereichsübergreifende Kerberos-Authentifizierung verwendet, als Administratorkonto festgelegt wird:

```
infasetup switchToKerberosMode -ad sysadmin@COMPANY.COM -srn
COMPANY.COM,COMPANY.EAST.COM,COMPANY.WEST.COM -urn
COMPANY.COM,COMPANY.EAST.COM,COMPANY.WEST.COM -spnSL NODE
```

Aktualisieren der Knoten in der Domäne

Aktualisieren Sie alle Gateway- und Worker-Knoten mit den Informationen des Kerberos-Authentifizierungsservers, außer den Gateway-Knoten, auf denen Sie den Befehl „switchToKerberosMode“ ausgeführt haben.

Verwenden Sie die folgenden Befehle, um die Gateway- und Worker-Knoten zu aktualisieren:

infasetup UpdateGatewayNode

Verwenden Sie den UpdateGatewayNode-Befehl, um die Kerberos-Authentifizierungsparameter auf einem Gateway-Knoten in der Domäne festzulegen. 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 die Kerberos-Authentifizierungsparameter auf einem Worker-Knoten in der Domäne festzulegen. Wenn die Domäne mehrere Worker-Knoten aufweist, führen Sie den UpdateWorkerNode-Befehl auf jedem Worker-Knoten aus.

1. Wechseln Sie an der Eingabeaufforderung auf einem Knoten zu dem Verzeichnis, in dem sich die ausführbare infasetup-Datei befindet.

```
<Informatica-Installationsverzeichnis>\isp\bin
```

2. Um die Kerberos-Authentifizierungsparameter auf einem Gateway-Knoten festzulegen, führen Sie den folgenden Befehl aus:

```
infasetup UpdateGatewayNode -krb <true|false> -srn <Kerberos realm names> -urn  
<Kerberos realm names>
```

Um die Kerberos-Authentifizierungsparameter auf einem Worker-Knoten festzulegen, führen Sie den folgenden Befehl aus:

```
infasetup UpdateWorkerNode -krb <true|false> -srn <Kerberos realm names> -urn  
<Kerberos realm names>
```

In der folgenden Tabelle werden die Optionen und Argumente beschrieben, die zur Aktivierung von Kerberos-Authentifizierung auf einem Knoten erforderlich sind:

Option	Argument	Beschreibung
-EnableKerberos -krb	true false	Konfiguriert die Informatica-Domäne zur Verwendung der Kerberos-Authentifizierung. Legen Sie die Eigenschaft auf „true“ fest, um Kerberos-Authentifizierung zu aktivieren. Der Standardwert ist „false“.
-ServiceRealmName -srn	Kerberos_realm_name	Name des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird. Der Bereichsname muss in Großbuchstaben angegeben werden und unterliegt der Groß-/Kleinschreibung. Zum Konfigurieren der bereichsübergreifenden Kerberos-Authentifizierung geben Sie den Namen des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird, getrennt durch Kommas ein. Beispiel: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Verwenden Sie ein Sternchen als Platzhalterzeichen vor dem Bereichsnamen, um alle Bereiche mit diesem Namen einzuschließen. Beispiel: *EAST.COMPANY.COM
-UserRealmName -urn	Kerberos_realm_name	Name des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird. Der Bereichsname muss in Großbuchstaben angegeben werden und unterliegt der Groß-/Kleinschreibung. Zum Konfigurieren der bereichsübergreifenden Kerberos-Authentifizierung geben Sie den Namen des Kerberos-Bereichs, der von der Domäne zum Authentifizieren von Benutzern verwendet wird, getrennt durch Kommas ein. Beispiel: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Verwenden Sie ein Sternchen als Platzhalterzeichen vor dem Bereichsnamen, um alle Bereiche mit diesem Namen einzuschließen. Beispiel: *EAST.COMPANY.COM

Im folgenden Beispiel wird ein Worker-Knoten zur Verwendung der Kerberos-Authentifizierung aktualisiert:

```
infasetup updateWorkerNode -krb true -srn COMPANY.COM -urn COMPANY.COM
```

Im folgenden Beispiel wird ein Worker-Knoten zur Verwendung der bereichsübergreifenden Kerberos-Authentifizierung aktualisiert:

```
infasetup updateWorkerNode -krb true -srn  
COMPANY.COM,COMPANY.EAST.COM,COMPANY.WEST.COM -urn  
COMPANY.COM,COMPANY.EAST.COM,COMPANY.WEST.COM
```

Aktivieren von Kerberos auf Informatica-Knoten

Nachdem Sie Kerberos in der Domäne aktiviert haben, müssen Sie die Kerberos-Konfigurationsdatei auf jeden Knoten in der Domäne kopieren. Außerdem müssen Sie die Webbrowser für den Zugriff auf Informatica-Webanwendungen konfigurieren.

Kopieren Sie die Keytab-Dateien auf jedem Knoten in folgendes Verzeichnis:

```
<Informatica-Installationsverzeichnis>\isp\config\keys
```

Welche Keytab-Dateien kopiert werden, hängt davon ab, ob Sie Kerberos-Authentifizierung auf Knotenebene oder auf Prozessebene aktivieren.

Keytab-Dateien auf Knotenebene

Kopieren Sie jede auf Knotenebene generierte Keytab-Datei auf den entsprechenden Knoten.

Die folgende Tabelle zeigt den Knoten, auf den jede Keytab-Datei kopiert wird:

Keytab-Datei	Speicherort auf dem Knoten
<Knotenname>.keytab	Kopieren Sie jede Datei auf den entsprechenden Knoten.
webapp_http.keytab	Kopieren Sie jede Datei auf den entsprechenden Gateway-Knoten.
ldapuser.keytab	Kopieren Sie die Datei auf jeden Gateway-Knoten.

Keytab-Dateien auf Prozessebene

Kopieren Sie jede auf Prozessebene generierte Keytab-Datei auf den entsprechenden Knoten.

Die folgende Tabelle zeigt den Knoten, auf den jede Keytab-Datei kopiert wird:

Keytab-Datei	Speicherort auf dem Knoten
<Knotenname>.keytab	Kopieren Sie jede Datei auf den entsprechenden Knoten.
webapp_http.keytab	Kopieren Sie jede Datei auf den entsprechenden Gateway-Knoten.
_AdminConsole.keytab	Kopieren Sie jede Datei auf den entsprechenden Gateway-Knoten.

Keytab-Datei	Speicherort auf dem Knoten
<Anwendungsdienstname>.keytab	Kopieren Sie jede Datei auf den entsprechenden Knoten, auf dem der Informatica-Anwendungsdienst ausgeführt wird.
ldapuser.keytab	Kopieren Sie die Datei auf jeden Gateway-Knoten.

Konfigurieren Sie Webbrowser für den Zugriff auf Informatica-Webanwendungen.

Fügen Sie in Microsoft Internet Explorer und Google Chrome die URL der Informatica-Webanwendungen wie z. B. des Analyst Tools zur Liste der vertrauenswürdigen Sites hinzu.

Wenn Sie Chrome Version 41 oder höher verwenden, müssen Sie auch die Richtlinien AuthServerWhitelist und AuthNegotiateDelegateWhitelist verwenden.

Kopieren der Keytab-Dateien auf die Informatica-Knoten

Nachdem Sie die Keytab-Dateien erstellt haben, kopieren Sie jede Keytab-Datei auf den entsprechenden Knoten.

Kopieren Sie die Keytab-Dateien auf jedem Knoten in folgendes Verzeichnis:

```
<Informatica-Installationsverzeichnis>\isp\config\keys
```

Welche Keytab-Dateien kopiert werden, hängt davon ab, ob Sie Kerberos-Authentifizierung auf Knotenebene oder auf Prozessebene aktivieren.

Keytab-Dateien auf Knotenebene

Kopieren Sie jede auf Knotenebene generierte Keytab-Datei auf den entsprechenden Knoten.

Die folgende Tabelle zeigt den Knoten, auf den jede Keytab-Datei kopiert wird:

Keytab-Datei	Speicherort auf dem Knoten
<Knotenname>.keytab	Kopieren Sie jede Datei auf den entsprechenden Knoten.
webapp_http.keytab	Kopieren Sie jede Datei auf den entsprechenden Knoten.
ldapuser.keytab	Kopieren Sie die Datei auf jeden Gateway-Knoten.

Keytab-Dateien auf Prozessebene

Kopieren Sie jede auf Prozessebene generierte Keytab-Datei auf den entsprechenden Knoten.

Die folgende Tabelle zeigt den Knoten, auf den jede Keytab-Datei kopiert wird:

Keytab-Datei	Speicherort auf dem Knoten
<Knotenname>.keytab	Kopieren Sie jede Datei auf den entsprechenden Knoten.
webapp_http.keytab	Kopieren Sie jede Datei auf den entsprechenden Knoten.
_AdminConsole.keytab	Kopieren Sie jede Datei auf den entsprechenden Knoten.

Keytab-Datei	Speicherort auf dem Knoten
<Anwendungsdienstname>.keytab	Kopieren Sie jede Datei auf den entsprechenden Knoten, auf dem der Informatica-Anwendungsdienst ausgeführt wird.
Idapuser.keytab	Kopieren Sie die Datei auf jeden Knoten.

Aktivieren der Kerberos-Authentifizierung für Informatica-Clients

Kopieren Sie die Kerberos-Konfigurationsdatei auf jeden Computer, der einen Informatica-Client hostet, und legen Sie dann eine Umgebungsvariable fest, um auf die Konfigurationsdatei zu zeigen. Außerdem müssen Sie den Client-Browsern den Zugriff auf Informatica-Webanwendungen ermöglichen.

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 jeden Informatica-Clienthost.

Kopieren Sie die Datei `krb5.conf` auf jeden Computer, der einen Informatica-Client hostet, wie z. B. der PowerCenter Client oder Informatica Developer (das Developer Tool). Kopieren Sie die Datei in folgendes Verzeichnis auf jedem Host:

```
<Informatica-Installationsverzeichnis>\clients\shared\security
```

Legen Sie die Umgebungsvariable KRB5_CONFIG auf jedem Informatica-Clienthost fest.

Legen Sie die Umgebungsvariable KRB5_CONFIG auf den Pfad und Dateinamen der Kerberos-Konfigurationsdatei auf jedem Computer fest, der Informatica-Clients wie den PowerCenter-Client und das Developer Tool hostet.

Konfigurieren Sie Webbrowser für den Zugriff auf Informatica-Webanwendungen.

Fügen Sie in Microsoft Internet Explorer und Google Chrome die URL der Informatica-Webanwendungen wie z. B. des Analyst Tools zur Liste der vertrauenswürdigen Sites hinzu.

Wenn Sie Chrome Version 41 oder höher verwenden, müssen Sie auch die Richtlinien `AuthServerWhitelist` und `AuthNegotiateDelegateWhitelist` verwenden.

Aktivieren von Kerberos für die Hadoop-Integration

Um Zuordnungen auf einem Kerberos-fähigen Cluster auszuführen und Metadaten über das Developer Tool anzuzeigen, führen Sie Konfigurationsaufgaben im Administrator Tool und auf jedem Developer Tool-Computer durch.

Führen Sie die folgenden Aufgaben durch:

- Konfigurieren der Kerberos-Konfigurationsdatei
- Erstellen von Benutzerauthentifizierungsartefakten
- Konfigurieren der Kerberos-Authentifizierungseigenschaften für die Informatica-Domäne
- Importieren von Konfigurationsdateien auf jeden Developer-Tool-Computer
- Generieren einer Kerberos-Anmeldeinformationsdatei für den Developer Tool-Computer

Um zu erfahren, wie Sie diese Aufgaben ausführen, lesen Sie das Kapitel über das Ausführen von Zuordnungen mit Kerberos-Authentifizierung im *Data Engineering-Administratorhandbuch*.

Aktivieren von Benutzerkonten für die Verwendung von Kerberos-Authentifizierung

Nachdem Sie Kerberos-Authentifizierung in der Domäne aktiviert haben, importieren Sie Informatica-Benutzerkonten aus Active Directory in die LDAP-Sicherheitsdomäne, die Kerberos-Benutzerkonten enthält. Sie müssen auch die Gruppen, Rollen, Rechte und Berechtigungen aus der nativen Sicherheitsdomäne zu den entsprechenden Active Directory-Benutzerkonten in der LDAP-Sicherheitsdomäne migrieren, die Kerberos-Benutzerkonten enthält.

Importieren von Benutzerkonten aus Active Directory in LDAP-Sicherheitsdomänen

Importieren Sie Benutzerkonten aus Active Directory in LDAP-Sicherheitsdomänen.

Wenn Sie Kerberos-Authentifizierung in der Domäne aktivieren, erstellt Informatica eine leere LDAP-Sicherheitsdomäne mit dem gleichen Namen wie der Kerberos-Bereich. Sie können Benutzerkonten aus Active Directory in die LDAP-Sicherheitsdomäne importieren oder die Benutzerkonten in eine andere LDAP-Sicherheitsdomäne importieren.

Sie verwenden das Administrator Tool, um die Konten, die Kerberos-Authentifizierung verwenden, aus Active Directory in eine LDAP-Sicherheitsdomäne zu importieren.

Stellen Sie zum Konfigurieren der bereichsübergreifenden Kerberos-Authentifizierung eine Verbindung zum globalen Active Directory-Katalog her. Beim Herstellen einer Verbindung zum globalen Katalog importieren Sie Benutzer aus dem Active Directory-Server, der von allen Kerberos-Bereichen verwendet wird.

1. Starten Sie die Domäne und alle Informatica-Dienste.
2. Melden Sie sich bei Windows mit dem Administratorkonto an, das Sie beim Aktivieren der Kerberos-Authentifizierung in der Domäne angegeben haben.
3. Melden Sie sich am Administrator Tool an. Wählen Sie „_infalInternalNamespace“ als Sicherheitsdomäne aus.
4. Klicken Sie im Administrator Tool auf die Registerkarte **Sicherheit**.
5. Klicken Sie auf das Menü **Aktionen** und wählen Sie **LDAP-Konfiguration** aus.
6. Klicken Sie im Dialogfeld **LDAP-Konfiguration** auf die Registerkarte **LDAP-Konnektivität**.
7. Konfigurieren Sie die Verbindungseigenschaften für Active Directory.

Möglicherweise müssen Sie den LDAP-Administrator konsultieren, um die benötigten Informationen für die Verbindung zum LDAP-Server zu erhalten.

Die folgende Tabelle beschreibt die LDAP-Konfigurationseigenschaften:

Eigenschaft	Beschreibung
Servername	<p>Hostname oder IP-Adresse des Active Directory-Servers.</p> <p>Stellen Sie zum Konfigurieren der bereichsübergreifenden Kerberos-Authentifizierung eine Verbindung zum Host des globalen Active Directory-Katalogs her. Geben Sie den vollqualifizierten Hostnamen an. Beispiel:</p> <p>host.company.local</p>
Port	<p>Listenerport für den Active Directory-Server.</p> <p>Der Standardwert ist 389. Der SSL-Standardport für die Verbindung lautet 636.</p> <p>Stellen Sie zum Konfigurieren der bereichsübergreifenden Kerberos-Authentifizierung eine Verbindung zum Port des globalen Active Directory-Katalogs her. Der Standardwert ist 3268. Der SSL-Standardport für die Verbindung lautet 3269.</p>
LDAP-Verzeichnisdienst	Wählen Sie Microsoft Active Directory-Dienst aus.
Name	<p>Geben Sie das Bind-Benutzerkonto an, das Sie in Active Directory erstellt haben, um Konten in Active Directory mit der LDAP-Sicherheitsdomäne zu synchronisieren.</p> <p>Da die Domäne für Kerberos-Authentifizierung aktiviert ist, ist keine Option zum Bereitstellen eines Passworts für das Konto vorhanden.</p> <p>Wird in der Domäne die bereichsübergreifende Kerberos-Authentifizierung verwendet, schließen Sie den Namen des Bereichs ein, zu dem die Active Directory-Prinzipaldatenbank gehört.</p>
SSL-Zertifikat verwenden	Zeigt an, dass der LDAP-Server das SSL (Secure Socket Layer)-Protokoll verwendet.
LDAP-Zertifikat vertrauen	<p>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.</p>
Ohne Beachtung der Groß-/Kleinschreibung	Gibt an, dass der Dienstmanager bei der Zuweisung von Benutzern zu Gruppen die Groß- und Kleinschreibung bei DN-Attributen ignorieren muss.
Gruppenmitgliedschaft sattribut	<p>Name des Attributs, das 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 <i>member</i> oder <i>memberof</i>.</p>
Maximale Größe	<p>Maximale Anzahl an Benutzerkonten zum Importieren in eine Sicherheitsdomäne. Beispiel: Wenn der Wert auf 100 gesetzt ist, können Sie maximal 100 Benutzerkonten in die Sicherheitsdomäne importieren.</p> <p>Wenn die Anzahl der zu importierenden Benutzer 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 importieren müssen.</p> <p>Standardwert ist „1000“.</p>

8. Klicken Sie im Dialogfeld **LDAP-Konfiguration** auf die Registerkarte **Sicherheitsdomänen**.
9. Klicken Sie auf **Hinzufügen**.

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

Eigenschaft	Beschreibung
Sicherheitsdomäne	Name der LDAP-Sicherheitsdomäne, in die Sie Benutzerkonten aus Active Directory importieren möchten.
Benutzersuchbasis	Distinguished Name (DN) des Eintrags, der als Ausgangspunkt für die Suche nach Benutzernamen in Active Directory dient. Bei der Suche wird ein Objekt im Verzeichnis anhand des Pfads im Distinguished Name des Objekts gefunden. Um beispielsweise nach dem Container USERS zu suchen, der Informatica-Benutzerkonten in der Windows-Domäne example.com enthält, geben Sie CN=USERS,DC=EXAMPLE,DC=COM an.
Benutzerfilter	Eine LDAP-Abfragezeichenfolge, mit der die Kriterien für die Suche nach Benutzern im Verzeichnisdienst festgelegt wird. Der Filter kann Attributtypen, Assertionswerte und Abgleichkriterien angeben. Beispiel: (objectclass=*) sucht nach allen Objekten. (&(objectClass=user)(!(cn=susan))) sucht nach allen Benutzerobjekten mit Ausnahme von „susan“. Weitere Informationen zu Suchfiltern finden Sie in der Dokumentation für den LDAP-Verzeichnisdienst.
Gruppensuchbasis	Distinguished Name (DN) des Eintrags, der als Ausgangspunkt für die Suche nach Gruppennamen im LDAP-Verzeichnisdienst dient.
Gruppenfilter	Eine LDAP-Abfragezeichenfolge, mit der die Kriterien für die Suche nach Gruppen im Verzeichnisdienst festgelegt wird.

Die folgende Abbildung zeigt die Informationen, die benötigt werden, um LDAP-Benutzer aus Active Directory in die LDAP-Sicherheitsdomäne zu importieren, die beim Aktivieren von Kerberos in der Domäne erstellt wurde:

The screenshot shows the 'LDAP Configuration' dialog box with the 'Security Domains' tab selected. The dialog has three tabs: 'LDAP Connectivity', 'Security Domains', and 'Schedule'. Below the tabs, there is a message: 'Fields marked with an asterisk (*) are required.' and 'You can specify multiple security domains for LDAP users and groups. Click Add to add a new security domain.' To the right of this message is a green plus icon and the text 'Add'. Below this is a section titled 'Add new Security Domain' with a dropdown arrow. To the right of this section are 'Preview' and 'Cancel' buttons. The form contains five input fields: 'Security Domain *' with the value 'COMPANY.COM', 'User search base' with the value 'CN=USERS,DC=COMPANY,DC=COM', 'User filter' (empty), 'Group search base' (empty), and 'Group filter' (empty). At the bottom of the dialog are three buttons: 'Synchronize Now', 'OK', and 'Cancel'.

10. 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.

11. Klicken Sie auf **OK**, um die LDAP-Sicherheitsdomäne zu speichern.

Migrieren von nativen Benutzerrechten und -berechtigungen zur Kerberos-Sicherheitsdomäne

Wenn die Informatica-Domäne über Benutzerkonten in der nativen Sicherheitsdomäne verfügt, müssen die entsprechenden Active Directory-Benutzerkonten in der Kerberos-Sicherheitsdomäne dieselben Gruppen, Rollen, Rechte und Berechtigungen aufweisen. Migrieren Sie die Gruppen, Rollen, Rechte und Berechtigungen der nativen Benutzer auf die entsprechenden Benutzerkonten in der LDAP-Sicherheitsdomäne für Kerberos.

1. Überprüfen Sie die Liste der nativen Benutzerkonten 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 Kerberos-Sicherheitsdomäne migrieren möchten, muss über ein entsprechendes Konto im Active Directory-Dienst verfügen, den Sie für Kerberos-Authentifizierung verwenden.

2. Erstellen Sie die Benutzermigrationsdatei.

Die Benutzermigrationsdatei ist eine Nur-Text-Datei mit einer Liste von nativen Benutzern und entsprechenden Kerberos-Benutzern, die dieselben Gruppen, Rollen, Rechte und Berechtigungen benötigen.

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

```
Native/<source user name>,<LDAP security domain>/<target user name>
```

Das folgende Beispiel zeigt eine Benutzermigrationsdatei mit der folgenden Liste von Benutzern, die zur Sicherheitsdomäne COMPANY.COM migriert werden sollen:

```
Native/User1,COMPANY.COM/User1
Native/User2,COMPANY.COM/User2
Native/User3,COMPANY.COM/User3
```

3. Führen Sie den Befehl „infacmd isp migrateUsers“ aus, um Kontorechte und -berechtigungen in der nativen Sicherheitsdomäne an die Konten in der Kerberos-Sicherheitsdomäne zu migrieren.

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

```
infacmd isp migrateUsers -dn <domain name> -un <administrator user name> -pd
<administrator password> -sdn <security domain> -umf <user migration file>
```

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

Option	Beschreibung
-DomainName -dn	Name der Informatica-Domäne.
-UserName -un	Benutzername zum Herstellen einer Verbindung zur Domäne. Geben Sie den Benutzernamen des Administratorkontos an, den Sie im Befehl „infasetup switchToKerberosMode“ angegeben haben.
-Password -pd	Passwort für das Administratorkonto.
-SecurityDomain -sdn	LDAP-Sicherheitsdomäne des Administratorkontos, das für die Verbindung zur Domäne verwendet wird. Geben Sie „_infaInternalNamespace“ an.
-UserMigrationFile -umf	Pfad und Dateiname der Benutzermigrationsdatei. Der Befehl überspringt Einträge mit einem doppelten Quell- oder Zielbenutzernamen.

Im folgenden Beispiel werden die Gruppen, Rollen, Rechte und Berechtigungen für Benutzer basierend auf der Benutzermigrationsdatei um_s.txt migriert:

```
infacmd isp migrateUsers -dn InfaDomain -un nodeuser01 -pd password -sdn
_infaInternalNamespace -umf C:\Infa\um_s.txt
```

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

Mit dem Befehl „migrateUsers“ wird eine detaillierte Protokolldatei mit dem Namen infacmd_uml_<date>_<time>.txt in dem Verzeichnis erstellt, in dem der Befehl ausgeführt wird.

Kerberos-Delegierung

Die Kerberos-Delegierung ermöglicht einem Kerberos-Dienst, die Identität eines Kerberos-Clientbenutzers anzunehmen und im Namen des Clientbenutzers ein Dienstticket für einen anderen Dienst zu erhalten.

Die Dienste in einer Informatica-Domäne müssen eine Verbindung zu anderen Diensten herstellen, um einen Vorgang abzuschließen. Sie können über delegierte Authentifizierung eine Verbindung zu anderen Diensten herstellen. Wenn ein Benutzer bei der delegierten Authentifizierung von einem Dienst authentifiziert wird, verwendet der Dienst diese Anmeldeinformationen, um eine Verbindung mit einem anderen Dienst herzustellen. Wenn beispielsweise ein pmcmd-Benutzer auf den Power Center-Integrationsdienst zugreift, fungiert der Dienst als pmcmd-Benutzer, um sich beim Power Center Repository-Dienst zu authentifizieren.

Arten der Kerberos-Delegierung

Wenn Sie die delegierte Authentifizierung verwenden, können Sie einen der folgenden Delegierungstypen auswählen:

Vollständige Delegierung

Die vollständige Delegierung ist die anfängliche Implementierung der Kerberos-Delegierung. Bei dieser Delegierungsmethode leitet ein Client sein Ticket Granting Ticket (TGT) nach der Kerberos-Authentifizierung an einen Dienst weiter. Der Dienst verwendet das TGT, um Diensttickets für den Zugriff auf einen beliebigen anderen Dienst im Netzwerk zu erhalten. Diese Art der Delegierung gilt nicht als sicher, da ein Administrator die Dienste, auf die der Server mit der Clientidentität zugreifen kann, nicht steuern kann. Die vollständige Delegierung wird auch als uneingeschränkte Delegierung bezeichnet.

Ressourcenbasierte eingeschränkte Delegierung

Mit der ressourcenbasierten eingeschränkten Delegierung können Administratoren die Verwendung der Clientidentität durch die Dienste einschränken. Bei dieser Delegierungsmethode leitet der Client TGT nicht an den Server weiter. Bei dieser Methode geben die Dienste an, wem sie vertrauen und wer die Authentifizierung an sie delegieren kann.

Die eingeschränkte Delegierung verwendet Kerberos-Protokollerweiterungen mit der Bezeichnung „Service for User (S4U)“, die es einem Dienst ermöglichen, ein Kerberos-Dienstticket im Namen eines Benutzers abzurufen.

Hinweis: Sie können die eingeschränkte Delegierung nicht zusammen mit der vollständigen Delegierung in ein und derselben Domäne verwenden. Sie können die Domäne so konfigurieren, dass entweder die vollständige Delegierung oder die eingeschränkte Delegierung verwendet wird.

Service for User (S4U)-Erweiterung

Service for User (S4U)-Erweiterungen ermöglichen einem Dienst, ein Kerberos-Dienstticket im Namen eines Benutzers abzurufen. Im Folgenden sind die zwei Arten von S4U-Erweiterungen aufgeführt:

- Service for User to Self (S4U2Self). Diese Erweiterung ermöglicht es einem Dienst, im Namen eines Clientbenutzers ein Dienstticket für sich selbst zu erhalten.
- Service for User to Proxy (S4U2Proxy). Diese Erweiterung ermöglicht es einem Dienst, im Namen eines Clientbenutzers ein Dienstticket für einen anderen Dienst zu erhalten. Um S4U2Proxy auszuführen, benötigt ein Dienst ein Dienstticket für sich selbst. Das Dienstticket kann vom Clientbenutzer vorgelegt oder über die S4U2Self-Erweiterung bezogen werden.

Weitere Informationen zu den S4U-Erweiterungen finden Sie in der Microsoft-Dokumentation.

Aktivieren der ressourcenbasierten eingeschränkten Delegierung mit S4U2Self

Stellen Sie sicher, dass das Weiterleitungs-Flag im Abschnitt „libdefaults“ der Datei krb5.conf auf TRUE festgelegt ist.

Sie können die ressourcenbasierte eingeschränkte Delegierung nur über Powershell-Befehle konfigurieren. Stellen Sie sicher, dass Powershell von einem Benutzer mit den erforderlichen Berechtigungen zum Ändern der Eigenschaften von KDC-Konten gestartet wird, vorzugsweise von einem KDC-Administrator.

Um die ressourcenbasierte eingeschränkte Delegierung mit S4U2Self zu aktivieren, führen Sie die folgenden Schritte für jedes Informatica-Keytab-Konto auf dem KDC-Server aus:

1. Klicken Sie mit der rechten Maustaste auf das Benutzerkonto und wählen Sie **Eigenschaften** aus.
Das Dialogfeld **Eigenschaften** wird angezeigt.
2. Klicken Sie auf der Registerkarte **Delegierung** auf **Diesem Computer nicht für die Delegierung vertrauen**.
3. Klicken Sie auf **Anwenden**.

4. Führen Sie den folgenden Befehl aus, um das Attribut `PrincipalsAllowedToDelegateToAccount` festzulegen:

```
$IntermediateService = Get-ADUser -Identity <samAccountName des Zwischenserverkontos> -  
Properties *
```

```
Set-ADUser -Identity <samAccountName des Zielservers> -  
PrincipalsAllowedToDelegateToAccount $IntermediateService1, $IntermediateService2,  
$IntermediateService3
```

Hinweis: Sie können durch Kommas getrennte Werte verwenden, um mehrere Konten im Attribut `PrincipalsAllowedToDelegateToAccount` hinzuzufügen.

5. Wenn Sie die Einstellung des Attributs `PrincipalsAllowedToDelegateToAccount` aufheben möchten, führen Sie den folgenden Befehl aus:

```
Set-ADUser -Identity <samAccountName des Zielservers>  
PrincipalsAllowedToDelegateToAccount $null
```

6. Um vorhandene Prinzipale in der Liste `PrincipalsAllowedToDelegateToAccount` anzuzeigen, führen Sie die folgenden Befehle aus:

```
$FormatEnumerationLimit=-1  
Get-ADUser -Identity <sam-Kontoname> -properties  
PrincipalsAllowedToDelegateToAccount
```

Hinweis: Standardmäßig zeigt die Ausgabe des Powershell-Befehls vier Werte in der Dienstprinzipalliste in der Ausgabe an. Setzen Sie diesen Parameter auf -1, um die vollständige Liste der Prinzipale anzuzeigen.

Aktivieren der vollständigen Delegierung für die Kerberos-Prinzipalbenutzerkonten in Active Directory

Erstellen Sie die Keytab-Dateien mit dem `ktpass`-Befehl.

Damit Sie die vollständige Delegierung verwenden können, müssen Sie die Delegierung für alle von Ihnen erstellten Konten aktivieren, mit Ausnahme des LDAP-Bind-Benutzerkontos, das Sie zum Zugriff auf und Durchsuchen von Active Directory während der LDAP-Synchronisierung verwenden.

Führen Sie die folgenden Schritte für jedes Benutzerkonto aus, um die vollständige Delegation zu aktivieren:

1. Klicken Sie mit der rechten Maustaste auf das Benutzerkonto und wählen Sie **Eigenschaften** aus.
Das Dialogfeld **Eigenschaften** wird angezeigt.
2. Klicken Sie auf der Registerkarte **Delegation** auf **Diesem Benutzer nur für die Delegation an beliebige Dienste vertrauen (nur Kerberos)**.
3. Klicken Sie auf **Anwenden**.
Die vollständige Delegation ist aktiviert.

Wechseln von der vollständigen Delegation zur eingeschränkten Delegation

Wenn Sie die vollständige Delegation verwenden und die eingeschränkte Delegation verwenden möchten, führen Sie die folgenden Schritte aus.

1. Fahren Sie die Domäne herunter.
2. ["Aktivieren der ressourcenbasierten eingeschränkten Delegation mit S4U2Self" auf Seite 67](#) für vorhandene Active Directory-Benutzer, die mit einem Keytab-Konto auf dem KDC-Server verknüpft sind.
3. Starten Sie die Domäne.

KAPITEL 5

SAML-Authentifizierung für Informatica-Webanwendungen

Dieses Kapitel umfasst die folgenden Themen:

- [SAML-Authentifizierung - Übersicht, 69](#)
- [SAML-Authentifizierungsprozess, 71](#)
- [Aktivieren von SAML-Authentifizierung in einer Domäne, 72](#)
- [Verbesserte Authentifizierungssicherheit, 75](#)
- [Konfigurieren von Webanwendungen zur Verwendung verschiedener Identitäts-Provider, 78](#)

SAML-Authentifizierung - Übersicht

Sie können die Authentifizierung anhand von Security Assertion Markup Language (SAML) für Informatica-Webanwendungen konfigurieren.

Bei SAML (Security Assertion Markup Language) handelt es sich um ein XML-basiertes Datenformat für den Austausch von Authentifizierungsinformationen zwischen einem Dienstanbieter und einem Identitäts-Provider. In einer Informatica-Domäne fungiert die Informatica-Webanwendung als Dienstanbieter.

Sie können die folgenden Informatica-Webanwendungen zur Verwendung von SAML-Authentifizierung konfigurieren:

- Informatica Administrator
- Informatica Analyst
- Massenerfassungstool
- Metadata Manager
- Enterprise Data Catalog
- Enterprise Data Preparation
- Data Privacy Management

Hinweis: SAML-Authentifizierung kann nicht in einer Informatica-Domäne verwendet werden, die zur Verwendung von Kerberos-Authentifizierung konfiguriert ist.

Wenn Sie eine Domäne zur Verwendung von SAML-Authentifizierung aktivieren, verwenden alle in der Domäne ausgeführten Webanwendungen standardmäßig den in der Domäne konfigurierten Identitäts-Provider. Sie können in einer Domäne ausgeführte Webanwendungen jedoch zur Verwendung verschiedener Identitäts-Provider konfigurieren. Sie möchten Informatica Administrator beispielsweise zur Verwendung von

AD FS als Identitäts-Provider und Informatica Analyst zur Verwendung von PingFederate als Identitäts-Provider konfigurieren.

Weitere Informationen zum Konfigurieren von Webanwendungen zur Verwendung verschiedener Identitäts-Provider finden Sie unter ["Konfigurieren von Webanwendungen zur Verwendung verschiedener Identitäts-Provider" auf Seite 78](#).

Default Keystore and Truststore Directory

The Informatica deployment includes default keystore and truststore files in the directory `<Informatica installation directory>\services\shared\security`.

Informatica recommends that you use the default keystore and truststore only for setup and proof-of-concept use cases. To secure a production environment, use the following guidelines:

- Configure a custom keystore and truststore for SAML authentication in a location other than the default directory:
`<Informatica installation directory>\services\shared\security`
- You cannot use the default keystore and truststore to configure other services or clients.
- When you enable SAML authentication, you import keystore or truststore certificate files and private keys into the default directory:
`<Informatica installation directory>\services\shared\security`
- When you assign an alias to the keystore or truststore, do not use "Informatica LLC," which Informatica uses for private key authentication and certificate signing.
- Modifying the default SAML keystore or truststore is allowed only when the default directory is configured as the SAML keystore and truststore directory and you want to import private key and certificate entries in the default keystore or truststore.

You cannot use "Informatica LLC" as the alias for new entries in default keystore and truststore. You can use "Informatica LLC" as the alias for custom keystore-truststore entries.

No other operation is allowed for the default keystore and truststore files, including deleting or replacing the files, changing the password of the keystore or truststore, or modifying, removing or replacing the Informatica-generated private key and signing certificate.

- If you replaced the default Informatica keystore and truststore files with custom keystore and truststore files in the previous Informatica installation directory structure, you must run the `infasetup UpdateGatewayNode` command to update the locations of the custom keystore and truststore for the domain.

Unterstützte Identitätsanbieter

Verwenden Sie einen unterstützten Identitätsanbieter, um die SAML-Authentifizierung in der Domäne für Webanwendungen zu verwalten.

Informatica unterstützt die folgenden Identitätsanbieter. Klicken Sie auf den Link zum How-to-Library-Artikel (H2L), um Anweisungen zur Integration zwischen den einzelnen Identitätsanbietern und der Domäne zu erhalten.

Identitätsanbieter	How-to-Library-Artikel (H2L)
Microsoft Active Directory-Verbunddienste (AD FS)	SAML Authentication with Active Directory Federation Services in Informatica 10.4.0
PingFederate	SAML Authentication with PingFederate in Informatica 10.4.0
F5 Big-IP	SAML Authentication with F5 Networks BIG-IP in Informatica 10.4.1
NetScaler	SAML Authentication with NetScaler for Web Applications
Oracle Access Manager (OAM)	SAML Authentication with Oracle Access Manager for Web Applications
Okta SSO	SAML Authentication with Okta SSO for Web Applications
Azure Active Directory	SAML Authentication with Azure Active Directory for Web Applications

Informationen zu den unterstützten Versionen dieser Identitätsanbieter finden Sie in der Produktverfügbarkeitsmatrix auf Informatica Network:
<https://network.informatica.com/community/informatica-network/product-availability-matrices>.

SAML-Authentifizierungsprozess

Informatica-Webanwendungen und der Identitäts-Provider tauschen Authentifizierungsinformationen aus, um SAML-Authentifizierung in einer Informatica-Domäne zu ermöglichen.

Die folgenden Schritte beschreiben den grundlegenden Ablauf der SAML-Authentifizierung:

1. Ein Benutzer greift auf eine Informatica-Webanwendung zu.
2. Der Benutzer wählt die Sicherheitsdomäne mit LDAP-Benutzerkonten aus, die für die SAML-Authentifizierung auf der Anmeldeseite der Anwendung verwendet werden, und klickt dann auf die Schaltfläche zum Anmelden.
Wenn der Benutzer die native Sicherheitsdomäne auswählt, gibt er einen Benutzernamen und ein Passwort ein und meldet sich bei der Anwendung an.
3. Basierend auf der Konfiguration des Identitäts-Providers wird der Benutzer aufgefordert, die Anmeldedaten für die erstmalige Authentifizierung bereitzustellen.
4. Der Identitäts-Provider überprüft die Anmeldedaten des Benutzers und erstellt eine Sitzung für den Benutzer.
Der Identitäts-Provider überprüft auch die Ziel-URL der Webanwendung und leitet den Benutzer dann an die Webanwendung mit einem SAML-Token um, das Informationen zur Identität des Benutzers enthält.
5. Die Anwendung überprüft das SAML-Token und die Benutzeridentität, erstellt eine Benutzersitzung und schließt dann den Benutzeranmeldevorgang ab.

Die vorhandene Benutzersitzung im Browser wird für nachfolgende Authentifizierungen verwendet. Für den Zugriff auf eine andere zur Verwendung von SAML-Authentifizierung konfigurierte Informatica-Webanwendung wählt der Benutzer die LDAP-Sicherheitsdomäne auf der Anmeldeseite der Anwendung aus. Der Benutzer muss weder einen Benutzernamen noch ein Passwort angeben.

Der Benutzer bleibt bei allen Informatica-Webanwendungen angemeldet, die in derselben Browsersitzung ausgeführt werden. Wenn sich der Benutzer jedoch von einer Informatica-Webanwendung abmeldet, wird er gleichfalls von anderen Informatica-Webanwendungen abgemeldet, die in derselben Browsersitzung ausgeführt werden.

Aktivieren von SAML-Authentifizierung in einer Domäne

Konfigurieren Sie den Identitäts-Provider, die Informatica-Domäne und die Knoten innerhalb der Domäne zur Verwendung der SAML-Authentifizierung.

Zum Konfigurieren von SAML-Authentifizierung für unterstützte Informatica-Webanwendungen, die in einer Domäne ausgeführt werden, führen Sie folgende Aufgaben durch:

1. Erstellen Sie eine LDAP-Konfiguration zum Herstellen einer Verbindung zum LDAP-Identitätsspeicher, der Benutzerkonten der Informatica-Webanwendung enthält. Sie erstellen auch eine LDAP-Sicherheitsdomäne und importieren die Benutzerkonten dann in die Sicherheitsdomäne.
2. Exportieren Sie das Assertionssignierzertifikat aus dem Identitäts-Provider.
3. Importieren Sie das Assertionssignierzertifikat in eine Truststore-Datei auf allen Gateway-Knoten in der Domäne. Sie können das Zertifikat in die Truststore-Standarddatei von Informatica oder in eine benutzerdefinierte Truststore-Datei kopieren.
4. Fügen Sie eine oder mehrere Vertrauensstellungen der vertrauenden Seite oder Dienstanbieter im Identitäts-Provider hinzu.
5. Fügen Sie die URL für jede Informatica-Webanwendung zum Identitäts-Provider hinzu.
6. Aktivieren Sie SAML-Authentifizierung in der Domäne.
7. Aktivieren Sie die SAML-Authentifizierung auf jedem Knoten in der Domäne.

Hinweis: Für einige der von Informatica unterstützten SAML-Identitätsanbieter können Sie detaillierte Integrationsschritte in einem H2L-Artikel (How-To Library) ausführen. Links zu den Artikeln finden Sie unter ["Unterstützte Identitätsanbieter" auf Seite 71](#).

Erstellen einer LDAP-Konfiguration für den Identitäts-Provider oder LDAP-Speicher

Erstellen Sie mithilfe des Administrator Tools eine LDAP-Konfiguration für den Identitäts-Provider oder LDAP-Speicher, der die Benutzerkonten der Webanwendung enthält, die SAML-Authentifizierung verwenden.

Beim Erstellen einer LDAP-Konfiguration wird eine Sicherheitsdomäne für die Benutzerkonten angelegt. Anschließend werden die Konten in die Sicherheitsdomäne importiert. Weisen Sie nach dem Importieren der Konten in die Sicherheitsdomäne die entsprechenden Rollen, Rechte und Berechtigungen der Informatica-Domäne zu den Konten in der Sicherheitsdomäne zu.

Weitere Informationen zum Erstellen einer LDAP-Konfiguration finden Sie unter ["Erstellen einer LDAP-Konfiguration" auf Seite 27](#).

Exportieren des Assertionssignierzertifikats

Der Identitätsanbieter sendet Authentifizierungsassertionen in Form eines Assertionssignaturzertifikats an Dienstanbieter.

Eine signierte Assertion enthält eine Signatur, die der Identitätsanbieter mithilfe eines vom Identitätsanbieteradministrator ausgewählten Algorithmus erstellt. Informatica überprüft dann die Signatur anhand des entsprechenden öffentlichen Zertifikats, das der Domänenadministrator in den SAML-Truststore importiert hat.

Informatica empfiehlt, dass Sie die signierte Assertion aktivieren.

Exportieren Sie das Assertionssignaturzertifikat vom Identitätsanbieter, um die signierte Assertion zu aktivieren.

Importieren des Zertifikats in den für SAML-Authentifizierung verwendeten Truststore

Importieren Sie das vom Identitäts-Provider verwendete Assertionssignierzertifikat in die Truststore-Datei, die für SAML-Authentifizierung auf jedem Gateway-Knoten innerhalb der Informatica-Domäne eingesetzt wird.

Sie können das Zertifikat in die standardmäßige Truststore-Datei von Informatica oder in eine benutzerdefinierte Truststore-Datei importieren.

Konfigurieren des Identitäts-Providers

Konfigurieren Sie den Identitäts-Provider zur Ausgabe von SAML-Token an Informatica-Webanwendungen.

Führen Sie die folgenden Aufgaben durch, um den Identitäts-Provider zu konfigurieren:

- Fügen Sie eine Vertrauensstellung der vertrauenden Seite für die Domäne im Identitäts-Provider hinzu. Durch die Definition als Vertrauensstellung der vertrauenden Seite kann der Identitäts-Provider Authentifizierungsanfragen von Informatica-Webanwendungen annehmen, die in der Domäne ausgeführt werden.
- Bearbeiten Sie die Regel „LDAP-Attribute als Ansprüche senden“, um LDAP-Attribute in Ihrem Identitätsspeicher zu den jeweiligen Typen zuzuordnen, die in vom Identitäts-Provider ausgegebenen SAML-Token verwendet werden.

Sie geben den Namen für die Vertrauensstellung der vertrauenswürdigen Partei ein, wenn Sie die SAML-Authentifizierung in einer Domäne aktivieren. Abhängig von den Sicherheitsanforderungen können Sie im Identitäts-Provider mehrere Vertrauensstellungen der vertrauenden Seite erstellen, um Domänen, die von verschiedenen Organisationen im Unternehmen verwendet werden, die Nutzung von SAML-Authentifizierung zu ermöglichen.

Informatica erkennt „Informatica“ als standardmäßigen Vertrauensstellungsnamen der vertrauenswürdigen Partei an. Wenn Sie eine einzelne Vertrauensstellung der vertrauenswürdigen Partei mit „Informatica“ als Vertrauensstellungsnamen erstellen, müssen Sie den Vertrauensstellungsnamen der vertrauenswürdigen Partei nicht angeben, wenn Sie die SAML-Authentifizierung in einer Domäne aktivieren.

Hinweis: Alle Zeichenfolgen im Identitäts-Provider unterliegen der Groß-/Kleinschreibung, einschließlich URLs.

Hinzufügen von Informatica-Webanwendungs-URLs zum Identitäts-Provider

Fügen Sie die URL für jede Informatica-Webanwendung, die SAML-Authentifizierung verwendet, zum Identitäts-Provider hinzu.

Stellen Sie die URL für eine Informatica-Webanwendung bereit, damit der Identitäts-Provider von der Anwendung gesendete Authentifizierungsanfragen annehmen kann. Durch Bereitstellung der URL kann der Identitäts-Provider darüber hinaus den SAML-Token an die Anwendung senden, nachdem der Benutzer authentifiziert wurde.

Einrichten der SAML-Authentifizierung in der Domäne

Sie können die SAML-Authentifizierung in einer vorhandenen Informatica-Domäne oder beim Erstellen einer Domäne aktivieren.

Wenn Sie eine Domäne zur Verwendung der SAML-Authentifizierung aktivieren, verwenden alle in der Domäne ausgeführten Webanwendungen standardmäßig den Identitätsanbieter, den Sie beim Aktivieren der SAML-Authentifizierung in der Domäne angegeben haben.

Wählen Sie eine der folgenden Optionen aus:

Aktivieren Sie SAML-Authentifizierung, wenn Sie das Informatica-Installationsprogramm ausführen.

Sie können SAML-Authentifizierung aktivieren und die URL des Identitäts-Providers angeben, wenn Sie die Domäne als Teil der Installation konfigurieren.

Aktivieren Sie SAML-Authentifizierung in einer vorhandenen Domäne.

Verwenden Sie den Befehl „infasetup updateDomainSamlConfig“, um SAML-Authentifizierung in einer vorhandenen Informatica-Domäne zu aktivieren. Sie können den Befehl auf allen Gateway-Knoten in der Domäne ausführen.

Aktivieren Sie SAML-Authentifizierung beim Erstellen einer Domäne.

Verwenden Sie den Befehl „infasetup defineDomain“, um SAML-Authentifizierung beim Erstellen einer Domäne zu aktivieren.

In der *Informatica-Befehlsreferenz* erhalten Sie Anweisungen zur Verwendung dieser Befehle.

Aktivieren der SAML-Authentifizierung auf den Knoten

Sie müssen die SAML-Authentifizierung auf jedem Gateway- und Worker-Knoten in der Informatica-Domäne konfigurieren.

Wählen Sie eine der folgenden Optionen aus, um SAML-Authentifizierung auf einem Gateway-Knoten zu konfigurieren:

Aktivieren Sie SAML-Authentifizierung, wenn Sie einen Gateway-Knoten auf einem Computer definieren.

Verwenden Sie den Befehl „infasetup DefineGatewayNode“, um SAML-Authentifizierung auf dem Gateway-Knoten zu aktivieren.

Aktivieren Sie SAML-Authentifizierung, wenn Sie einen Gateway-Knoten für den Beitritt zu einer Domäne konfigurieren, die SAML-Authentifizierung verwendet.

Verwenden Sie den Befehl „infasetup UpdateGatewayNode“, um SAML-Authentifizierung auf dem Gateway-Knoten zu aktivieren.

Aktivieren Sie SAML-Authentifizierung, wenn Sie einen Worker-Knoten in einen Gateway-Knoten umwandeln.

Verwenden Sie den Befehl „isp SwitchToGatewayNode“, um SAML-Authentifizierung auf dem Knoten zu aktivieren.

Wählen Sie eine der folgenden Optionen aus, um die SAML-Authentifizierung auf einem Worker-Knoten zu konfigurieren:

Aktivieren Sie die SAML-Authentifizierung, wenn Sie einen Worker-Knoten auf einem Computer definieren.

Verwenden Sie den Befehl „infasetup DefineWorkerNode“, um die SAML-Authentifizierung auf dem Worker-Knoten zu aktivieren.

Aktivieren Sie die SAML-Authentifizierung, wenn Sie einen Worker-Knoten für den Beitritt zu einer Domäne konfigurieren, die die SAML-Authentifizierung verwendet.

Verwenden Sie den Befehl „infasetup UpdateWorkerNode“, um die SAML-Authentifizierung auf dem Worker-Knoten zu aktivieren.

In der *Informatica-Befehlsreferenz* erhalten Sie Anweisungen zur Verwendung dieser Befehle.

Verbesserte Authentifizierungssicherheit

Sie können die Anforderungssignierung, die signierte Antwort oder die verschlüsselte Assertion aktivieren, um die Authentifizierungssicherheit zu verbessern:

Anforderungssignierung

Eine signierte Authentifizierungsanforderung enthält eine Signatur, um die Authentizität der eigentlichen Anforderung zu überprüfen. Informatica sendet in seiner Funktion als Dienstanbieter eine Authentifizierungsanforderung an den Identitätsanbieter. Um die Integrität der Anforderung aufrechtzuerhalten, kann die Authentifizierungsanforderung signiert werden.

Informatica signiert eine SAML-Anforderung mit einem privaten Schlüssel, und der Identitätsanbieter überprüft die Signatur mithilfe des entsprechenden öffentlichen Zertifikats.

Informatica sendet SAML-Authentifizierungsanforderungen über HTTP-Redirect. Die Anforderungen verwenden die Deflate-Codierung, die die Signatur in einen URL-Parameter einfügt.

Signierte Antwort

Der Identitätsanbieter antwortet auf Authentifizierungsanforderungen eines Dienstanbieters. Eine signierte Antwort enthält eine Signatur, die der Identitätsanbieter mithilfe eines vom Identitätsanbieteradministrator ausgewählten Algorithmus erstellt. Informatica überprüft dann die Signatur anhand des entsprechenden öffentlichen Zertifikats, das der Domänenadministrator in den SAML-Truststore importiert hat.

Signierte Assertion und verschlüsselte Assertion

Der Identitätsanbieter sendet Authentizitätsassertionen an Dienstanbieter.

Eine signierte Assertion enthält eine Signatur, die der Identitätsanbieter mithilfe eines vom Identitätsanbieteradministrator ausgewählten Algorithmus erstellt. Informatica überprüft dann die Signatur anhand des entsprechenden öffentlichen Zertifikats, das der Domänenadministrator in den SAML-Truststore importiert hat. Informatica empfiehlt, dass Sie die signierte Assertion aktivieren.

Informatica Administrator generiert einen asymmetrischen Schlüssel (öffentlich-privaten Schlüssel).

Die signierte Assertion kann vom Identitäts-Provider mit einem Assertionsverschlüsselungsschlüssel verschlüsselt werden, bei dem es sich um einen vom Identitäts-Provider generierten symmetrischen Schlüssel handelt.

Wenn Sie die verschlüsselte Assertion aktivieren, verschlüsselt der Identitätsanbieter den symmetrischen Schlüssel auch mit dem öffentlichen Zertifikat, das der Sicherheitsadministrator in den Identitätsanbieter importiert hat. Die SAML-Antwort enthält die verschlüsselte Assertion und einen verschlüsselten symmetrischen Schlüssel. Als Dienstanbieter entschlüsselt Informatica den verschlüsselten symmetrischen Schlüssel mit dem entsprechenden privaten Schlüssel, den Informatica Administrator in den SAML-Schlüsselspeicher importiert. Nach Erhalt des symmetrischen Schlüssels entschlüsselt Informatica die verschlüsselte Assertion.

Befolgen Sie die Schritte in diesem Abschnitt, um die Anforderungssignierung, die verschlüsselte Assertion oder die signierte Antwort zu aktivieren.

Anforderungssignierung

Sie können die Anforderungssignierung während des Installations-Upgrade-Vorgangs oder nach dem Installations-Upgrade mithilfe von `infasetup` aktivieren.

Überprüfen Sie während des Installations- oder Upgrade-Prozesses die Option **Signierte Anforderung** im Installationsprogramm.

Richten Sie nach dem Installations- oder Upgrade-Vorgang die Anforderungssignierung mit `infasetup` ein.

Sie können die Anforderungssignierung für die Webanwendungen auch mit dem Administrator Tool oder der Benutzeroberfläche der Webanwendung konfigurieren.

infasetup

Um `infasetup` zu verwenden, verwenden Sie die folgenden Optionen mit dem Befehl `infasetup`

`updateDomainSamlConfig:`

```
[<-SignSamlRequest|-ssr> sign_saml_request]
[<-RequestSigningPrivateKeyAlias|-rspa> saml_request_signing_private_key_alias]
[<-RequestSigningPrivateKeyPassword|-rspp> saml_request_signing_private_key_password]
[<-RequestSigningAlgorithm|-rsa> saml_request_signing_algorithm]
```

Details zu diesen Befehlen finden Sie in der *Informatica-Befehlsreferenz*.

Administrator-Tool

Konfigurieren Sie die Anforderungssignierung im Administrator-Tool.

1. Wählen Sie die Domäne im Domänennavigator aus.
2. Klicken Sie in den Knoteneigenschaften im Abschnitt **SAML-Konfiguration** auf das Symbol **Bearbeiten**.
3. Wählen Sie **Signaturanforderung aktivieren** aus.
4. Füllen Sie die folgenden Eigenschaften aus:
 - Alias des privaten Schlüssels für Signatur
 - Passwort des privaten Schlüssels für Signatur
 - Signieralgorithmus
5. Klicken Sie auf **OK**.
6. Starten Sie die Domäne neu.

Signierte Antwort

Aktivieren Sie die signierte Antwort, damit der Identitätsanbieter die Antworten der Authentifizierungsanforderung vom Dienstanbieter signieren kann.

Sie können die Antwortsignierung während des Installations-Upgrade-Vorgangs oder nach dem Installations-Upgrade mithilfe von `infasetup` aktivieren.

Überprüfen Sie während des Installations- oder Upgrade-Prozesses die Option **Signierte Antwort** im Installationsprogramm.

Richten Sie nach dem Installations- oder Upgrade-Vorgang die Antwortsignierung mit `infasetup` ein.

Sie können die signierte Antwort für die Webanwendungen auch mithilfe des Administrator Tools oder der Benutzeroberfläche der Webanwendung konfigurieren.

Hinweis: Der Okta SSO-Identitätsanbieter unterstützt keine signierte Antwort.

infasetup

Um `infasetup` zu verwenden, verwenden Sie die folgenden Optionen mit dem Befehl `infasetup updateDomainSamlConfig`:

```
[<-SamlResponseSigned|-srs> saml_response_signed]
[<-ResponseSigningCertificateAlias|-rsca> idp_response_signing_certificate_alias]
```

Informationen zu den Befehlen finden Sie in der *Informatica-Befehlsreferenz*.

Administrator-Tool

Konfigurieren Sie die Anforderungssignierung im Administrator-Tool.

1. Wählen Sie die Domäne im Domänennavigator aus.
2. Klicken Sie in den Knoteneigenschaften im Abschnitt **SAML-Konfiguration** auf das Symbol **Bearbeiten**.
3. Wählen Sie **Antwortsignatur aktivieren** aus.
4. Füllen Sie die Eigenschaft „Alias für Antwortsignaturzertifikat“ aus.
5. Klicken Sie auf **OK**.
6. Starten Sie die Domäne neu.

Verschlüsselte Assertion

Aktivieren Sie die verschlüsselte Assertion, damit der Identitätsanbieter die Assertionen der Authentizität mit einem symmetrischen Schlüssel verschlüsseln kann.

Sie können die Assertion-Signierung oder die verschlüsselte Assertion während des Installations-Upgrade-Vorgangs oder nach dem Installations-Upgrade mithilfe von `infasetup` aktivieren.

Überprüfen Sie während des Installations- oder Upgrade-Prozesses die Option **Assertion verschlüsseln** im Installationsprogramm.

Richten Sie nach dem Installations- oder Upgrade-Vorgang die verschlüsselte Assertion mit `infasetup` ein.

Sie können die signierte Antwort für die Webanwendungen auch mithilfe des Administrator Tools oder der Benutzeroberfläche der Webanwendung konfigurieren.

infasetup

Um **infasetup** zu verwenden, verwenden Sie die folgenden Optionen mit dem Befehl **infasetup updateDomainSamlConfig**:

```
[<-SamlAssertionEncrypted|-sae> saml_assertion_encrypted]
[<-EncryptedAssertionPrivateKeyAlias|-eapa> saml_encrypted_assertion_private_key_alias]
[<-EncryptedAssertionPrivateKeyPassword|-eapp>
saml_encrypted_assertion_private_key_password]
```

Informationen zu den Befehlen finden Sie in der *Informatica-Befehlsreferenz*.

Administrator-Tool

Konfigurieren Sie die verschlüsselte Assertion im Administrator-Tool.

1. Wählen Sie den Domänenknoten im Domänennavigator aus.
2. Klicken Sie in den Knoteneigenschaften im Abschnitt **SAML-Konfiguration** auf das Symbol **Bearbeiten**.
3. Wählen Sie **Assertion-Verschlüsselung aktivieren** aus.
4. Füllen Sie die folgenden Eigenschaften aus:
 - Alias des privaten Schlüssels der Verschlüsselungs-Assertion
 - Passwort des privaten Schlüssels der Verschlüsselungs-Assertion
5. Klicken Sie auf **OK**.
6. Starten Sie die Domäne neu.

Konfigurieren von Webanwendungen zur Verwendung verschiedener Identitäts-Provider

Sie können in einer Domäne ausgeführte Informatica-Webanwendungen zur Verwendung verschiedener Identitäts-Provider konfigurieren. Sie möchten Informatica Administrator beispielsweise zur Verwendung von AD FS als Identitäts-Provider und Informatica Analyst zur Verwendung von PingFederate als Identitäts-Provider konfigurieren.

Wenn Sie eine Domäne zur Verwendung von SAML-Authentifizierung aktivieren, verwenden alle in der Domäne ausgeführten Webanwendungen standardmäßig den Identitäts-Provider, den Sie beim Aktivieren von SAML-Authentifizierung in der Domäne angegeben haben. Wenn Sie beispielsweise AD FS als Identitäts-Provider konfigurieren, verwenden alle Webanwendungen AD FS als Identitäts-Provider, es sei denn, Sie konfigurieren eine Webanwendung zur Verwendung eines anderen Identitäts-Providers.

Sie geben den standardmäßigen Identitäts-Provider an, wenn Sie eine der folgenden Optionen zum Aktivieren von SAML-Authentifizierung verwenden:

- Beim Erstellen der Domäne und Installieren der Informatica-Dienste.
- Beim Ausführen des Befehls „infasetup defineDomain“ zum Erstellen der Domäne.
- Beim Ausführen des Befehls „infasetup updateDomainSamlConfig“ zum Aktivieren von SAML-Authentifizierung in einer vorhandenen Domäne.

Sie konfigurieren mithilfe des Administrator Tools eine Webanwendung zur Verwendung eines anderen Identitäts-Providers. Zum Konfigurieren des Administrator Tools oder der Überwachungsanwendung zur Verwendung eines anderen Identitäts-Providers ändern Sie die SAML-Konfiguration auf dem Knoten, auf dem

die Anwendung ausgeführt wird. Zum Konfigurieren weiterer Webanwendungen zur Verwendung eines anderen Identitäts-Providers ändern Sie die SAML-Konfiguration innerhalb des Anwendungsprozesses.

Vorbereiten der Verwendung eines Identitäts-Providers

Führen Sie die folgenden Aufgaben durch, um eine Informatica-Webanwendung auf die Verwendung eines Identitäts-Providers vorzubereiten.

1. Erstellen Sie eine LDAP-Konfiguration für den Identitäts-Provider-Speicher, der Benutzerkonten der Informatica-Webanwendung enthält. Sie erstellen auch eine LDAP-Sicherheitsdomäne und importieren die Benutzerkonten dann in die Sicherheitsdomäne.
2. Exportieren Sie das Assertionssignierzertifikat des Identitäts-Providers aus dem Identitäts-Provider.
3. Importieren Sie das Assertionssignierzertifikat des Identitäts-Providers in eine Truststore-Datei auf allen Gateway-Knoten in der Domäne. Sie können das Zertifikat in die Truststore-Standarddatei von Informatica oder in eine benutzerdefinierte Truststore-Datei kopieren.

Importieren Sie zum Ändern des Aliasnamens das entsprechende Zertifikat in die Truststore-Datei auf allen Gateway-Knoten und starten Sie die Knoten dann neu.
4. Fügen Sie eine oder mehrere Vertrauensstellungen der vertrauenden Seite im Identitäts-Provider hinzu und ordnen Sie LDAP-Attribute zu den jeweiligen Typen zu, die in vom Identitäts-Provider ausgegebenen Sicherheitstoken verwendet werden.
5. Fügen Sie die URL für die Informatica-Webanwendung zum Identitäts-Provider hinzu.

Konfigurieren von Informatica Administrator zur Verwendung eines Identitäts-Providers

Konfigurieren Sie mithilfe des Administrator Tools das Administrator Tool oder die Überwachungsanwendung zur Verwendung eines SAML-Identitäts-Providers. Sie konfigurieren das Administrator Tool oder die Überwachungsanwendung zur Verwendung eines Identitäts-Providers auf dem Knoten, auf dem die Anwendung ausgeführt wird.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Dienste und Knoten**.
2. Wählen Sie im Domänennavigator den Gateway-Knoten aus, auf dem das Administrator Tool und die Überwachungsanwendung ausgeführt werden.
3. Klicken Sie auf das Bearbeitungssymbol neben „SAML-Konfiguration“.
4. Geben Sie die notwendigen Eigenschaften ein, um die Anwendung zur Verwendung eines Identitäts-Providers zu aktivieren.

In der folgenden Tabelle werden die einzugebenden Verbindungseigenschaften beschrieben:

Eigenschaft	Beschreibung
URL des Identitäts-Providers	Optional. Die URL für den Server des Identitäts-Providers. Sie müssen die vollständige URL-Zeichenfolge angeben.
Dienstanbieter-ID	Optional. Der Name der Vertrauensstellung der vertrauenden Seite oder der Bezeichner des Dienstanbieters für die Domäne, die im Identitäts-Provider festgelegt ist.

Eigenschaft	Beschreibung
Alias für das Assertionssignierzertifikat	Optional. Der Aliasname, der beim Importieren des Assertionssignierzertifikats des Identitäts-Providers in die für die SAML-Authentifizierung verwendete Truststore-Datei angegeben wird. Importieren Sie zum Ändern des Aliasnamens das entsprechende Zertifikat in die Truststore-Datei auf allen Gateway-Knoten und starten Sie die Knoten dann neu.
Uhrabweichungstoleranz	Optional. Der zulässige zeitliche Unterschied zwischen der Systemuhr des Identitäts-Provider-Hosts und der Systemuhr auf dem Master-Gateway-Knoten. Optional. Die Lebensdauer der vom Identitäts-Provider ausgegebenen SAML-Token wird entsprechend der Systemuhr des Identitäts-Provider-Hosts festgelegt. Die Lebensdauer eines vom Identitäts-Provider ausgegebenen SAML-Tokens ist gültig, wenn die im Token festgelegte Start- oder Endzeit mit der in der Systemuhr auf dem Master-Gateway-Knoten angegebenen Anzahl an Sekunden übereinstimmt. Die Werte müssen zwischen 0 und 600 Sekunden liegen. Legen Sie den Wert auf -1 fest, um den für die Domäne konfigurierten Wert zu verwenden. Standardwert ist 120 Sekunden.

Die folgende Abbildung zeigt die Konfiguration, mit der das Administrator Tool zur Verwendung von AD FS als Identitäts-Provider aktiviert wird: Wenn Sie keinen Wert für eine Eigenschaft angeben, verwendet die Domäne den in der SAML-Standardkonfiguration festgelegten Wert.

Edit SAML Configuration [X]

Fields marked with an asterisk (*) are required.

Web Application ID * monitoring

Identity Provider URL

Service Provider ID

Assertion Signing Certificate Alias

Clock Skew Tolerance -1

Web Application ID * AdministratorConsole

Identity Provider URL https://server.company.com/adfs/ls/

Service Provider ID ADFS_Prod

Assertion Signing Certificate Alias adfs_cert

Clock Skew Tolerance 240

[?] [OK] [Cancel]

- Klicken Sie auf **OK**.
- Starten Sie die Anwendung neu.

Konfigurieren einer Informatica-Webanwendung

Konfigurieren Sie mithilfe des Administrator Tools eine Informatica-Webanwendung zur Verwendung eines SAML-Identitäts-Providers.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Dienste und Knoten**.
2. Wählen Sie die Anwendung oder den Anwendungsdienst im Domänennavigator aus.
 - Wählen Sie den Analyst-Dienst aus, um das Analyst Tool zur Verwendung eines Identitäts-Providers zu konfigurieren, und klicken Sie dann auf die Registerkarte **Prozesse**.
 - Wählen Sie den Massenerfassungsdienst aus, um das Massenerfassungstool zur Verwendung eines Identitäts-Providers zu konfigurieren, und klicken Sie dann auf die Registerkarte **Prozesse**.
 - Wählen Sie den Metadata Manager-Dienst aus, um die Metadata Manager-Anwendung zur Verwendung eines Identitäts-Providers zu konfigurieren, und klicken Sie dann auf die Registerkarte **Eigenschaften**.
 - Wählen Sie den Katalogdienst aus, um die Enterprise Data Catalog- oder Catalog Administrator-Anwendung zur Verwendung eines Identitäts-Providers zu konfigurieren, und klicken Sie dann auf die Registerkarte **Prozesse**.
 - Wählen Sie den Enterprise Data Preparation-Dienst aus, um die Enterprise Data Preparation-Anwendung zur Verwendung eines Identitäts-Providers zu konfigurieren, und klicken Sie dann auf die Registerkarte **Prozesse**.
 - Um die Data Privacy Management-Anwendung zur Verwendung eines Identitätsanbieters zu konfigurieren, wählen Sie den Data Privacy Management-Dienst aus und klicken Sie dann auf die Registerkarte **Prozesse**.
3. Klicken Sie auf das Bearbeitungssymbol neben **SAML-Konfiguration**.
4. Geben Sie die notwendigen Eigenschaften ein, um die Webanwendung zur Verwendung eines Identitäts-Providers zu aktivieren.

In der folgenden Tabelle werden die einzugebenden Verbindungseigenschaften beschrieben:

Eigenschaft	Beschreibung
URL des Identitäts-Providers	Optional. Die URL für den Server des Identitäts-Providers. Sie müssen die vollständige URL-Zeichenfolge angeben.
Dienstanbieter-ID	Optional. Der Name der Vertrauensstellung der vertrauenden Seite oder der Bezeichner des Dienstanbieters für die Domäne, die im Identitäts-Provider festgelegt ist.

Eigenschaft	Beschreibung
Alias für das Assertionssignierzertifikat	Optional. Der Aliasname, der beim Importieren des Assertionssignierzertifikats des Identitäts-Providers in die für die SAML-Authentifizierung verwendete Truststore-Datei angegeben wird. Importieren Sie zum Ändern des Aliasnamens das entsprechende Zertifikat in die Truststore-Datei auf allen Gateway-Knoten und starten Sie die Knoten dann neu.
Uhrabweichungstoleranz	Optional. Der zulässige zeitliche Unterschied zwischen der Systemuhr des Identitäts-Provider-Hosts und der Systemuhr auf dem Master-Gateway-Knoten. Optional. Die Lebensdauer der vom Identitäts-Provider ausgegebenen SAML-Token wird entsprechend der Systemuhr des Identitäts-Provider-Hosts festgelegt. Die Lebensdauer eines vom Identitäts-Provider ausgegebenen SAML-Tokens ist gültig, wenn die im Token festgelegte Start- oder Endzeit mit der in der Systemuhr auf dem Master-Gateway-Knoten angegebenen Anzahl an Sekunden übereinstimmt. Die Werte müssen zwischen 0 und 600 Sekunden liegen. Standardwert ist 120 Sekunden.

Die folgende Abbildung zeigt die Konfiguration, mit der Enterprise Data Catalog zur Verwendung von PingFederate als Identitäts-Provider aktiviert wird:

Edit Ldadmin SAML Configuration

Fields marked with an asterisk (*) are required.

Web Application ID: catalog_service_ldadmin

IDP URL: https://10.70.140.70:9031/idp/startSSO.saml2

Service Provider ID: PingFed_Dev

Assertion Signing Certificate Alias: pingfed_cert

Clock Skew Tolerance: 240

OK Cancel

- Klicken Sie auf **OK**.
- Starten Sie die Anwendung oder den Anwendungsdienst neu, nachdem Sie eine Anwendung zur Verwendung eines SAML-Identitäts-Providers konfiguriert haben.

KAPITEL 6

Domänensicherheit

Dieses Kapitel umfasst die folgenden Themen:

- [Domänensicherheit - Übersicht, 83](#)
- [Secure Communication Within the Domain, 84](#)
- [Sichere Verbindungen zu einem Webanwendungsdienst, 96](#)
- [Chiffre-Suites für die Informatica-Domäne, 100](#)
- [Sichere Quellen und Ziele, 104](#)
- [Secure Data Storage, 106](#)
- [Anwendungsdienste und Ports, 110](#)

Domänensicherheit - Übersicht

Sie können Optionen in der Informatica-Domäne aktivieren, um sichere Kommunikation zwischen den Komponenten in der Domäne und zwischen der Domäne und den Clientkomponenten 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 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. Nach der Installation können Sie den Verschlüsselungsschlüssel für vertrauliche Daten ändern. Sie müssen den Inhalt der Repositories aktualisieren, um die verschlüsselten Daten zu aktualisieren.

Sie können 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, z. B. dem Analyst-Dienst oder dem REST Operations Hub-Dienst, und dem Browser sichern.

Quellen und Ziele

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

Datenspeicher

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

Secure Communication Within the Domain

You can use the Secure Communication option to secure the connection between services and between services and the service managers in the domain. Additionally, you can enable security for workflows and use secure databases for the repositories that you create in the domain.

After you secure the domain, configure the Informatica client applications to work with a secure domain.

Default Directory for Keystore and Truststore

The Informatica deployment includes default keystore and truststore files in the following default directory:

```
<Informatica installation directory>\services\shared\security
```

Informatica recommends that you use the default keystore and truststore only for setup and proof-of-concept use cases.

To secure a production environment, use the following guidelines:

- When you configure secure communication, do not modify, replace, or delete files in the default directory:

```
<Informatica installation directory>\services\shared\security
```
- You cannot use the default keystore and truststore to configure other services or clients.
- Configure a custom keystore and truststore for secure communication in a location other than the default directory.
- If you replaced the default Informatica keystore and truststore files with custom keystore and truststore files in the previous Informatica installation directory structure, you must run the `infasetup UpdateGatewayNode` command to update the locations of the custom keystore and truststore for the domain.

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 SSL-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 bereitstellen, verwendet Informatica denselben privaten Standardschlüssel 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

Requirements for Secure Communication within the Domain

Before you enable secure communication within the domain, ensure that the following requirements are met:

Sie haben eine Zertifikatssignieranfrage und einen privaten Schlüssel erstellt.

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

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

Sie haben ein signiertes SSL-Zertifikat.

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

Sie haben das Zertifikat in Schlüsselspeicher importiert.

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

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

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

Sie haben das Zertifikat in Truststores importiert.

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

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

Die Schlüsselspeicher und Truststores befinden sich im richtigen Verzeichnis.

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.

You enforced the HTTP Strict Transport Security (HSTS) response header.

You can choose to enable HSTS response header in your domain to prevent man-in-the-middle (MITM) security threats. If you enable HSTS response header, you can stop HTTP redirects to HTTPS and ensure that only secured URLs (HTTPS) are accessed.

Wichtig: Informatica supports multiple applications and services running on both HTTP and HTTPS. If you enable this option, you cannot access the applications or services with HTTP URL.

To enable this option, set the `INFA_HSTS_HEADER_ENABLED` environment variable to `true` and import the certificates from `infa_truststore` and Informatica Administrator keystore to your browser.

Richtlinien für die Verwendung von Standard- und benutzerdefinierten Truststore-Dateien

Das Installationsprogramm legt die Standarddateien „infa_truststore.jks“ und „keystore“ im Verzeichnis `<Informatica installation directory>/services/shared/security` auf jedem Knoten ab. Sie können den Standard-Truststore für das Setup und die Machbarkeitsstudie verwenden. Die Standard-Truststore- und Schlüsselspeicherdateien bieten jedoch eingeschränkte Sicherheit. Für die Produktion empfiehlt Informatica die Verwendung benutzerdefinierter Truststore- und Schlüsselspeicherdateien für eine sicherere Kommunikation und SAML-Authentifizierung.

Platzieren Sie benutzerdefinierte Truststore- und Schlüsselspeicherdateien in einem benutzerdefinierten Verzeichnis. Der Truststore-Datei muss folgender Name zugewiesen werden: `infa_truststore.jks`.

Die standardmäßigen Truststore- und Schlüsselspeicherdateien sollten weder überschrieben, gelöscht noch verschoben werden. Platzieren Sie benutzerdefinierte Truststore- und Schlüsselspeicherdateien nicht im Verzeichnis `<Informatica installation directory>/services/shared/security`

Verwenden Sie beim Erstellen eines Alias für neue Zertifikate und private Schlüssel nicht den Standardnamen „Informatica LLC“, der von den standardmäßigen Truststore- und Schlüsselspeicherdateien verwendet wird.

Richtlinien zum Erstellen von Zertifikaten und benutzerdefinierten Truststore- und Schlüsselspeicherdateien

Sie können das Java-Keytool-Dienstprogramm zur Schlüssel- und Zertifikatsverwaltung zum Erstellen eines SSL-Zertifikats oder eines CSR (Certificate Signing Request) sowie von Schlüsselspeicherdateien und Truststore-Dateien im JKS-Format verwenden.

Das Keytool ist im folgenden Verzeichnis auf Domänenknoten verfügbar:

```
<Informatica installation directory>\java\bin
```

Wenn die Domänenknoten auf AIX ausgeführt werden, können Sie das bereitgestellte Keytool mit dem IBM JDK zum Erstellen eines SSL-Zertifikats oder eines CSR (Certificate Signing Request) sowie von Schlüsselspeicherdateien und Truststore-Dateien verwenden.

1. Kopieren Sie die Zertifikatsdateien in einen lokalen Ordner auf einem Gateway-Knoten innerhalb der Informatica-Domäne.
2. Wechseln Sie von der Befehlszeile zum Speicherort des Keytool-Dienstprogramms auf dem Knoten.
3. Führen Sie zum Importieren des Zertifikats das Keytool-Dienstprogramm aus.
4. Starten Sie den Knoten neu.

Next Steps

For more information about how to create a custom keystore and truststore and import certificates in your browser, see the Informatica How-To Library article [How to Create Keystore and Truststore Files for Secure Communication in the Informatica Domain](https://docs.informatica.com/data-quality-and-governance/data-quality/h2l/0700-how-to-create-keystore-and-truststore-files-for-secure-comm/abstract.html):

<https://docs.informatica.com/data-quality-and-governance/data-quality/h2l/0700-how-to-create-keystore-and-truststore-files-for-secure-comm/abstract.html>

After you secure the domain, configure the Informatica client applications to work with a secure domain.

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-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. Aktualisieren Sie die Domäne.

Führen Sie den folgenden Befehl mit den erforderlichen Optionen und Argumenten aus:

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

3. Fahren Sie die Domäne herunter.

Die Domäne muss heruntergefahren werden, bevor Sie die `infasetup`-Befehle ausführen.

4. 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. Das Verzeichnis, das die Truststore-Dateien enthält. Sie können dieselbe Truststore-Datei für mehrere Knoten verwenden.
-NodeTruststorePass -ntp	node_truststore_password	Optional, wenn Sie das Standard-SSL-Zertifikat von Informatica verwenden. Passwort für die infa_truststore.jks-Datei.

5. 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 Schlüsselspeicherdateien verwenden.

6. Starten Sie die Domäne neu.

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 aktivieren, 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-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 „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. Das Verzeichnis, das die Truststore-Dateien enthält. Sie können dieselbe Truststore-Datei für mehrere Knoten verwenden.
-NodeTruststorePass -ntp	node_truststore_password	Optional, wenn Sie das Standard-SSL-Zertifikat von Informatica verwenden. Passwort für die infa_truststore.jks-Datei.

8. 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 Schlüsselspeicherdateien verwenden.

9. Starten Sie die Domäne neu.

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

Wenn Sie sichere Kommunikation innerhalb der Domäne aktivieren, sichern Sie auch Verbindungen zwischen der Domäne und Informatica-Client-Anwendungen, wie z. B. dem Developer Tool. Sie müssen unter Umständen den Speicherort und das Passwort für die Truststore-Dateien angeben, die zum Sichern der Domäne in Umgebungsvariablen verwendet werden. Sie richten die Umgebungsvariablen auf Computern ein, auf denen Client-Anwendungen gehostet werden, die auf Dienste innerhalb der Domäne zugreifen.

SSL-Zertifikate, die zum Sichern einer Informatica-Domäne verwendet werden, befinden sich in Truststore-Dateien mit der Bezeichnung `infa_truststore.jks` und `infa_truststore.pem`. Die Truststore-Dateien müssen auf jedem Client-Host verfügbar sein.

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

INFA_TRUSTSTORE

Legen Sie diese Variable auf das Verzeichnis fest, das die Truststore-Dateien `infa_truststore.jks` und `infa_truststore.pem` enthält.

INFA_TRUSTSTORE_PASSWORD

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

Informatica stellt ein SSL-Zertifikat in Truststore-Standarddateien bereit, die Sie zum Sichern der Domäne verwenden können. Wenn Sie die Informatica-Clients installieren, legt das Installationsprogramm die Umgebungsvariablen fest und installiert die Truststore-Dateien standardmäßig in folgendem Verzeichnis:

`<Informatica installation directory>\clients\shared\security`

Wenn Sie das SSL-Standardzertifikat von Informatica verwenden und sich die Dateien `infa_truststore.jks` und `infa_truststore.pem` im Standardverzeichnis befinden, müssen Sie die Umgebungsvariable `INFA_TRUSTSTORE` oder `INFA_TRUSTSTORE_PASSWORD` nicht festlegen.

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

Sie verwenden ein benutzerdefiniertes SSL-Zertifikat zum Sichern der Domäne.

Wenn Sie ein SSL-Zertifikat zum Sichern der Domäne bereitstellen, importieren Sie das Zertifikat in die Truststore-Dateien mit der Bezeichnung `infa_truststore.jks` und `infa_truststore.pem` und kopieren Sie die Truststore-Dateien dann auf alle Client-Hosts. Sie müssen den Speicherort der Dateien und das Truststore-Passwort angeben.

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

Sie ersetzen die Truststore-Standarddateien von Informatica mit eigenen Truststore-Dateien im Standardverzeichnis.

Wenn Sie die Truststore-Standarddateien mit der Bezeichnung `infa_truststore.jks` und `infa_truststore.pem` durch eigene Truststore-Dateien im Informatica-Standardverzeichnis ersetzen, müssen Sie das Truststore-Passwort angeben. Die Truststore-Dateien müssen dieselben Dateinamen aufweisen wie die Truststore-Standarddateien.

Sie verwenden das SSL-Standardzertifikat von Informatica, die Truststore-Dateien befinden sich aber nicht im Informatica-Standardverzeichnis.

Wenn Sie das SSL-Standardzertifikat von Informatica verwenden, die Truststore-Standarddateien `infa_truststore.jks` und `infa_truststore.pem` jedoch nicht im Standardverzeichnis enthalten sind, müssen Sie den Speicherort der Dateien und das Truststore-Passwort angeben.

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

Obligatorisch. Gibt an, ob Daten bei der Netzwerkübertragung verschlüsselt werden. Dieser Parameter muss auf `SSL` festgelegt werden.

ValidateServerCertificate

Optional. Gibt an, ob Informatica das Zertifikat validiert, das der Datenbankserver sendet.

Wenn dieser Parameter auf `TRUE` gesetzt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat. Wenn Sie den Parameter `HostNameInCertificate` angeben, validiert Informatica auch den Hostnamen im Zertifikat.

Wenn dieser Parameter auf `FALSE` gesetzt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat nicht. Informatica ignoriert alle Truststore-Informationen, die Sie angeben.

Der Standardwert ist `TRUE`.

HostNameInCertificate

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

cryptoProtocolVersion

Obligatorisch. Gibt das Kryptografieprotokoll an, das für die Verbindung mit einer gesicherten Datenbank verwendet werden soll. Sie können je nach dem vom Datenbankserver verwendeten

Kryptografieprotokoll den Parameter auf `cryptoProtocolVersion=TLSv1.1` oder `cryptoProtocolVersion=TLSv1.2` einstellen.

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 „ <code>infasetup RestoreDomain</code> “ 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

Obligatorisch. Gibt an, ob Daten bei der Netzwerkübertragung verschlüsselt werden. Dieser Parameter muss auf `SSL` festgelegt werden.

ValidateServerCertificate

Optional. Gibt an, ob Informatica das Zertifikat validiert, das der Datenbankserver sendet.

Wenn dieser Parameter auf `TRUE` gesetzt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat. Wenn Sie den Parameter `HostNameInCertificate` angeben, validiert Informatica auch den Hostnamen im Zertifikat.

Wenn dieser Parameter auf `FALSE` gesetzt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat nicht. Informatica ignoriert alle Truststore-Informationen, die Sie angeben.

Der Standardwert ist `TRUE`.

HostNameInCertificate

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

cryptoProtocolVersion

Obligatorisch. Gibt das Kryptografieprotokoll an, das für die Verbindung mit einer gesicherten Datenbank verwendet werden soll. Sie können je nach dem vom Datenbankserver verwendeten Kryptografieprotokoll den Parameter auf `cryptoProtocolVersion=TLSv1.1` oder `cryptoProtocolVersion=TLSv1.2` einstellen.

TrustStore

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

Wenn Sie den Pfad für die Truststore-Datei nicht hinzufügen, sucht Informatica im folgenden Standardverzeichnis nach der Datei: `<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
- Metadata Manager-Dienst
- REST Operations Hub-Dienst
- Test Data Manager-Dienst
- Hub-Konsolendienst für Webdienste

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.

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

Sie haben ein signiertes SSL-Zertifikat.

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

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

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

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

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

Der Schlüsselspeicher muss sich in einem Verzeichnis befinden, auf das das Administrator-Tool 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 <i>changeit</i> .
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 den REST Operations Hub-Dienst

Wenn Sie den REST Operations Hub-Dienst verwenden, können Sie die sicheren HTTPS-Eigenschaften für den REST Operations Hub konfigurieren.

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

Eigenschaft	Beschreibung
HTTP-Port	Eindeutige HTTP-Portnummer für den REST Operations Hub-Dienstprozess, wenn der Dienst das HTTP-Protokoll verwendet. Der Standardwert ist 6555.
HTTPS-Port	Nummer des HTTPS-Ports, auf dem der REST Operations Hub-Dienst ausgeführt wird, wenn Sie das TLS-Protokoll (Transport Layer Security) aktivieren. Verwenden Sie eine Portnummer, die sich von der HTTP-Portnummer unterscheidet.
TLS (Transport Layer Security) aktivieren	Mit dieser Option wird eine sichere Verbindung zwischen dem REST Operations Hub-Dienst und dem REST-Client aktiviert.
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 REST Operations Hub-Dienst das Standardpasswort.
SSL-Protokoll	Bei einem leeren Feld wird die höchste der verfügbaren TLS-Versionen aktiviert. Welche TLS-Version aktiviert wird, hängt vom eingegebenen Wert ab. 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: <ul style="list-style-type: none">- 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 <i>changeit</i> .

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.

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 ["Standardliste der Chiffre-Suites" auf Seite 101](#)

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 Gültigkeitslisten:

- 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 v1.2 oder 1.3 unterstützt wird.
- Bei der Gültigkeitsliste muss es sich um eine gültige Chiffre-Suite für Windows, die Java-Laufzeitumgebung und OpenSSL handeln.

Erstellen von Listen mit Chiffre-Suites

Um die Informatica-Domäne zur Verwendung bestimmter Chiffre-Suites zu konfigurieren, erstellen Sie eine Whitelist, in der die zusätzlichen zu unterstützenden Chiffre-Suites angegeben werden. Sie können auch eine Blacklist erstellen, in der die zu blockierenden Chiffre-Suites angegeben werden.

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 kommasetrennte 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 konfigurieren die Whitelist und die Blacklist mit Infasetup. Sie können die Listen direkt in Befehlsparametern bereitstellen oder Klartextdateien angeben, die kommasetrennte 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. Verwenden Sie `infasetup`, um die Informatica-Domäne sowie die Gateway- und Worker-Knoten zu erstellen. Weitere Informationen zu Infasetup-Befehlen finden Sie in der *Informatica-Befehlsreferenz*.

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

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
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256
- TLS_AES_128_CCM_8_SHA256
-
- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256

TLS 1.3 aktivieren

Aktualisieren Sie die Chiffren für TLS 1.3.

Wenn Sie die Chiffren für eine neu definierte Domäne oder eine vorhandene Domäne aktualisieren, führen Sie die folgenden Schritte aus:

1. Fahren Sie die Domäne herunter.
2. Um die Domänen-Chiffren zu aktualisieren, führen Sie den folgenden Befehl aus:

```
./infasetup.sh updateDomainCiphers -cwl -cbl
```
3. Um den Gateway-Knoten zu aktualisieren, führen Sie den folgenden Befehl aus:

```
./infasetup.sh updategatewaynode -cwl -cbl
```
4. Starten Sie die Domäne neu.

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 listDomainCiphers -l EFFECTIVE
```

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 Profilerstellungsverbindungen 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

Obligatorisch. Gibt an, ob Daten bei der Netzwerkübertragung verschlüsselt werden. Dieser Parameter muss auf `SSL` festgelegt werden.

ValidateServerCertificate

Optional. Gibt an, ob Informatica das Zertifikat validiert, das der Datenbankserver sendet.

Wenn dieser Parameter auf `TRUE` gesetzt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat. Wenn Sie den Parameter `HostNameInCertificate` angeben, validiert Informatica auch den Hostnamen im Zertifikat.

Wenn dieser Parameter auf `FALSE` gesetzt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat nicht. Informatica ignoriert alle Truststore-Informationen, die Sie angeben.

Der Standardwert ist `TRUE`.

HostNameInCertificate

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

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.

Secure Data Storage

Informatica encrypts sensitive data, such as passwords and secure connection parameters, before it stores the data in the domain configuration repository. Informatica uses an encryption key to encrypt sensitive data.

During installation, the installer generates the encryption key for the domain. All nodes in a domain must use the same encryption key. If you install on multiple nodes, the installer uses the same encryption key for all nodes in the domain. For more information about generating an encryption key for the domain during installation, see the Informatica installation guides.

After installation, you can change the encryption key for the domain. Run the `infasetup` command to generate an encryption key and change the encryption key for the domain. After you change the encryption key for the domain, you must upgrade the content of the repositories in the domain to update the encrypted data.

Hinweis: You must keep the encryption key file in a secure location. The encryption key is required when you change the encryption key for the domain or move a repository to another domain.

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

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

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

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

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 Option encryptionKeyLocation zum Generieren eines Verschlüsselungsschlüssels an:

Option	Argument	Beschreibung
-encryptionKeyLocation -kl	encryption_key_location	Verzeichnis, das den aktuellen Verschlüsselungsschlüssel enthält. Der Name der Verschlüsselungsdatei lautet <i>sitekey</i> . Informatica benennt die aktuelle <i>sitekey</i> -Datei in <i>sitekey_old</i> um und generiert einen Verschlüsselungsschlüssel in einer neuen Datei mit dem Namen <i>sitekey</i> im selben Verzeichnis.

Hinweis: Das Installationsprogramm erstellt während der Installation und des Upgrades einen Verschlüsselungsschlüssel. Sie benötigen beim Generieren des Site-Schlüssels für die Verschlüsselungsdatei nicht die Optionen für Schlüsselwörter und Domänennamen. Stellen Sie sicher, dass Sie eine Kopie des eindeutigen Site-Schlüssels speichern. Wenn Sie den Site-Schlüssel verlieren, können Sie ihn nicht erneut generieren. Teilen Sie den eindeutigen Site-Schlüssel nicht mit anderen.

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	<p>Verzeichnis, in dem die alte Verschlüsselungsschlüsseldatei mit dem Namen <i>siteKey_old</i> und die neue Verschlüsselungsschlüsseldatei mit dem Namen <i>siteKey</i> gespeichert sind.</p> <p>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.</p> <p>Wenn die Domäne mehrere Knoten enthält, muss dieses Verzeichnis allen Knoten in der Domäne zugänglich sein, in der Sie den Befehl „migrateEncryptionKey“ ausführen.</p> <p>Wenn Sie eine Domäne mit mehreren Knoten migrieren, müssen alle Knoten in der Domäne denselben Verschlüsselungsschlüssel verwenden. Zum Ändern des Verschlüsselungsschlüssels für die Domäne führen Sie den Befehl „infasetup migrateEncryptionKey“ auf allen Knoten in der Domäne aus.</p> <p>Hinweis: Unter UNIX wird beim Dateinamen <i>siteKey_old</i> die Groß- und Kleinschreibung berücksichtigt. Wenn Sie die vorherige Verschlüsselungsschlüsseldatei manuell umbenennen, überprüfen Sie die Groß- und Kleinschreibung beim Dateinamen auf ihre Richtigkeit.</p>
-IsDomainMigrated -mig	is_domain_migrated	<p>Gibt an, ob die Domäne für die Verwendung des neuesten Verschlüsselungsschlüssels aktualisiert wurde.</p> <p>Beim erstmaligen Ausführen des Befehls „migrateEncryptionKey“ legen Sie diese Option auf FALSE fest, um anzugeben, dass die Domäne den alten Verschlüsselungsschlüssel verwendet.</p> <p>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.</p> <p>Standardwert ist „true“.</p>

- 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 Repositories mit dem neuen Verschlüsselungsschlüssel zu aktualisieren und zu verschlüsseln. Sie müssen auch den Site-Schlüssel nach dem Upgrade der Domäne migrieren.

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	<code>infacmd mrs UpgradeContents</code>
PowerCenter-Repository-Dienst	<code>pmrep Upgrade</code>

Anwendungsdienste und Ports

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

Informatica-Domäne

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

Port	Beschreibung
Dienstmanager-Port	Die vom Dienstmanager auf dem Knoten verwendete Portnummer. Der Dienstmanager überwacht eingehende Verbindungsanfragen an diesem Port. Clientanwendungen verwenden diesen Port zur Kommunikation mit den Diensten in dieser Domäne. Die Informatica-Befehlszeilenprogramme verwenden diesen Port für die Kommunikation mit der Domäne. Dies ist auch der Port für den JDBC-/ODBC-Treiber des SQL-Datendiensts. Der Standardwert ist 6006.
Schließungsport des Dienstmanagers	Die Portnummer, über die das Herunterfahren des Servers für den Dienstmanager der Domäne gesteuert wird. An diesem Port hört der Dienstmanager auf Ausschaltbefehle ab. Der Standardwert ist 6007.
Informatica Administrator-Port	Portnummer von Informatica Administrator. Der Standardwert ist 6008.

Port	Beschreibung
Informatica Administrator-HTTPS-Port	Kein Standardport. Geben Sie die erforderliche Portnummer beim Erstellen des Diensts ein. Durch Setzen dieses Ports auf 0 wird eine HTTPS-Verbindung zum Administrator Tool deaktiviert.
Informatica Administrator-Schließungsport	Portnummer, die das Herunterfahren des Servers für Informatica Administrator steuert. An diesem Port hört Informatica Administrator auf Befehle zum Herunterfahren ab. Der Standardwert ist 6009.
Niedrigste Portnummer	Niedrigste Portnummer des dynamischen Portnummernbereichs, die den auf diesem Knoten ausgeführten Anwendungsdienstprozessen zugewiesen werden kann. Der Standardwert ist 6014.
Höchste Portnummer	Höchste Portnummer des dynamischen Portnummernbereichs, die den auf diesem Knoten ausgeführten Anwendungsdienstprozessen zugewiesen werden kann. Der Standardwert ist 6114.

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.

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.

Datenintegrationsdienst

In der folgenden Tabelle wird der mit dem Datenintegrationsdienst verbundene Standardport aufgelistet:

Typ	Standardport
Datenintegrationsdienst (HTTP-Proxy)	8080
Datenintegrationsdienst (HTTP)	8095

Typ	Standardport
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.

Metadaten-Zugriffsdienst

Die folgende Tabelle listet den mit dem Metadaten-Zugriffsdienst verbundenen Standardport auf:

Typ	Standardport
Metadaten-Zugriffsdienst (HTTP)	7080 Der Metadaten-Zugriffsdienst verwendet fortlaufende Portnummern, um Verbindungen zu mehreren Hadoop-Distributionen herzustellen.
Metadaten-Zugriffsdienst (HTTPS)	Kein Standardport. Geben Sie die erforderliche Portnummer beim Erstellen des Dienstes ein. Der Metadaten-Zugriffsdienst verwendet fortlaufende Portnummern, um Verbindungen zu mehreren Hadoop-Distributionen herzustellen.

Metadata Manager-Dienst

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

Typ	Standardport
Metadata Manager-Dienst (HTTP)	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.

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 7

Sicherheitsverwaltung in Informatica Administrator

Dieses Kapitel umfasst die folgenden Themen:

- [Verwenden von Informatica Administrator - Übersicht, 114](#)
- [Benutzersicherheit, 115](#)
- [Registerkarte Sicherheit, 117](#)
- [Passwortverwaltung, 121](#)
- [Domänensicherheitsmanagement, 122](#)
- [Sicherheitsverwaltung für Benutzer, 123](#)

Verwenden von Informatica Administrator - Übersicht

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

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

- Verwaltungsaufgaben in der Domäne. Verwalten von Protokollen, Domänenobjekten, Benutzerberechtigungen und Domänenberichten. Erzeugen und Hochladen der Knotendiagnose. Überwachen der Jobs und Anwendungen des Datenintegrationsdiensts. Zu den Domänenobjekten gehören Anwendungsdienste, Knoten, Gitter, Ordner, Datenbankverbindungen, Betriebssystemprofile und Lizenzen.
- Verwaltungsaufgaben für die Sicherheit. Verwalten von Benutzern, Gruppen, Rollen und Rechten.

Im Administrator Tool gibt es folgende Registerkarten:

- **Verwalten.** Anzeigen und Bearbeiten der Eigenschaften der Domäne und der Objekte innerhalb der Domäne.
- **Überwachen.** Anzeigen des Status von Profil-, Scorecard-, Vorschau- und Zuordnungsjobs, SQL-Datendiensten, Webdiensten und Arbeitsabläufen für jeden Datenintegrationsdienst.
- **Überwachen.** Anzeigen des Status von Profil-, Vorschau- und Zuordnungsjobs, SQL-Datendiensten und Webdiensten für jeden Datenintegrationsdienst.
- **Protokolle.** Anzeigen von Protokollereignissen für die Domäne und die Dienste innerhalb der Domäne.
- **Berichte.** Ausführen eines Webdienst- oder Lizenzverwaltungsberichts.

- **Sicherheit.** Verwalten von Benutzern, Gruppen, Rollen und Rechten.
- **Cloud.** Anzeigen von Informationen zur Informatica Cloud®-Verwaltung.

Das Administrator Tool besitzt die folgenden Kopfzeileinträge:

- **Abmelden.** Abmelden beim Administrator Tool.
- **Verwalten.** Verwalten Ihres Kontos.
- **Hilfe.** Zugriff auf die Hilfe für die aktuelle Registerkarte und Bestimmen der Informatica-Version.

Benutzersicherheit

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

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
- Metadaten-Zugriffsdienst
- Metadata Manager-Dienst
- Webdienst-Hub-Dienst

Encryption

Informatica encrypts passwords sent from application clients to the Service Manager. Informatica uses AES encryption with multiple 128-bit or 256-bit keys to encrypt passwords and stores the encrypted passwords in the domain configuration database. Configure HTTPS to encrypt passwords sent to the Service Manager from application clients.

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.

Single Sign-On

Nach der Anmeldung bei einem Anwendungs-Client ermöglicht der Dienstmanager 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 Dienstmanager 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 Dienstmanager erneuert in regelmäßigen Abständen, vor Ablauf der Gültigkeit, den Authentifizierungs-Token.

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

Wenn Sie einen Web-Anwendungs-Client von einem anderen aus starten, übergibt der Anwendungs-Client den Authentifizierungs-Token an den nächsten Anwendungs-Client. Der nächste Web-Anwendungs-Client sendet den Authentifizierungs-Token an den Dienstmanager, um den Benutzer zu authentifizieren. Sie müssen sich von jedem Web-Anwendungs-Client separat abmelden. Wenn Sie beispielsweise das Analyst Tool über das Administrator Tool öffnen, müssen Sie sich vom Analyst Tool und dem Administrator Tool separat abmelden.

Hinweis: Um Single Sign-On zwischen dem Administrator Tool, dem Analyst Tool und dem Monitoring Tool verwenden zu können, müssen Sie deren vollständig qualifizierte Domännennamen zur Hostdatei für jeden Knoten hinzufügen.

Sie können Single Sign-On nicht verwenden, um über ein Client-Tool eine Verbindung mit einem Web-Anwendungs-Client herzustellen. Wenn Sie beispielsweise das Administrator Tool über das Developer Tool starten, müssen Sie sich beim Administrator Tool anmelden.

Autorisierung

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

- Datenintegrationsdienst
- Metadata Manager-Dienst
- Modellrepository-Dienst
- PowerCenter-Repository-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 Repositories:

- Modellrepository
- PowerCenter-Repository
- PowerCenter Repository für Metadata Manager

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

- Sie starten den Metadata Manager-Dienst, den Modellrepository-Dienst oder den PowerCenter-Repository-Dienst neu.
- 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.

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 LDAP-Konfigurationen und Betriebssystemprofile verwalten. Sie können auch Benutzer anzeigen, die Berechtigungen für einen Dienst besitzen.

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 Sternchen (*) 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:

Auf der Registerkarte „Sicherheit“ im Navigator wird abhängig von Ihrer Ansicht einer der folgenden Bereiche angezeigt:

- 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.
- Abschnitt „Betriebsprofile“. Wählen Sie ein Betriebsprofil aus, um die Eigenschaften des Betriebssystemprofils und die Berechtigungen anzuzeigen, die Benutzern und Gruppen zugewiesen wurden, die das Betriebssystemprofil verwenden.
- Abschnitt „LDAP-Konfiguration“. Wählen Sie eine Konfiguration aus, um die Verbindungsdetails des LDAP-Servers, den LDAP-Synchronisierungszeitplan und die LDAP-Sicherheitsdomäne mit Benutzern und Gruppen anzuzeigen, die aus dem LDAP-Verzeichnisdienst importiert wurden.

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 ein Menü mit der Bezeichnung „Aktionen“ zum Verwalten von Gruppen, Benutzern, Rollen, Betriebssystemprofilen oder LDAP-Konfigurationen.
- Rechter Mausklick auf Objekt. Klicken Sie im Navigator mit der rechten Maustaste auf ein Objekt, um die im Menü „Aktionen“ verfügbaren Optionen anzuzeigen.
- Tastenkombinationen verwenden. Mithilfe von Tastenkombinationen können Sie die verschiedenen Abschnitte des Navigators ansteuern.

Gruppen

Eine Gruppe ist eine Anhäufung von Benutzern und Gruppen mit denselben Rechten, 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 verwendet LDAP-Sicherheitsdomänen, die Benutzer und Gruppen enthält, die aus dem LDAP-Verzeichnisdienst importiert wurden.

Wenn Sie einen Sicherheitsdomänen-Ordner im Abschnitt „Gruppen“ des Navigators auswählen, werden in der Inhaltsübersicht alle zu dieser Sicherheitsdomäne gehörenden Gruppen eingeblendet.

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.
- Berechtigungen. Zeigt die Zugriffsebene an, auf der die Benutzer innerhalb der Gruppe Aufgaben für Domänenobjekte ausführen müssen, einschließlich Knoten, Tabellen und Anwendungsdienste. Zeigt außerdem die Zugriffsebene an, auf der die Benutzer innerhalb der Gruppe Aufgaben für Verbindungsobjekte und Betriebssystemprofile ausführen müssen.

Benutzer

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

- Informatica Administrator
- PowerCenter Client
- Informatica Developer
- Informatica Analyst
- Metadata Manager

Im Abschnitt "Benutzer" des Navigators sind die Benutzer in Sicherheitsdomänenordnern zusammengefasst. Eine Sicherheitsdomäne ist eine Sammlung 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 verwendet LDAP-Sicherheitsdomänen, die Benutzer und Gruppen enthält, die aus dem LDAP-Verzeichnisdienst importiert wurden.

Wenn Sie im Abschnitt „Benutzer“ des Navigators einen Ordner für eine Sicherheitsdomäne auswählen, erscheinen im Inhaltsbereich alle Benutzer, die zu dieser Sicherheitsdomäne gehören.

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.
- Berechtigungen. Zeigt die Zugriffsebene an, auf der die Benutzer Aufgaben für Domänenobjekte ausführen müssen, einschließlich Knoten, Tabellen und Anwendungsdienste. Zeigt außerdem die Zugriffsebene an, auf der die Benutzer Aufgaben für Verbindungsobjekte und Betriebssystemprofile ausführen müssen.

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 Rollen an, die zu diesem Ordner gehören.

Wenn Sie eine 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.

Betriebssystemprofile

Ein Betriebssystemprofil ist ein Sicherheitsmechanismus, mit dem der Datenintegrationsdienst und der PowerCenter-Integrationsdienst Mappings, Arbeitsabläufe und Profiling-Jobs ausführen.

Im Abschnitt „Betriebssystemprofile“ des Navigators werden die in der Domäne konfigurierten Betriebssystemprofile aufgelistet.

Wenn Sie im Navigator ein Betriebssystemprofil auswählen, zeigt der Inhaltsbereich die folgenden Registerkarten an:

- Eigenschaften. Zeigt allgemeine Eigenschaften des Betriebssystemprofils an, die für den Datenintegrationsdienst, den PowerCenter-Integrationsdienst oder für beide Anwendungsdienste konfiguriert sind.
- Berechtigungen. Zeigt die Berechtigungen an, die Benutzern und Gruppen zugewiesen wurden, die das Betriebssystemprofil verwenden. Gibt außerdem an, ob das Betriebssystemprofil das Standardprofil ist, das einem Benutzer oder einer Gruppe zugewiesen ist.

LDAP-Konfiguration

Sie können eine Informatica-Domäne konfigurieren, damit sich Benutzer und Gruppen, die aus einem oder mehreren LDAP-Verzeichnisdiensten importiert wurden, bei Informatica-Knoten, -Diensten und -Anwendungsclients anmelden können.

Im Abschnitt „LDAP-Konfiguration“ des Navigators werden die von der Domäne verwendeten LDAP-Konfigurationen aufgelistet.

Wenn Sie eine LDAP-Konfiguration auswählen, werden folgende Registerkarten auf der Registerkarte „LDAP-Konfiguration“ angezeigt:

- Übersicht. Listet die Verbindungsdetails für den LDAP-Server mit dem Verzeichnisdienst auf, aus dem Benutzer und Gruppen importiert werden sollen.
- Sicherheitsdomänen. Listet die Details für die LDAP-Sicherheitsdomäne auf, die aus dem LDAP-Verzeichnisdienst importierte Benutzer und Gruppen enthält.
- Zeitplan. Listet die Details für den Synchronisierungszeitplan auf, in dem der Zeitpunkt angegeben wird, an dem der Dienstmanager die Sicherheitsdomäne mit den Benutzern und Gruppen im LDAP-Verzeichnisdienst aktualisiert.

Kontoverwaltung

Um die Sicherheit in der Informatica-Domäne zu verbessern, können Sie die Sperrung von Benutzer- und Administratorkonten nach einer bestimmten Anzahl von fehlgeschlagenen Anmeldeversuchen erzwingen.

Im Abschnitt „Konfiguration Kontosperre“ der Seite „Kontoverwaltung“ ist angegeben, ob die Kontosperre für Benutzer- und Administratorkonten aktiviert ist. Im Abschnitt wird außerdem die maximal zulässige Anzahl fehlgeschlagener Anmeldeversuche angegeben.

Im Abschnitt „Gesperrte native Benutzer“ der Seite sind die gesperrten Benutzerkonten in der nativen Sicherheitsdomäne aufgelistet. Sie können ein Benutzerkonto in der nativen Sicherheitsdomäne entsperren.

Im Abschnitt „Gesperrte LDAP-Benutzer“ der Seite sind die gesperrten Benutzerkonten in einer LDAP-Sicherheitsdomäne aufgelistet. Sie können ein Benutzerkonto in der Informatica-Domäne entsperren. Allerdings muss der LDAP-Administrator zuvor das Benutzerkonto auf dem LDAP-Server entsperren. Der Benutzer kann sich erst dann bei der Informatica-Domäne anmelden, wenn der LDAP-Administrator das Benutzerkonto entsperrt hat.

Auditberichte

Auditberichte enthalten Informationen über Benutzer und Gruppen in der Informatica-Domäne sowie über die Rechte, Rollen und Berechtigungen, die den einzelnen Benutzern oder Gruppen zugewiesen sind.

Sie wählen den zu erstellenden Auditbericht über das Menü „Berichtstyp auswählen“ aus. Sie können die folgenden Auditberichte generieren:

Persönliche Benutzerinformationen

Zeigt Kontaktinformationen und Statusdetails der Benutzerkonten in der Domäne 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.

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://<fully qualified host name>:<port>/passwordchange/`

Der Dienstmanager 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 Dienstmanager das Passwort für jeden Worker-Knoten. Der Dienstmanager kann nur Knoten aktualisieren, die ausgeführt werden. Bei Knoten, die nicht ausgeführt werden, aktualisiert der Dienstmanager das Passwort, wenn die Knoten neu gestartet werden.

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

Sie können die internen URLs aktivieren oder deaktivieren, wenn Sie das Passwort für LDM admin im Administrator Tool ändern, das für den Lastenausgleich eingerichtet ist.

Verwenden Sie die folgende benutzerdefinierte Option für interne URLs für die Passwortverwaltung:

enableChangePwdUrlProxyHost

Zeigen Sie die internen URLs im Zusammenhang mit der Passwortverwaltung an und greifen Sie darauf zu. Standardwert ist „false“.

Verwenden Sie für ein Benutzerkonto in einer Domäne, die die native Authentifizierung verwendet, bei aktivierter Kennwortkomplexität die folgenden Richtlinien, wenn Sie ein Passwort erstellen oder ändern:

- Das Passwort muss aus mindestens acht Zeichen bestehen.
- Es muss mindestens einen Buchstaben, eine Zahl und ein nicht alphanumerisches Zeichen enthalten, z. B.:
! \ " # \$ % & ' () * + , - . / : ; < = > ? @ [] ^ _ ` { | } ~

Manche Sonderzeichen in Passwörtern können von der Shell anders interpretiert werden. Beispielsweise wird \$ als Variable interpretiert. Setzen Sie in diesem Fall ein Escape-Zeichen vor das betreffende Sonderzeichen.

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 eine 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.

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.

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.

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 8

Benutzer und Gruppen

Dieses Kapitel umfasst die folgenden Themen:

- [Benutzer und Gruppen - Übersicht, 124](#)
- [Standardgruppen, 125](#)
- [Das Konzept der Benutzerkonten, 126](#)
- [Benutzer verwalten, 128](#)
- [Gruppen verwalten, 137](#)
- [Managing operating system profiles, 138](#)
- [Kontosperre, 148](#)

Benutzer und Gruppen - Übersicht

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.

Die Benutzerkontenverwaltung umfasst in Informatica die folgenden Hauptkomponenten:

- Benutzer. Sie können verschiedene Typen von Benutzerkonten in der Informatica-Domäne einrichten. Benutzer können Aufgaben basierend auf den ihnen zugewiesenen Rollen, Berechtigungen und Rechten durchführen.
- Authentifizierung. Wenn sich ein Benutzer an einem Anwendungs-Client anmeldet, authentifiziert der Dienstmanager 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 Dienstmanager organisiert Benutzerkonten und Gruppen nach Sicherheitsdomäne. Er authentifiziert Benutzer auf der Basis der Sicherheitsdomäne, der der Benutzer angehört.
- 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 Integrationsdienst unter UNIX oder Linux ausführen, können Sie den Integrationsdienst zur Verwendung von Betriebssystemprofilen konfigurieren. Verwenden Sie Betriebssystemprofile, um die Sicherheit zu erhöhen und die Laufzeitumgebung für Benutzer zu isolieren. 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.

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:

- Administrator
- Jeder
- Operator

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.

Operatorgruppe

Die Informatica-Domäne enthält die Standardgruppe „Operator“.

Standardmäßig verfügt die Operatorgruppe über Berechtigungen für alle Objekte in der Domäne. Sie können der Operatorgruppe die Operatorrolle zuweisen und die Rolle dazu verwenden, die Operatorbenutzer in der Domäne zu verwalten.

Sie können die folgenden Aufgaben in der Operatorgruppe durchführen:

- Der Gruppe Berechtigungen und Rollen zuweisen.
- Benutzer in die Gruppe hinzufügen oder daraus entfernen.
- Eine Gruppe in die Gruppe verschieben.
- Die Gruppe bearbeiten oder löschen.

Das Konzept der Benutzerkonten

Eine Informatica-Domäne kann folgende Arten von Benutzerkonten haben:

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

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.

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.

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:

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.

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 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

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 mehr als 128 Zeichen umfassen. Er darf weder einen Tabulator noch ein Zeilenendezeichen noch folgende Sonderzeichen enthalten: , + " \ < > ; / * % ? & Der Name kann ein ASCII-Leerzeichen enthalten, jedoch nicht als erstes oder letztes Zeichen. Alle anderen Leerzeichen sind nicht zulässig.
Passwort	Passwort für das Benutzerkonto. Das Passwort kann zwischen 1 und 80 Zeichen umfassen.

Eigenschaft	Beschreibung
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: < > "
Beschreibung	Beschreibung des Benutzerkontos. Die Beschreibung darf maximal 765 Zeichen umfassen 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: < > "

- 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 Anmeldenamen eines nativen Benutzers nicht ändern. Sie können das Passwort und andere Details eines nativen Benutzerkontos ändern.

- Klicken Sie im Administrator Tool auf die Registerkarte Sicherheit.
- Im Abschnitt Benutzer des Navigators wählen Sie ein natives Benutzerkonto aus und klicken auf Bearbeiten.
- Um ein anderes Passwort festzulegen, wählen Sie Passwort ändern.
Auf der Registerkarte Sicherheit werden die Einträge in den Feldern Passwort und Passwort bestätigen gelöscht.
- Geben Sie ein neues Passwort ein und bestätigen Sie dieses.
- Ändern Sie den kompletten Namen, die Beschreibung, E-Mail und Telefon wie erforderlich.
- 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.

- Klicken Sie im Administrator Tool auf die Registerkarte Sicherheit.
- Wählen Sie im Abschnitt „Benutzer“ des Navigators ein natives Benutzerkonto aus und klicken Sie auf **Bearbeiten**.
- 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 Abschnitt „Gruppen“ 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 dann 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 dann 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.

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 Status 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 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, ExportUsersandGroups, ImportDomainObjects und ImportUsersandGroups
- infacmd-Tools ExportObjects und ImportObjects

Möglicherweise müssen Sie bei einer Vielzahl von Benutzern in der Domäne den von Informatica-Diensten, 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-Dienste 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 die Registerkarte „Protokolle“ des Administrator Tools, um die Benutzeraktivitätsprotokolle anzuzeigen. Zeigen Sie Benutzeraktivitätsprotokolle an, um Anmeldeversuche aus Informatica-Clientanwendungen zu überprüfen. Sie können die Protokolle auch anzeigen, um festzustellen, wann ein Benutzer Dienste, Knoten, Benutzer, Gruppen oder Rollen erstellt, aktualisiert oder entfernt hat.

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

Sie können auch den Befehl „`infacmd isp getUserActivityLog`“ verwenden, um Daten des Benutzeraktivitätsprotokolls anzuzeigen. Der Befehl „`infacmd isp getUserActivityLog`“ verwendet die folgende Syntax:

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

Der Befehl „`infacmd isp getUserActivityLog`“ erfordert die Administratorrolle oder Mitgliedschaft in der Administratorgruppe. Weitere Informationen über den Befehl „`infacmd isp getUserActivityLog`“ finden Sie in der *Informatica-Befehlsreferenz*.

Die Benutzeraktivitätsprotokolle enthalten erfolgreiche und fehlgeschlagene Anmeldeversuche von Informatica-Clients. Wenn der Client benutzerdefinierte Eigenschaften für Anmeldeabfragen festlegt, enthalten die Protokolldaten die benutzerdefinierten Eigenschaften.

Hinweis: Die Benutzeraktivitätsprotokolle enthalten keine Benutzeranmeldeversuche in einer Domäne, die zur Verwendung von Kerberos-Authentifizierung konfiguriert ist.

Die Benutzeraktivitätsdaten umfassen die folgenden Eigenschaften für alle Anmeldeversuche eines Informatica-Clients:

- Name der Anwendung
- Version der Anwendung
- Hostname oder IP-Adresse des Anwendungshosts

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 Eingabeaufforderung anzeigen oder die Ereignisse in einem der folgenden Formate in eine Datei schreiben:

- Binär
- Text
- XML

Wenn Sie ein Protokoll im binären Format drucken, können Sie den Befehl „`infacmd isp convertUserActivityLog`“ verwenden, um eine Konvertierung in das Text- oder XML-Format durchzuführen. Weitere Informationen zur Verwendung des Befehls „`infacmd isp convertUserActivityLog`“ finden Sie in der *Informatica-Befehlsreferenz*.

Benutzeraktivitätscodes

Benutzeraktivitätsprotokolle enthalten Codes, die jede erfolgreiche oder fehlgeschlagene Aktivität angeben.

Zu den gültigen Aktivitätscodes gehören:

- CCM_10437. Gibt an, dass eine Aktivität erfolgreich war.
- CCM_10438. Gibt an, dass eine Aktivität fehlgeschlagen ist.
- CCM_10778. Gibt an, dass ein Anmeldeversuch mit benutzerdefinierten Eigenschaften erfolgreich war.
- CCM_10779. Gibt an, dass ein Anmeldeversuch mit benutzerdefinierten Eigenschaften fehlgeschlagen ist.
- CCM_10786. Gibt an, dass ein Anmeldeversuch ohne benutzerdefinierte Eigenschaften erfolgreich war.
- CCM_10787. Gibt an, dass ein Anmeldeversuch ohne benutzerdefinierte Eigenschaften fehlgeschlagen ist.

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.
- CCM_10778. Gibt an, dass ein Anmeldeversuch mit benutzerdefinierten Eigenschaften erfolgreich war.
- CCM_10779. Gibt an, dass ein Anmeldeversuch mit benutzerdefinierten Eigenschaften fehlgeschlagen ist.
- CCM_10786. Gibt an, dass ein Anmeldeversuch ohne benutzerdefinierte Eigenschaften erfolgreich war.
- CCM_10787. Gibt an, dass ein Anmeldeversuch ohne benutzerdefinierte Eigenschaften 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.

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.

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 eine 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.

Managing operating system profiles

Create and manage operating system profiles on the Security tab of the Administrator tool or from the command line. You can create, edit, and delete operating system profiles. You can assign or change the default operating system profile to users and groups.

If the Data Integration Service is configured to use operating system profiles, it runs mappings, profiles, and workflows with the operating system profile. If the PowerCenter Integration Service is configured to use operating system profiles, it runs workflows with the operating system profile.

Create, edit, and delete operating system profiles in the **Operating System Profiles** view of the **Security** tab.

Complete the following steps to create an operating system profile:

1. Enter an operating system profile name and a system user name.
2. Select the Integration Services and configure the operating system profile properties.
3. Optionally, assign permissions on the operating system profile.

You can assign users and groups to operating system profiles and assign a default profile to users and groups after you create an operating system profile.

Eigenschaften des Betriebssystemprofils für den PowerCenter-Integrationsdienst

Dienstprozessvariablen, die in Sitzungseigenschaften und Parameterdateien festgelegt sind, überschreiben die Einstellungen des Betriebssystemprofils.

In der folgenden Tabelle werden die Eigenschaften des Betriebssystemprofils für den PowerCenter-Integrationsdienst beschrieben:

Eigenschaft	Beschreibung
Name	Schreibgeschützter Name des Betriebssystemprofils. Der Name darf nicht mehr als 128 Zeichen umfassen. Er darf keine Leerzeichen oder die folgenden Sonderzeichen enthalten: \\ : * ? " < > [] = + ; ,
Systembenutzername	Schreibgeschützter Name eines Betriebssystembenutzers, der auf den Computern vorhanden ist, auf denen der PowerCenter-Integrationsdienst ausgeführt wird. Der PowerCenter-Integrationsdienst führt Arbeitsabläufe mit dem Systemzugriff des Systembenutzers aus, der für das Betriebssystemprofil definiert wurde.
\$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 sein: * ? < > " ,
\$PMSessionLogDir	Verzeichnis für Sitzungsprotokolle. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " , Standardwert ist \$PMRootDir/SessLogs.
\$PMBadFileDir	Verzeichnis für Ablehnungsdateien. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " , Standardwert ist \$PMRootDir/BadFiles.
\$PMCacheDir	Verzeichnis für Index- und Datencache-Dateien. Sie können die Leistung steigern, wenn als Cache-Verzeichnis für den PowerCenter-Integrationsdienstprozess ein lokales Laufwerk verwendet wird. Verwenden Sie kein zugeordnetes oder gemountetes Laufwerk für Cache-Dateien. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " , Standardwert ist \$PMRootDir/Cache.
\$PMTargetFileDir	Verzeichnis für Zieldateien. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " , Standardwert ist \$PMRootDir/TgtFiles.

Eigenschaft	Beschreibung
\$PMSourceFileDir	Verzeichnis für Quelldateien. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " , Standardwert ist \$PMRootDir/SrcFiles.
\$PmExtProcDir	Verzeichnis für externe Prozeduren. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " , Standardwert ist \$PMRootDir/ExtProc.
\$PMTempDir	Verzeichnis für temporäre Dateien. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " , Standardwert ist \$PMRootDir/Temp.
\$PMLookupFileDir	Verzeichnis für Lookup-Dateien. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " , Standardwert ist \$PMRootDir/LkpFiles.
\$PMStorageDir	Verzeichnis für Laufzeitdateien. Wiederherstellungsdateien des Arbeitsablaufs werden im Verzeichnis \$PMStorageDir gespeichert, das in den Eigenschaften des PowerCenter-Integrationsdiensts konfiguriert ist. Wiederherstellungsdateien der Sitzung werden im Verzeichnis \$PMStorageDir gespeichert, das im Betriebssystemprofil konfiguriert ist. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " , Standardwert ist \$PMRootDir/Storage.
Umgebungsvariablen	Name und Wert von Umgebungsvariablen, die vom Integrationsdienst zur Laufzeit verwendet werden. Wenn Sie die LD_LIBRARY_PATH-Umgebungsvariable in den Eigenschaften des Betriebssystemprofils angeben, hängt der Integrationsdienst den Wert dieser Variable an seine LD_LIBRARY_PATH-Umgebungsvariable an. Der Datenintegrationsdienst verwendet den Wert seiner LD_LIBRARY_PATH-Umgebungsvariable, um die Umgebungsvariablen untergeordneter Prozesse festzulegen, die für das Betriebssystemprofil erzeugt werden. Wenn Sie die LD_LIBRARY_PATH-Umgebungsvariable in den Eigenschaften des Betriebssystemprofils nicht angeben, verwendet der Integrationsdienst seine LD_LIBRARY_PATH-Umgebungsvariable.

Eigenschaften des Betriebssystemprofils für den Datenintegrationsdienst

In der folgenden Tabelle werden die Eigenschaften des Betriebssystemprofils für den Datenintegrationsdienst beschrieben:

Eigenschaft	Beschreibung
Name	Schreibgeschützter Name des Betriebssystemprofils. Der Name darf nicht mehr als 128 Zeichen umfassen. Er darf weder Leerzeichen noch die folgenden Sonderzeichen enthalten: % * + \ / ? ; < >
Systembenutzername	Schreibgeschützter Name eines Betriebssystembenutzers, der auf den Systemen vorhanden ist, auf denen der Datenintegrationsdienst ausgeführt wird. Der Datenintegrationsdienst führt Mappings, Arbeitsabläufe und Profiling-Jobs mithilfe des Systemzugriffs des Betriebssystembenutzers aus.
\$DISRootDir	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 sein: * ? < > " , []
\$DISTempDir	Verzeichnis für temporäre Dateien, die während der Ausführung von Jobs erstellt werden. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " , [] Standardwert ist <Root-Verzeichnis>/disTemp. Hinweis: Wenn der Datenintegrationsdienst für die Verwendung mehrerer Betriebssystemprofile konfiguriert ist, geben Sie ein gemeinsames Verzeichnis für alle Profile an, da ein separates Verzeichnis für jedes Profil zu einer übermäßigen Nutzung des Speicherplatzes führt.
\$DISCacheDir	Verzeichnis für Index- und Daten-Cache-Dateien für Umwandlungen. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " , [] Standardwert ist <Root-Verzeichnis>/cache.
\$DISSourceDir	Verzeichnis für Einfachdateien der Quelle, die in einem Mapping verwendet werden. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " , [] Standardwert ist <Root-Verzeichnis>/source.
\$DISTargetDir	Verzeichnis für Einfachdateien des Ziels, die in einem Mapping verwendet werden. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " , [] Standardwert ist <Root-Verzeichnis>/target.
\$DISRejectedFilesDir	Verzeichnis für Ablehnungsdateien. Ablehnungsdateien enthalten Zeilen, die beim Ausführen eines Mappings zurückgewiesen wurden. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " , [] Standardwert ist <Root-Verzeichnis>/reject.

Eigenschaft	Beschreibung
\$DISLogDir	<p>Verzeichnis für Protokolle. Es darf keines der folgenden Sonderzeichen enthalten sein: * ? < > " , []</p> <p>Standardwert ist <Root-Verzeichnis>/disLogs.</p>
Eigenschaften für Hadoop-Identitätswechsel aktivieren	<p>Gibt an, dass der Datenintegrationsdienst den Benutzer für den Hadoop-Identitätswechsel verwendet, um Mappings, Arbeitsabläufe und Profiling-Jobs in einer Hadoop-Umgebung auszuführen.</p> <p>Bei dem Standardbenutzer für den Hadoop-Identitätswechsel handelt es sich um den angemeldeten Benutzer. Wählen Sie zur Angabe eines anderen Benutzers für den Hadoop-Identitätswechsel die Option Angegebenen Benutzer als Benutzer für den Hadoop-Identitätswechsel verwenden aus und geben Sie einen Benutzernamen ein.</p>
Umgebungsvariablen	<p>Name und Wert von Umgebungsvariablen, die vom Integrationsdienst zur Laufzeit verwendet werden.</p> <p>Wenn Sie die LD_LIBRARY_PATH-Umgebungsvariable in den Eigenschaften des Betriebssystemprofils angeben, hängt der Integrationsdienst den Wert dieser Variable an seine LD_LIBRARY_PATH-Umgebungsvariable an. Der Datenintegrationsdienst verwendet den Wert seiner LD_LIBRARY_PATH-Umgebungsvariable, um die Umgebungsvariablen untergeordneter Prozesse festzulegen, die für das Betriebssystemprofil erzeugt werden.</p> <p>Wenn Sie die LD_LIBRARY_PATH-Umgebungsvariable in den Eigenschaften des Betriebssystemprofils nicht angeben, verwendet der Integrationsdienst seine LD_LIBRARY_PATH-Umgebungsvariable.</p> <p>Hinweis: Unter AIX müssen Sie die LD_LIBRARY_PATH-Umgebungsvariable für den Datenintegrationsdienst auf INFA_HOME/services/shared/bin setzen, um Mappings, Profile und Arbeitsabläufe erfolgreich mit Betriebssystemprofilen auszuführen.</p>
Verzeichnis des Einfachdatei-Cache	<p>Verzeichnis des Einfachdatei-Cache, in dem das Analyst Tool hochgeladene Einfachdateien speichert.</p> <p>Wenn der Analyst-Dienst eine Verbindung zu einem Datenintegrationsdienst herstellt, der Betriebssystemprofile verwendet, muss der im Betriebssystemprofil angegebene Betriebssystembenutzer über Zugriff auf das Verzeichnis des Einfachdatei-Cache verfügen. Wenn Sie eine Referenztabelle oder eine Einfachdatei-Quelle importieren, verwendet das Analyst Tool die Dateien aus diesem Verzeichnis, um eine Referenztabelle oder ein Einfachdatei-Datenobjekt zu erstellen. Starten Sie den Analyst-Dienst neu, wenn Sie den Einfachdatei-Speicherort ändern.</p>

Eigenschaften des Betriebssystemprofils für den Metadaten-Zugriffsdienst

In der folgenden Tabelle werden die Eigenschaften des Betriebssystemprofils für den Metadaten-Zugriffsdienst beschrieben:

Eigenschaft	Beschreibung
Name	Schreibgeschützter Name des Betriebssystemprofils. Der Name darf nicht mehr als 128 Zeichen umfassen. Er darf weder Leerzeichen noch die folgenden Sonderzeichen enthalten: % * + \ / ? ; < >
Systembenutzername	Schreibgeschützter Name eines Betriebssystembenutzers, der auf den Systemen vorhanden ist, auf denen der Metadaten-Zugriffsdienst ausgeführt wird. Der Metadaten-Zugriffsdienst ermöglicht dem Developer Tool den Zugriff auf Hadoop-Verbindungsinformationen, um Metadaten anhand des Systemzugriffs des Betriebssystembenutzers zu importieren und in der Vorschau anzuzeigen.
Eigenschaften für Hadoop-Identitätswechsel aktivieren	Gibt an, dass der Metadaten-Zugriffsdienst den Hadoop-Identitätswechsel verwendet, um Metadaten zu importieren und in der Vorschau anzuzeigen. Bei dem Standardbenutzer für den Hadoop-Identitätswechsel handelt es sich um den angemeldeten Benutzer. Wählen Sie zur Angabe eines anderen Benutzers für den Hadoop-Identitätswechsel die Option Angegebenen Benutzer als Benutzer für den Hadoop-Identitätswechsel verwenden aus und geben Sie einen Benutzernamen ein.

Betriebssystemprofil erstellen

Erstellen Sie ein Betriebssystemprofil und weisen Sie es Benutzern und Gruppen zu, um die Sicherheit zu erhöhen und die Laufzeitbenutzerumgebung zu isolieren. Sie können ein oder mehrere Betriebssystemprofile erstellen. Der PowerCenter-Integrationsdienst verwendet das Betriebssystemprofil zum Ausführen von Arbeitsabläufen. Der Datenintegrationsdienst verwendet das Betriebssystemprofil zum Ausführen von Mappings, Profilen und Arbeitsabläufen. Der Metadaten-Zugriffsdienst verwendet das Betriebssystemprofil für den Zugriff auf Hadoop-Verbindungsinformationen, um Metadaten zu importieren und in der Vorschau anzuzeigen.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Sicherheit**.
2. Klicken Sie im Menü „Sicherheitsaktionen“ auf **Betriebssystemprofil erstellen**.

Das Dialogfeld **Betriebssystemprofil erstellen - Schritt 1 von 3** wird angezeigt.

3. Geben Sie die folgenden allgemeinen Eigenschaften für das Betriebssystemprofil ein:

Eigenschaft	Beschreibung
Name	Name des Betriebssystemprofils. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Er darf weder mehr als 128 Zeichen enthalten noch mit @ beginnen. Außerdem darf er keines der folgenden Sonderzeichen enthalten: % * + \ / ? ; < > Der Name kann ein ASCII-Leerzeichen enthalten, jedoch nicht als erstes oder letztes Zeichen. Alle anderen Leerzeichen sind nicht zulässig.
Systembenutzername	Name eines Betriebssystembenutzers, der auf den Computern vorhanden ist, auf denen der Integrationsdienst ausgeführt wird. Der Integrationsdienst führt Arbeitsabläufe oder Jobs mit dem Systemzugriff des Systembenutzers aus, der für das Betriebssystemprofil definiert wurde. Hinweis: Beim Erstellen von Betriebssystemprofilen können Sie weder den Systembenutzernamen als Root angeben noch einen Nicht-Root-Benutzer mit uid==0 verwenden.

4. Klicken Sie auf **Weiter**.

Das Dialogfeld **Betriebssystemprofil konfigurieren - Schritt 2 von 3** wird angezeigt.

5. Wählen Sie den Dienst aus, der das Betriebssystemprofil verwenden soll.
- PowerCenter-Integrationsdienst
 - Datenintegrationsdienst
 - Metadaten-Zugriffsdienst
6. Konfigurieren Sie die Eigenschaften des Betriebssystemprofils für die ausgewählten Dienste. Um ein Betriebssystemprofil für den Metadaten-Zugriffsdienst zu erstellen, müssen Sie zudem den Datenintegrationsdienst sowie den Metadaten-Zugriffsdienst auswählen und die Variable „\$DISRootDir“ für den Datenintegrationsdienst angeben.
7. Wenn die Dienste zur Entwurfs- oder Laufzeit auf eine Hadoop-Umgebung zugreifen, konfigurieren Sie die Hadoop-Identitätswechseleigenschaften wie folgt:
- Wählen Sie **Hadoop-Eigenschaften für den Identitätswechsel aktivieren** aus.
 - Verwenden Sie den angemeldeten Benutzer oder geben Sie einen Hadoop-Benutzer für den Identitätswechsel an, um Hadoop-Jobs auszuführen.
8. Konfigurieren Sie optional die Umgebungsvariablen.
9. Wenn der Analyst-Dienst eine Verbindung zu einem Datenintegrationsdienst herstellt, der Betriebssystemprofile verwendet, konfigurieren Sie die Eigenschaften des Analyst-Diensts.
10. Klicken Sie auf **Weiter**.
- Das Dialogfeld **Benutzer und Gruppen zu Betriebssystemprofil zuweisen - Schritt 3 von 3** wird geöffnet.
11. Auf der Registerkarte **Gruppen** weisen Sie dem Betriebssystemprofil wie folgt Gruppen zu:
- Wählen Sie zum Zuweisen bestimmter Gruppen zum Betriebssystemprofil eine oder mehrere Gruppen aus und klicken Sie auf **Hinzufügen**.
 - Um alle verfügbaren Gruppen zum Betriebssystemprofil zuzuweisen, klicken Sie auf **Alle hinzufügen**.
12. Weisen Sie mindestens einer Gruppe das Betriebssystemprofil optional als Standardprofil zu. Wählen Sie zum Zuweisen eines Standardprofils die Option **Standardprofil** für die Gruppe in der Liste „Ausgewählte Gruppe(n)“ aus.

13. Auf der Registerkarte **Benutzer** weisen Sie dem Betriebssystemprofil wie folgt Benutzer zu:
 - a. Wählen Sie zum Zuweisen bestimmter Benutzer zum Betriebssystemprofil einen oder mehrere Benutzer aus und klicken Sie auf **Hinzufügen**.
 - b. Um alle verfügbaren Benutzer zum Betriebssystemprofil zuzuweisen, klicken Sie auf **Alle hinzufügen**.
14. Weisen Sie mindestens einem Benutzer das Betriebssystemprofil optional als Standardprofil zu. Wählen Sie zum Zuweisen eines Standardprofils die Option **Standardprofil** für den Benutzer in der Liste „Ausgewählte Benutzer“ aus.
15. Klicken Sie auf **Fertig stellen**.

Nach der Erstellung des Betriebssystemprofils werden im Detailbereich die Eigenschaften des Betriebssystemprofils sowie die Gruppen und Benutzer angezeigt, denen das Profil zugewiesen ist.

Bearbeiten eines Betriebssystemprofils

Sie können ein Betriebssystemprofil bearbeiten, um dessen Eigenschaften zu ändern.

Den Namen oder den Systembenutzernamen können Sie nach dem Erstellen eines Betriebssystemprofils nicht mehr bearbeiten. Wenn Sie den im Betriebssystemprofil angegebenen Betriebssystembenutzer nicht verwenden möchten, löschen Sie das Betriebssystemprofil.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Sicherheit**.
2. Wählen Sie die Ansicht **Betriebssystemprofile** aus.
3. Wählen Sie das Betriebssystemprofil aus.
4. Klicken Sie auf der Registerkarte **Eigenschaften** auf **Bearbeiten**.

Das Dialogfeld **Eigenschaften bearbeiten** wird angezeigt.
5. Wählen Sie den Datenintegrationsdienst, den PowerCenter-Integrationsdienst oder den Metadaten-Zugriffsdienst aus, den Sie konfigurieren möchten.
6. Bearbeiten Sie die Diensteigenschaften.
7. Klicken Sie auf **OK**.

Zuweisen eines Standardbetriebssystemprofils zu einem Benutzer oder einer Gruppe

Wenn ein Benutzer oder eine Gruppe über Zugriff auf mehrere Betriebssystemprofile verfügt, weisen Sie ein Standardbetriebssystemprofil zu, das vom Integrationsdienst zum Ausführen von Jobs und Arbeitsabläufen verwendet wird. Sie können jedes Betriebssystemprofil mit direkten Berechtigungen als Standardprofil zu einem Benutzer oder einer Gruppe zuweisen. Ein Benutzer oder eine Gruppe kann nur ein Standardbetriebssystemprofil aufweisen. Es ist jedoch möglich, dasselbe Betriebssystemprofil als Standardprofil zu mehreren Benutzern oder Gruppen hinzuzufügen.

1. Wählen Sie auf der Registerkarte „Sicherheit“ die Ansicht **Benutzer** oder **Gruppen** aus.
2. Wählen Sie im Navigator den Benutzer oder die Gruppe aus.
3. Klicken Sie im Inhaltsbereich auf die Ansicht **Berechtigungen**.
4. Klicken Sie auf die Registerkarte **Betriebssystemprofile**.
5. Klicken Sie auf die Schaltfläche **Standardbetriebssystemprofil zuweisen oder ändern**.

Das Dialogfeld **Standardbetriebssystemprofil zuweisen oder ändern** wird angezeigt.

6. Wählen Sie ein Profil in der Liste **Standardbetriebssystemprofil** aus. Wählen Sie alternativ dazu **Standardbetriebssystemprofil nicht zuweisen** in der Liste aus, um das Standardprofil zu entfernen, das einem Benutzer oder einer Gruppe zugewiesen ist.
7. Klicken Sie auf **OK**.
Im Detailbereich wird in der Spalte **Standardprofil** der Wert **Ja (Direkt)** für das Betriebssystemprofil angezeigt.

Löschen eines Betriebssystemprofils

Klicken Sie zum Löschen eines Betriebssystemprofils mit der rechten Maustaste auf den Namen des Betriebssystemprofils im Abschnitt „Betriebssystem“ des Navigators und wählen Sie **Profil löschen** aus.

Verwenden Sie nach dem Löschen eines Betriebssystemprofils für die Benutzer und Gruppen, denen das Betriebssystemprofil als Standardprofil zugewiesen war, ein anderes Betriebssystemprofil. Wenn der PowerCenter-Integrationsdienst Betriebssystemprofile verwendet, weisen Sie den Repository-Ordnern und -Arbeitsabläufen, denen das Betriebssystemprofil zugeordnet war, ein anderes Betriebssystemprofil zu.

Working with Operating System Profiles in a Secure Domain

You can use operating system profiles in an Informatica domain that has secure communication enabled.

Consider the following rules and guidelines when you use operating system profiles in a domain that has secure communication enabled:

You must set the following environment variable for the operating system profile:

INFA_TRUSTSTORE

Set the value to the directory that contains the truststore files for the SSL certificates for the secure domain. The directory must contain a truststore file named `infa_truststore.pem`.

INFA_TRUSTSTORE_PASSWORD

If you use a custom truststore, set the value to the password for the `infa_truststore.pem` that contains the SSL certificate for the secure domain. The password must be encrypted. Use the command line program `pmpasswd` to encrypt the password.

Additionally, if the PowerCenter Integration Service uses the Session on Grid option, you must set the following environment variable for the operating system profile:

INFA_KEYSTORE

Set the value to the directory that contains the keystore files for the SSL certificates for the secure domain. The directory must contain a keystore file named `infa_keystore.pem`.

You can set the environment variables for the operating system profile in the Administrator tool. To set the environment variables for the operating system profile, click **Security > Operating System Profiles**. Edit the properties of the operating system profile and set the environment variables.

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.

You can set the environment variables for the operating system profile in the Administrator tool. To set the environment variables for the operating system profile, click **Security > Operating System Profiles**. Edit the properties of the operating system profile and set the environment variables.

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 Kontosperrung

Beachten Sie die folgenden Regeln und Richtlinien, wenn Sie die Kontosperrung für Informatica-Benutzer erzwingen:

- Wenn ein Anwendungsdienst unter einem Benutzerkonto ausgeführt wird und das falsche Passwort für den Anwendungsdienst angegeben wird, 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 Kontosperrung 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 Kontosperrung zu vermeiden.
- Wenn die Kontosperrung 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 9

Berechtigungen und Rollen

Dieses Kapitel umfasst die folgenden Themen:

- [Berechtigungen, 150](#)
- [Rollen, 152](#)
- [Domänenberechtigungen, 152](#)
- [Berechtigungen für den Analyst-Dienst, 160](#)
- [Berechtigungen für den Content-Management-Dienst, 162](#)
- [Datenintegrationsdienst-Berechtigungen, 162](#)
- [Berechtigung für den Massenerfassungsdienst, 163](#)
- [Metadata Manager Service-Berechtigungen, 163](#)
- [Berechtigungen für den Modellrepository-Dienst, 168](#)
- [PowerCenter Repository Service-Berechtigungen, 169](#)
- [Berechtigungen des PowerExchange Listener Service, 183](#)
- [PowerExchange Logger Service-Berechtigungen, 183](#)
- [Berechtigungen des Scheduler-Diensts, 184](#)
- [Berechtigungen für Test Data Manager-Dienst, 185](#)
- [Verwalten von Rollen, 189](#)
- [Benutzern und Gruppen Berechtigungen und Rollen zuweisen, 192](#)
- [Benutzer mit Berechtigungen für einen Dienst anzeigen, 194](#)
- [Fehlerbehebung bei Berechtigungen und Rollen, 194](#)

Berechtigungen

Berechtigungen bestimmen die Aktionen, die Benutzer in Anwendungs-Clients ausführen können. Informatica beinhaltet die folgenden Berechtigungen:

- Domänenberechtigungen. Legen Sie Aktionen fest, die Benutzer mithilfe des Administrator Tools und der Befehlszeilenprogramme infacmd und pmrep für die Informatica-Domäne durchführen können.
- Berechtigung für den Analyst-Dienst. Bestimmt 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.

- Datenintegrationsdienst-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.
- Berechtigung für den Massenerfassungsdienst. Bestimmt Aktionen, die Benutzer mithilfe des Massenerfassungstools durchführen können.
- Metadata Manager-Dienst-Berechtigungen. Bestimmen der Aktionen, die Benutzer mit Metadata Manager ausführen können.
- Modellrepository-Dienst-Berechtigung. Bestimmen der Aktionen bei Projekten, die Benutzer mit Informatica Analyst und Informatica Developer ausführen können.
- PowerCenter-Repository-Dienst-Berechtigungen. Bestimmen die PowerCenter-Repository-Aktionen, die Benutzer mit dem Repository Manager, Designer, Arbeitsablauf-Manager, Workflow Monitor und den Befehlszeilenprogrammen pmrep und pmcmd ausführen können.
- PowerExchange Anwendungsdienst-Berechtigungen. Bestimmen der Aktionen, die Benutzer beim PowerExchange-Listenerdienst und PowerExchange-Protokollierungsdienst mit den infacmd pwx-Befehlen ausführen können.
- Berechtigungen des Scheduler-Diensts. Legen Sie Aktionen fest, die Benutzer mithilfe des Scheduler-Diensts durchführen 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.

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.
- Domänenverwaltung. Beinhaltet Berechtigungen zum Verwalten der Domäne, Ordner, Knoten, Gitter, Lizenzen und Anwendungsdienste.

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 Berechtigungen oder Aktionen des PowerCenter-Repository-Diensts, 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 in folgendem Artikel in der Informatica-Ratgeber-Bibliothek:

[Using Groups and Roles to Manage Access Controls.](#)

Domänenberechtigungen

Domänenberechtigungen legen fest, welche Aktionen Benutzer mit dem Administrator Tool und den Befehlszeilenprogrammen infacmd und pmrep ausführen können.

Die nachstehende Tabelle beschreibt jede Domänenberechtigungsgruppe:

Berechtigungsgruppe	Beschreibung
Sicherheitsverwaltung	Beinhaltet Berechtigungen zum Verwalten von Benutzern, Gruppen, Rollen und Berechtigungen.
Domänenverwaltung	Enthält Rechte zum Verwalten von Ordnern, Knoten, Rastern, Lizenzen, Anwendungsdiensten, Verbindungen, Cluster-Konfigurationen und der Domäne.
Überwachung	Enthält Berechtigungen zum Konfigurieren von Überwachungsstatistiken und -berichten, zum Anzeigen der Überwachung für Integrationsobjekte 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 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. Ein Benutzer, dem die Administratorrolle für die Domäne zugewiesen wurde, kann folgende Aufgaben ausführen:

- Erstellen, bearbeiten und löschen Sie Betriebssystemprofile.
- Berechtigungen für Betriebssystemprofile vergeben.

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: <ul style="list-style-type: none">- 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: <ul style="list-style-type: none">- 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.

Berechtigungsgruppe „Domänenverwaltung“

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:

- Konfigurieren von Domäneneigenschaften.

- Konfigurieren Sie Cluster-Konfigurationen.
- 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.

Benutzer, denen Domänenobjektberechtigungen, aber keine Rechte zugewiesen sind, können bestimmte Domänenverwaltungsaufgaben abschließen. 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: <ul style="list-style-type: none"> - Anzeigen von Domäneneigenschaften und Protokollereignissen. - Konfigurieren der Überwachungseinstellungen.
Ordner	Benutzer kann Ordneigenschaften anzeigen.
Anwendungsdienst	Benutzer kann Eigenschaften von Anwendungsdiensten und Protokollereignisse anzeigen.
Lizenzobjekt	Benutzer kann Eigenschaften von Lizenzobjekten anzeigen.
Gitter	Benutzer kann Gittereigenschaften anzeigen.
Knoten	Benutzer kann Knoteneigenschaften anzeigen.
Webdienst-Hub	Benutzer kann den Webdienstbericht ausführen.

Hinweis: Für Domänenverwaltungsaufgaben im Administrator Tool müssen die Benutzer ebenfalls über die Zugriffsberechtigung von Informatica Administrator 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: <ul style="list-style-type: none"> - 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 Anwendungsdienstes.

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: <ul style="list-style-type: none">- 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.
Analyst-Dienst	Der Benutzer kann Audit-Trail-Tabellen erstellen und löschen.
Metadata Manager-Dienst	Der Benutzer kann die folgenden Aktionen durchführen: <ul style="list-style-type: none">- 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: <ul style="list-style-type: none">- 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.

Berechtigung für	Beschreibung
PowerCenter-Repository-Dienst	<p>Der Benutzer kann die folgenden Aktionen durchführen:</p> <ul style="list-style-type: none"> - 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.
Test Data Manager-Dienst	<p>Der Benutzer kann die folgenden Aktionen durchführen:</p> <ul style="list-style-type: none"> - Test Data Manager-Repository-Inhalt erstellen und löschen. - Inhalt des Test Data Manager-Diensts aktualisieren.
Lizenzobjekt	<p>Der Benutzer kann die folgenden Aktionen durchführen:</p> <ul style="list-style-type: none"> - Bearbeiten von Lizenzobjekten. - Gewähren von Berechtigungen für Lizenzobjekte.
Lizenzobjekt und Anwendungsdienst	Der Benutzer kann einem Anwendungsdienst eine Lizenz zuweisen.
Domäne oder übergeordneter Ordner und Lizenzobjekt	Benutzer können Lizenzobjekte entfernen.

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 zugewiesen sind	Der Benutzer kann Gitter erstellen.
Knoten oder Gitter	<p>Der Benutzer kann die folgenden Aktionen durchführen:</p> <ul style="list-style-type: none"> - Knoten und Gitter zu konfigurieren und herunterzufahren. - Berechtigungen auf Knoten und Gittern gewähren.

Berechtigung für	Beschreibung
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: <ul style="list-style-type: none"> - 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 der Berechtigung „Verbindungen verwalten“ können auch Cluster-Konfigurationen erstellen, aktualisieren und löschen sowie Konfigurationseigenschaften im Administrator Tool und im infacmd-Befehlszeilenprogramm einrichten und löschen.

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.

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 und Cluster-Konfigurationen erstellen.
In Verbindung schreiben	Der Benutzer kann Verbindungen kopieren, bearbeiten und löschen.
Verbindung zuweisen	Der Benutzer kann Berechtigungen für Verbindungen gewähren und aufheben.
Schreiben in Cluster-Konfiguration	Der Benutzer kann Cluster-Konfigurationen erstellen, aktualisieren und löschen. Der Benutzer kann die Eigenschaften der Cluster-Konfiguration festlegen und löschen.

Überwachen-Berechtigungsgruppe

Die Berechtigungen in der Überwachen-Berechtigungsgruppe 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 Gruppe „Überwachung verwalten“ ausführen können:

Übergeordnete Berechtigung	Berechtigung	Berechtigung für	Beschreibung
Überwachung verwalten	Überwachungskonfiguration	Domäne	Benutzer können Überwachungseinstellungen konfigurieren.
Überwachung verwalten	Berichts- und Statistikeinstellungen	Domäne	Benutzer können Überwachungsstatistiken und -berichte konfigurieren.
Ansicht	Anzeigen der Jobs aller Benutzer in den Gruppen, zu denen der Benutzer gehört	Domäne	Ein Benutzer in einer Gruppe kann die Jobs überwachen, die von anderen Benutzern in der Gruppe ausgeführt werden. Wenn der Benutzer mehreren Gruppen angehört, kann der Benutzer die Jobs aus allen Gruppen anzeigen.
Anzeigen der Jobs aller Benutzer in den Gruppen, zu denen der Benutzer gehört	Jobs von anderen Benutzern anzeigen	Domäne	Benutzer können Jobs von anderen Benutzern anzeigen.
Ansicht	Statistik anzeigen	Domäne	Benutzer können die Ansicht „Übersichtsstatistik“ und Statistiken für Domänenobjekte anzeigen. Hinweis: In einer Domäne, die die Kerberos-Authentifizierung verwendet, benötigen Benutzer zudem die Administratorrolle für den überwachenden Modellrepository-Dienst, um die Ansicht „Übersichtsstatistik“ und Statistiken für die Domänenobjekte anzuzeigen.

Übergeordnete Berechtigung	Berechtigung	Berechtigung für	Beschreibung
Ansicht	Berichte anzeigen	Domäne	Benutzer können Berichte für die Domänenobjekte anzeigen.
Zugriffsüberwachung	Zugriff über das Analyst Tool	Domäne	Benutzer können auf den Arbeitsbereich „Jobstatus“ im Analyst Tool zugreifen.
Zugriffsüberwachung	Zugriff über Developer Tool	Domäne	Benutzer können über das Developer Tool auf das Monitoring Tool zugreifen.
Zugriffsüberwachung	Zugriff über Administrator Tool	Domäne	Benutzer können im Administrator Tool auf die Registerkarte „Überwachen“ zugreifen.
N/V	Aktionen für Jobs durchführen	Domäne	Benutzer können die folgenden Aktionen durchführen: <ul style="list-style-type: none"> - Abbrechen von Jobs. - Mapping-Jobs erneut ausgeben. - Job-Protokolle anzeigen.

Benutzer benötigen die Berechtigung „Zugriff auf Informatica Administrator“ nicht, um auf das Monitoring Tool zugreifen zu können.

Berechtigungsgruppe „Tools“

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	Beschreibung
Zugriff auf Informatica Administrator	Der Benutzer kann die folgenden Aktionen durchführen: <ul style="list-style-type: none"> - Melden Sie sich beim Administrator Tool an. - Das eigene Benutzerkonto im Administrator Tool zu verwalten. - Log-Ereignisse zu exportieren.

Der Benutzer muss über die Berechtigung „Zugriff auf Informatica Administrator“ verfügen, um Aufgaben im Administrator Tool abschließen zu können. Benutzer benötigen die Berechtigung „Zugriff auf Informatica Administrator“ nicht, um infacmd-Befehle auszuführen oder auf das Überwachungstool zuzugreifen.

Berechtigungsgruppe „Cloud-Verwaltung“

Über die Berechtigungen in der Gruppe „Cloud-Verwaltung“ wird festgelegt, welche Benutzer Informatica Cloud-Unternehmen 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-Dienst

Die Berechtigungen für den Analyst-Dienst 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 in Projekten. Ausführen auf einer relationalen Datenquellenverbindung.	Der Benutzer kann Profile und Scorecards für lizenzierte Benutzer im Analyst Tool ausführen.
Zugriff auf Mapping-Spezifikationen	Lesen in Projekten.	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.
Glossare anzeigen	–	Benutzer kann veröffentlichte Business Glossary-Objekte im Bibliotheks-Arbeitsbereich anzeigen. Dies entspricht dem Erteilen von Schreibberechtigungen für Glossare und Glossarobjekte im Glossarsicherheits-Arbeitsbereich.

Berechtigung	Berechtigung	Beschreibung
Zugriff auf Arbeitsbereiche	–	<p>Der Benutzer hat Zugriff auf die folgenden Arbeitsbereiche im Analyst Tool:</p> <ul style="list-style-type: none"> - Design-Arbeitsbereich. - Entdeckungs-Arbeitsbereich. - Glossary-Arbeitsbereich. - Scorecards-Arbeitsbereich. <p>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.</p>
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 Referenztabelle durchführen können.

In der folgenden Tabelle finden Sie eine Auflistung der Berechtigungen und Rechte, die zum Verwalten von Referenztabelle erforderlich sind:

Berechtigung	Berechtigung	Beschreibung
Referenztabelle erstellen	Schreiben in Projekt	<ul style="list-style-type: none">- Erstellen einer Referenztabelle im Analyst-Tool und im Developer-Tool.- Erstellen einer Referenztabelle mit infacmd rtm import.- Importieren eines Referenztabelleobjekt 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".
Referenztabelle und -Metadaten bearbeiten	Lesen im Projekt	<ul style="list-style-type: none">- Bearbeiten von Referenztabelle-Datenwerten im Developer-Tool und Analyst-Tool.- Hinzufügen von Profildaten zu einer Referenztabelle.- Hinzufügen oder Löschen von Spalten in einer Referenztabelle. Ändern der Referenztabelle-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.

Die folgende Tabelle enthält die Aktionen, die die Benutzer mit der Berechtigung in der Anwendungs-Administrations-Berechtigungsgruppe durchführen können:

Berechtigungsname	Beschreibung
Anwendungen verwalten	<p>Der Benutzer kann die folgenden Aktionen durchführen:</p> <ul style="list-style-type: none">- 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.

Berechtigung für den Massenerfassungsdienst

Die Berechtigung für den Massenerfassungsdienst bestimmt die Aktionen, die Benutzer mit dem Massenerfassungstool durchführen können.

In der folgenden Tabelle sind die Aktionen aufgelistet, die Benutzer mit der Berechtigung für den Massenerfassungsdienst durchführen können:

Berechtigung	Beschreibung
Zugriff auf Massenerfassungsspezifikation	Benutzer können die folgenden Aktionen durchführen: - Durchsuchen aller Massenerfassungsspezifikationen - Bearbeiten einer Massenerfassungsspezifikation - Ausführen einer Massenerfassungsspezifikation - Löschen einer Massenerfassungsspezifikation

Hinweis: Benutzer, denen die Zugriffsberechtigung für die Massenerfassungsspezifikation oder die Administratorrolle für die Domäne nicht zugewiesen wird, können diese Aktionen nur für die von ihnen selbst erstellten Massenerfassungsspezifikationen durchführen.

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.

Berechtigungsgruppe	Beschreibung
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: <ul style="list-style-type: none"> - 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.
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: <ul style="list-style-type: none"> - 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.

Berechtigung	Beinhaltet Berechtigungen	Berechtigung	Beschreibung
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	<ul style="list-style-type: none"> - Kommentare posten - Kommentare anzeigen 	Schreiben	Der Benutzer kann Kommentare zu Metadatenobjekten, Kategorien und Geschäftsbegriffen löschen.
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: <ul style="list-style-type: none"> - Anzeigen von Geschäftsglossaren in der Ansicht Glossar. - Suchen von Geschäftsglossaren.
Objekte verwalten	n/v	Schreiben	Der Benutzer kann die folgenden Aktionen durchführen: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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. Fügen Sie im Lieferumfang enthaltenen und universellen Modellen Attribute hinzu.
Modelle exportieren und importieren	Modell anzeigen	-	Der Benutzer kann benutzerdefinierte Modelle importieren und exportieren. Importieren und exportieren Sie geänderte, im Lieferumfang enthaltene und universelle Modelle.

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 Sicherheitsberechtigungsgruppe 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: <ul style="list-style-type: none">- 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 Objektberechtigungen des Modellrepository legen die Aufgaben fest, die Benutzer mit 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
N. z.	Lesen im Projekt	Benutzer können Projekte und Objekte in Projekten anzeigen.
N. z.	Schreiben in Projekt	Benutzer können Objekte in Projekten erstellen, bearbeiten und löschen.
N. z.	Gewähren bei Projekten	Benutzer können Benutzern und Gruppen Berechtigungen für Projekte gewähren und entziehen.
Zugriff auf Analyst	N. z.	Benutzer können über das Analyst Tool auf das Modellrepository zugreifen.
Zugriff auf Developer	N. z.	Benutzer können über das Developer Tool auf das Modellrepository zugreifen.
Erstellen, Bearbeiten und Löschen von Projekten	N. z.	Benutzer können Projekte erstellen.
Erstellen, Bearbeiten und Löschen von Projekten	Schreiben in Projekten	Benutzer können die folgenden Aktionen durchführen: <ul style="list-style-type: none"> - 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	N. z.	Benutzer können Datendomänen im Datendomänenglossar erstellen, bearbeiten und löschen. Diese Berechtigung ist Teil der Berechtigungsgruppe Datendomänen-Administration .
Verwalten von Benachrichtigungen	N. z.	Benutzer können Scorecard-Benachrichtigungen konfigurieren. Diese Berechtigung ist Teil der Berechtigungsgruppe Profiling-Administration .

Berechtigung	Berechtigung	Beschreibung
Verwalten von teambasierter Entwicklung	N. z.	Benutzer können den Status von gesperrten oder entsperrten Modellrepository-Objekten verwalten. Wenn das Modellrepository mit einem Versionsverwaltungssystem integriert ist, kann der Benutzer den Status von ausgecheckten oder eingecheckten Objekten verwalten. Der Benutzer kann zudem die Eigentümerschaft von ausgecheckten Objekten verwalten.
Anzeigen von Sicherheitsdetails	N. z.	Benutzer können die folgenden Details anzeigen: <ul style="list-style-type: none"> - Namen der Projekte, für die Benutzer keine Leseberechtigung haben. - Fehler- und Warnmeldungsdetails.

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-Ordern.
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: <ul style="list-style-type: none">- Verbindung mit dem PowerCenter-Repository mithilfe von Repository Manager herstellen.- <i>pmrep</i>-Befehle ausführen.
Workflow Manager öffnen	-	Der Benutzer kann die folgenden Aktionen durchführen: <ul style="list-style-type: none">- 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: <ul style="list-style-type: none">- 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 Ordneigentum 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 Ordneigentümers.
- 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: <ul style="list-style-type: none"> - 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 Ordner Ebene durchführen.

In der folgenden Tabelle werden die zusätzlich erforderlichen Berechtigungen aufgelistet und die Aktionen, die Benutzer mit der Berechtigung "Ordner Versionen verwalten" ausführen können:

Berechtigung	Beschreibung
Lesen und Schreiben in Ordner	Der Benutzer kann die folgenden Aktionen durchführen: <ul style="list-style-type: none"> - Den Status von Ordnern zu ändern. - Weitreichende Löschaktionen für Objektversionen auf Ordner Ebene 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: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none">- 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: <ul style="list-style-type: none">- 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 denselben 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: <ul style="list-style-type: none"> - 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
- Quellddefinitionen
- 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: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none">- 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: <ul style="list-style-type: none">- 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	<p>Der Benutzer kann die folgenden Aktionen durchführen:</p> <ul style="list-style-type: none"> - 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	<p>Der Benutzer kann die folgenden Aktionen durchführen:</p> <ul style="list-style-type: none"> - 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	<p>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.</p>

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: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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	<p>Der Benutzer kann die folgenden Aktionen durchführen:</p> <ul style="list-style-type: none"> - 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	<p>Der Benutzer kann die folgenden Aktionen durchführen:</p> <ul style="list-style-type: none"> - Eigenschaften von Laufzeitobjekten im Workflow Monitor anzeigen. - Sitzungs- und Arbeitsablauf-Logs im Workflow Monitor anzeigen. - Laufzeitobjekte und Performedetails im Workflow Monitor anzeigen. <p>Wenn der PowerCenter Integration Service im abgesicherten Modus läuft, müssen die Benutzer über die Administrator-Rolle für den zugehörige PowerCenter Repository Service verfügen.</p>

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	<p>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.</p> <p>Wenn der PowerCenter Integration Service im abgesicherten Modus läuft, müssen die Benutzer über die Administrator-Rolle für den zugehörige PowerCenter Repository Service verfügen.</p>

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: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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	<p>Der Benutzer kann die folgenden Aktionen durchführen:</p> <ul style="list-style-type: none"> - Wiederherstellen von Tasks und Arbeitsabläufen, die von anderen Benutzern gestartet wurden. - Wiederherstellen von Tasks, die automatisch wiederhergestellt wurden. <p>Wenn der PowerCenter Integration Service Betriebssystemprofile nutzt, müssen die Benutzer auch über Berechtigungen für das Betriebssystemprofil verfügen.</p> <p>Wenn der PowerCenter Integration Service im abgesicherten Modus läuft, müssen die Benutzer über die Administrator-Rolle für den zugehörige PowerCenter Repository Service verfügen.</p>
Schreiben, Lesen und Ausführen in Ordner Lesen und Ausführen in Verbindungsobjekten	<p>Der Benutzer kann die folgenden Aktionen durchführen:</p> <ul style="list-style-type: none"> - 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. <p>Wenn der PowerCenter Integration Service Betriebssystemprofile nutzt, müssen die Benutzer auch über Berechtigungen für das Betriebssystemprofil verfügen.</p> <p>Wenn der PowerCenter Integration Service im abgesicherten Modus läuft, müssen die Benutzer über die Administrator-Rolle für den zugehörige PowerCenter Repository Service verfügen.</p>

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: <ul style="list-style-type: none"> - 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.

Berechtigungen des Scheduler-Diensts

Berechtigungen des Scheduler-Diensts bestimmen die Aktionen, die die Benutzer für Zeitpläne und geplante Jobs ausführen können.

In der folgenden Tabelle werden die Rechte des Scheduler-Diensts sowie die erforderlichen Berechtigungen beschrieben:

Berechtigung	Beschreibung	Erfordert Berechtigung für
Zeitplan erstellen	Benutzer kann Zeitpläne erstellen. Zum Erstellen eines Zeitplans muss der Benutzer auch über das Anwendungsverwaltungsrecht im Datenintegrationsdienst verfügen.	<ul style="list-style-type: none"> - Scheduler-Dienst - Datenintegrationsdienst, in dem die vom Benutzer zu planenden Jobs ausgeführt werden
Zeitplan bearbeiten	Benutzer können Zeitpläne bearbeiten, anhalten und fortsetzen. Zum Bearbeiten eines Zeitplans muss der Benutzer auch über das Anwendungsverwaltungsrecht im Datenintegrationsdienst verfügen.	<ul style="list-style-type: none"> - Scheduler-Dienst - Datenintegrationsdienst, in dem die vom Benutzer zu planenden Jobs ausgeführt werden

Berechtigung	Beschreibung	Erfordert Berechtigung für
Zeitplan löschen	Benutzer können Zeitpläne löschen.	Scheduler-Dienst
Zeitpläne anzeigen	Benutzer können die Ansicht Zeitpläne und Zeitpläne anzeigen.	Scheduler-Dienst

Berechtigungen für Test Data Manager-Dienst

Die Berechtigungen für den Test Data Manager-Dienst bestimmen die Aktionen, die Benutzer mithilfe von Test Data Manager durchführen können. Sie können Berechtigungen auf der Registerkarte **Sicherheit** des Administrator Tools konfigurieren.

In der folgenden Tabelle werden alle Test Data Manager-Berechtigungsgruppen beschrieben:

Berechtigungsgruppe	Beschreibung
Verwaltung	Enthält Berechtigungen zum Erstellen und Verwalten von Verbindungen, Passphrasen und Rollen, zum Zuweisen von Rechten zu Benutzern und Benutzergruppen über Informatica Administrator, zum Verwalten von Repositories, 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	Enthält Berechtigungen zum Anzeigen und Verwalten von Datendomänen im Test Data Manager.
Datenmaskierung	Enthält Berechtigungen zum Anzeigen und Verwalten von Maskierungsregeln und Richtlinienzuweisungen im Test Data Manager.
Richtlinien	Enthält Berechtigungen zum Anzeigen und Verwalten von Richtlinien im Test Data Manager.
Projekte	Enthält Berechtigungen zum Anzeigen und Verwalten von Projekten, zum Prüfen und Importieren von Metadaten sowie zum Ausführen von Plänen und Arbeitsabläufen im Test Data Manager.

Berechtigungsgruppe „Verwaltung“

Die Berechtigungen in der Berechtigungsgruppe „Verwaltung“ bestimmen die Verwaltungsaufgaben, die Testdaten-Administratoren durchführen können.

Die folgende Tabelle enthält eine Liste der Berechtigungen in der Berechtigungsgruppe „Verwaltung“ und die für die Ausführung einer Aufgabe an einem Objekt erforderlichen Berechtigungen.

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: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none">- 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.

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: <ul style="list-style-type: none">- Richtlinien erstellen- Richtlinien bearbeiten- Richtlinien löschen- Richtlinien anzeigen

Berechtigungsgruppe „Projekte“

Die Berechtigungen in der Berechtigungsgruppe „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 „Projekte“ und die für die Ausführung einer Aufgabe an einem Objekt erforderlichen Berechtigungen.

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 Berechtigungsgruppe „Verwaltung“ anzeigen. Zum Erstellen eines Plans.
- Datenteilmenge aus der Berechtigungsgruppe für Datenteilmenge anzeigen. Zum Erstellen eines Plans mit Teilmengenkompontenten.
- Maskierungsregeln aus der Berechtigungsgruppe „Regeln“ anzeigen. Zum Erstellen eines Plans mit Maskierungskomponenten.

Regel-Berechtigungsgruppe

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.

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: <ul style="list-style-type: none">- 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.

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 einem Benutzer oder einer Gruppe für die Domäne, den Analyst-Dienst, den Datenintegrationsdienst, den Massenerfassungsdienst, den Metadata Manager-Dienst, den Modellrepository-Dienst oder den PowerCenter-Repository-Dienst die Administratorrolle zuweisen, erhält dieser Benutzer oder 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.

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.

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, den Massenerfassungsdienst und den PowerCenter-Repository-Dienst erfordern:

Dienst	Aufgaben
Domäne	<ul style="list-style-type: none"> - Konfigurieren von Domäneneigenschaften. - Konfigurieren Sie Cluster-Konfigurationen. - 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	<ul style="list-style-type: none"> - Upgraden des Datenintegrationsdienstes mit dem Menü Aktionen.
Massenerfassungsdienst	<ul style="list-style-type: none"> - Durchsuchen aller Massenerfassungsspezifikationen. - Bearbeiten einer Massenerfassungsspezifikation. - Ausführen einer Massenerfassungsspezifikation. - Löschen einer Massenerfassungsspezifikation.
PowerCenter-Repository-Dienst	<ul style="list-style-type: none"> - Zuweisen von Betriebssystemprofilen zu Repository-Ordnern, wenn der PowerCenter-Integrationsdienst Betriebssystemprofile verwendet.* - Ändern des Besitzers von Ordnern und globalen Objekten.* - Konfigurieren von 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 der gemeinsam zu verwendenden Ordner.* - Bearbeiten des Namens und der Beschreibung von Ordnern.* <p>*Diese Aufgaben kann auch der Eigentümer des PowerCenter-Repository-Ordners oder der globale Objekteigentümer ausführen.</p>

Benutzerdefinierte Rollen

Eine benutzerdefinierte Rolle lässt sich bearbeiten und löschen.

Standardmäßig enthält das Administrator Tool die folgenden benutzerdefinierten Rollen:

- Benutzerdefinierte Rolle für den Analyst-Dienst
- Benutzerdefinierte Rollen für den Metadata Manager-Dienst
- Benutzerdefinierte Rolle für den Operator
- Benutzerdefinierte Rollen für den PowerCenter-Repository-Dienst
- Benutzerdefinierte Rollen für den Test Data Manager-Dienst

Sie können die Berechtigungen für diese Rollen bearbeiten oder die Rollen löschen. Außerdem können Sie Ihre eigenen benutzerdefinierten Rollen erstellen.

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. Wenn 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.

Sie können Benutzern und Gruppen in den folgenden Situationen keine Berechtigungen oder Rollen für einen Metadata Manager- oder PowerCenter-Repository-Dienst zuweisen:

- Der Anwendungsdienst ist deaktiviert.
- Der PowerCenter-Repository-Dienst 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 können Sie nicht widerrufen. Sie können einem Benutzer oder einer Gruppe weitere Berechtigungen zuweisen, die keine von einer Gruppe oder Rolle geerbt 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.

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.

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 oder PowerCenter-Repository-Dienst zuweisen.

Sie können Benutzern in den folgenden Situationen keine Berechtigungen oder Rollen für einen vorhandenen Metadata Manager-Dienst oder PowerCenter-Repository-Dienst zuweisen:

- Der Anwendungsdienst ist deaktiviert.
- Der PowerCenter-Repository-Dienst wird im exklusiven Modus ausgeführt.

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.

- Ordneigentümer 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 10

Berechtigungen

Dieses Kapitel umfasst die folgenden Themen:

- [Berechtigungen - Übersicht, 197](#)
- [Domänenobjektberechtigungen, 199](#)
- [Verbindungsberechtigungen, 204](#)
- [Berechtigungen für die Cluster-Konfiguration, 206](#)
- [Anwendungs- und Anwendungsobjektberechtigungen, 207](#)
- [SQL-Datendienst-Berechtigungen, 209](#)
- [Web-Dienstmodul, 213](#)

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 PowerCenter-Repository-Dienst der Entwicklung, aber nicht für den PowerCenter-Repository-Dienst der Produktion. Der Benutzer kann den PowerCenter-Repository-Dienst der Entwicklung bearbeiten oder entfernen, aber nicht den PowerCenter-Repository-Dienst der Produktion. 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:

Objektyp	Tool	Beschreibung
Anwendungen und Anwendungsobjekte	Administrator Tool	Sie können Anwendungen und Anwendungsobjekten, wie z. B. Mappings und Arbeitsabläufen, Berechtigungen zuweisen.
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.

Objekttyp	Tool	Beschreibung
Domänenobjekte	Administrator Tool	Sie können Berechtigungen für die folgenden Domänenobjekte zuweisen: Domäne, Ordner, Knoten, Gitter, Lizenzen, Anwendungsdienste und Betriebssystemprofile.
Metadata Manager-Katalogobjekte	Metadata Manager	Sie können Ordnern und Katalogobjekten in Metadata Manager Berechtigungen 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 Ordner, Bereitstellungsgruppen, Bezeichnungen, Abfragen und Verbindungsobjekte in PowerCenter 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 Webdienstvorgänge zuweisen.

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.

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.

Domänenobjekttyp	Beschreibung der Berechtigung
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 Informatica-Entwicklern, -Analysten und -Anwendern, die dem Betriebssystemprofil zugeordnet sind, das Ausführen von Mappings, Profilen und Arbeitsabläufen. Ermöglicht PowerCenter-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.

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 auf der Registerkarte „Verwalten“ die Ansicht **Dienste und Knoten** aus.
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 die Herkunft effektiver Berechtigungen anzeigen.

1. Wählen Sie auf der Registerkarte „Verwalten“ die Ansicht **Dienste und Knoten** aus.
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 auf der Registerkarte „Verwalten“ die Ansicht **Dienste und Knoten** aus.
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 Administrator Tool auf die Registerkarte **Sicherheit**.
2. Klicken Sie auf die Registerkarte **Gruppen** oder **Benutzer**.
3. Wählen Sie einen Benutzer oder eine Gruppe aus.
4. Klicken Sie auf die Registerkarte **Berechtigungen**.

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.

Durch Anklicken von **Berechtigungsdetails anzeigen** können Sie anzeigen, ob die Berechtigung direkt zugeordnet oder geerbt wurde. Wenn Sie eine Berechtigung für das Objekt widerrufen, kann der Benutzer oder die Gruppe die Berechtigung trotzdem von einer übergeordneten Gruppe oder einem übergeordneten Objekt erben.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Sicherheit**.
2. Klicken Sie auf die Registerkarte **Gruppen** oder **Benutzer**.
3. Wählen Sie einen Benutzer oder eine Gruppe aus.
4. Klicken Sie auf die Registerkarte **Berechtigungen**.
5. Wählen Sie ein Domänenobjekt aus, und klicken Sie auf **Direkte Berechtigungen bearbeiten**.
6. Um dem Objekt eine Berechtigung zuzuweisen, wählen Sie **Zulassen**.
7. Um Berechtigungen für das Objekt zu widerrufen, wählen Sie **Widerrufen**.
8. Klicken Sie auf **OK**.

Betriebssystemprofil-Berechtigungen

Weisen Sie Berechtigungen für Betriebssystemprofile auf der Seite „Sicherheit“ des Administrator Tools zu, zeigen Sie sie an und bearbeiten Sie sie.

Die Administratorgruppe verfügt über Berechtigungen für alle Betriebssystemprofile.

Berechtigungen für ein Betriebssystemprofil zuweisen

Wenn Sie einem Betriebssystemprofil Berechtigungen zuweisen, führen Informatica-Benutzer Mappings, Profile und Arbeitsabläufe mit dem Betriebssystemprofil aus. PowerCenter-Benutzer führen Arbeitsabläufe aus, die dem Betriebssystemprofil zugewiesen sind.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Sicherheit**.
2. Klicken Sie auf die Registerkarte **Betriebssystemprofile**.
3. Wählen Sie ein Betriebssystemprofil aus, und klicken Sie dann auf die Registerkarte **Berechtigungen**.

4. Klicken Sie auf die Registerkarte **Gruppen** oder **Benutzer**, und wählen Sie dann **Direkte Berechtigungen bearbeiten** aus.
5. Wählen Sie ein Domänenobjekt aus, und klicken Sie auf **Direkte Berechtigungen bearbeiten**.
6. Um dem Objekt eine Berechtigung zuzuweisen, wählen Sie **Zulassen**.
7. Um Berechtigungen für das Objekt zu widerrufen, wählen Sie **Widerrufen**.
8. Klicken Sie auf **OK**.

Berechtigungsdetails zu Betriebssystemprofilen anzeigen

Beim Anzeigen von Berechtigungsdetails können Sie die Herkunft effektiver Berechtigungen anzeigen.

1. Wählen Sie auf der Registerkarte **Sicherheit** die Ansicht **Betriebssystemprofile** aus.
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 **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. Wählen Sie auf der Registerkarte **Sicherheit** die Ansicht **Betriebssystemprofile** aus.
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 **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.

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. Gruppe A verfügt auch über eine Berechtigung für Verbindung A 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 Gewährsberechtigungen 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 Ausführungsberechtigungen, wenn ein Benutzer versucht, eine Datenvorschau anzuzeigen oder ein Mapping, eine Scorecard 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.	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. Wählen Sie auf der Registerkarte „Verwalten“ 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. Wählen Sie auf der Registerkarte „Verwalten“ 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. 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.

6. Klicken Sie auf **Schließen**
7. 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. Wählen Sie auf der Registerkarte „Verwalten“ 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**.

Berechtigungen für die Cluster-Konfiguration

Berechtigungen steuern die Zugriffsebene für Benutzer oder Gruppen in einer Cluster-Konfiguration.

Sie können Berechtigungen für eine Cluster-Konfiguration im Administrator Tool und in der Informatica-Befehlszeilenschnittstelle konfigurieren.

Ein Benutzer oder eine Gruppe kann über die folgenden Berechtigungen in einer Cluster-Konfiguration verfügen:

- Lesen. Der Benutzer oder die Gruppenmitglieder können die Cluster-Konfiguration anzeigen.
- Schreiben. Der Benutzer oder die Gruppenmitglieder können die Cluster-Konfiguration bearbeiten. Enthält Leseberechtigungen.
- Ausführen. Der Benutzer oder die Gruppenmitglieder können Zuordnungen in der Hadoop-Umgebung ausführen.
- Gewähren. Der Benutzer oder die Gruppenmitglieder können anderen Benutzern und Gruppen die Berechtigung für die Cluster-Konfiguration erteilen. Enthält Leseberechtigungen.
- Alle. Der Benutzer erbt alle zulässigen Berechtigungen.

Standardmäßig verfügen alle Benutzer über die Berechtigung zum Anzeigen des Namens der Cluster-Konfiguration.

Anwendungs- und Anwendungsobjektberechtigungen

Mit Berechtigungen wird die Zugriffsebene eines Benutzers oder einer Gruppe für Anwendungen und Anwendungsobjekte, wie z. B. Mappings und Arbeitsabläufe, gesteuert.

Sie können Berechtigungen für Anwendungen oder Anwendungsobjekte im Administrator Tool oder über die Befehlszeile konfigurieren.

Typen von Anwendungs- und Anwendungsobjektberechtigungen

Sie können Benutzern und Gruppen Berechtigungen zuweisen und gewähren sowie Berechtigungen anzeigen und ausführen.

Sie können Benutzern und Gruppen die folgenden Berechtigungen zuweisen:

Berechtigung anzeigen

Zeigen Sie Anwendungen und Anwendungsobjekte an.

Berechtigung gewähren

Gewähren und widerrufen Sie Berechtigungen für Anwendungen und Anwendungsobjekte.

Berechtigung ausführen

Führen Sie Anwendungen und Anwendungsobjekte aus.

Hinweis: Um Anwendungsvorgänge wie Starten, Stoppen oder Sichern im Administrator Tool oder über die Befehlszeile durchzuführen, muss der Benutzer über die Ausführungsberechtigung und die Berechtigung zum Verwalten von Anwendungen für die Anwendung verfügen.

Zuweisen von Berechtigungen zu einer Anwendung oder einem Anwendungsobjekt

Wenn Sie einer Anwendung oder einem Anwendungsobjekt Berechtigungen zuweisen, definieren Sie die Zugriffsebene eines Benutzers oder einer Gruppe für die Anwendung oder das Anwendungsobjekt.

1. Wählen Sie auf der Registerkarte „Verwalten“ die Ansicht **Dienste und Knoten** aus.
2. Wählen Sie im Navigator einen Datenintegrationsdienst.
3. In der Inhaltsübersicht wählen Sie die Ansicht **Anwendungen**.
4. Wählen Sie eine Anwendung, ein Mapping oder einen Arbeitsablauf aus.
5. Wählen Sie im Fenster „Details“ die Ansicht **Gruppenberechtigungen** oder **Benutzerberechtigungen** aus.
6. Klicken Sie auf die Schaltfläche **Berechtigung zuweisen**.
Im Dialogfeld **Berechtigungen zuweisen** werden alle Benutzer oder Gruppen angezeigt, die keine Berechtigung für die Anwendung oder das Anwendungsobjekt aufweisen.
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**.

Anzeigen von Berechtigungsdetails für eine Anwendung oder ein Anwendungsobjekt

Beim Anzeigen von Berechtigungsdetails können Sie die Herkunft effektiver Berechtigungen anzeigen.

1. Wählen Sie auf der Registerkarte „Verwalten“ die Ansicht **Dienste und Knoten** aus.
2. Wählen Sie im Navigator einen Datenintegrationsdienst.
3. In der Inhaltsübersicht wählen Sie die Ansicht **Anwendungen**.
4. Wählen Sie die Anwendung, das Mapping oder den Arbeitsablauf aus.
5. Wählen Sie im Fenster „Details“ die Ansicht **Gruppenberechtigungen** oder **Benutzerberechtigungen** aus.
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 eine Anwendung oder ein Anwendungsobjekt

Sie können direkte Berechtigungen für eine Anwendung oder ein Anwendungsobjekt 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 auf der Registerkarte „Verwalten“ die Ansicht **Dienste und Knoten** aus.
2. Wählen Sie im Navigator einen Datenintegrationsdienst.
3. In der Inhaltsübersicht wählen Sie die Ansicht **Anwendungen**.
4. Wählen Sie die Anwendung oder das Anwendungsobjekt aus.
5. Wählen Sie im Fenster „Details“ die Ansicht **Gruppenberechtigungen** oder **Benutzerberechtigungen** aus.
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 eine Anwendung oder ein Anwendungsobjekt

Sie können Berechtigungen für eine Anwendung und Anwendungsobjekte explizit verweigern. Wenn Sie eine Berechtigung verweigern, wenden Sie eine Ausnahme auf die gültige Berechtigung an.

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 auf der Registerkarte „Verwalten“ die Ansicht **Dienste und Knoten** aus.
2. Wählen Sie im Navigator einen Datenintegrationsdienst.
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 die Herkunft effektiver Berechtigungen anzeigen.

1. Wählen Sie auf der Registerkarte „Verwalten“ die Ansicht **Dienste und Knoten** aus.
2. Wählen Sie im Navigator einen Datenintegrationsdienst.
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 auf der Registerkarte „Verwalten“ die Ansicht **Dienste und Knoten** aus.
2. Wählen Sie im Navigator einen Datenintegrationsdienst.
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 verweigte 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 Ergebniserersatz 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-Produktverwendung:

https://kb.informatica.com/h2l/HowTo%20Library/1/0266_ConfiguringSecurityForSQLDataServices.pdf.

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 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 eingeschränkte Spalte konfigurieren, schlägt 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
- REST-Webdienstressource
- SOAP-Webdienstvorgang

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

Ein Administrator weist den folgenden Benutzer- und Gruppentypen Webdienstberechtigungen zu:

- Webdienstbenutzer. Der Benutzer einer nativen Domäne, der eine Anfrage an den Webdienst sendet und eine Antwort vom Webdienst erhält. Der Benutzer muss über Ausführungsberechtigungen für den Webdienst verfügen.
- Webdienstadministrator. Ein Benutzer, der sich als Administrator anmelden, die Webdiensteigenschaften bearbeiten und anderen Benutzern Berechtigungen gewähren kann.
- Webdienstbetreiber. Ein Benutzer, der sich als Administrator anmelden, einen Webdienst überwachen und einen Webdienst starten oder beenden kann.

Ein Administrator kann Benutzern und Gruppen die folgenden Berechtigungen zuweisen:

- 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.

In der folgenden Tabelle werde die Berechtigungen für jedes SOAP-Webdienstobjekt beschrieben:

Objekt	Berechtigung gewähren	Ausführungsberechtigung
SOAP-Webdienst	Gewähren und Entziehen der Berechtigung für den Webdienst sowie für alle Webdienstvorgänge innerhalb des Webdiensts.	Senden von Webdienstanfragen und Empfangen von Webdienstantworten aus allen Webdienstvorgängen innerhalb des Webdiensts.
SOAP-Webdienstvorgang	Gewähren, Entziehen und Verweigern der Berechtigung für den Webdienstvorgang.	Senden von Webdienstanfragen und Empfangen von Webdienstantworten aus dem Webdienstvorgang.

In der folgenden Tabelle werden die Berechtigungen für jedes REST-Webdienstobjekt beschrieben:

Objekt	Berechtigung gewähren	Ausführungsberechtigung
REST-Webdienst	Gewähren und Entziehen der Berechtigung für den REST-Webdienst sowie für alle Webdienstressourcen innerhalb des Webdiensts.	Senden von Webdienstanfragen und Empfangen von Webdienstantworten aus allen Webdienstressourcen im REST-Webdienst.
REST-Ressource	Gewähren, Entziehen und Verweigern der Berechtigung für die REST-Webdienstressource.	Senden von Webdienstanfragen und Empfangen von Webdienstantworten aus der REST-Webdienstressource.

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 auf der Registerkarte „Verwalten“ die Ansicht **Dienste und Knoten** aus.
2. Wählen Sie im Navigator einen Datenintegrationsdienst.
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 die Herkunft effektiver Berechtigungen anzeigen.

1. Wählen Sie auf der Registerkarte „Verwalten“ die Ansicht **Dienste und Knoten** aus.
2. Wählen Sie im Navigator einen Datenintegrationsdienst.
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 auf der Registerkarte „Verwalten“ die Ansicht **Dienste und Knoten** aus.
2. Wählen Sie im Navigator einen Datenintegrationsdienst.
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 11

Auditberichte

Dieses Kapitel umfasst die folgenden Themen:

- [Auditberichte - Übersicht, 217](#)
- [Persönliche Benutzerinformationen, 218](#)
- [Benutzergruppen-Zuordnung, 218](#)
- [Berechtigungen, 220](#)
- [Rollenzuordnung, 220](#)
- [Domänenobjektberechtigung, 221](#)
- [Auswählen von Benutzern für einen Auditbericht, 221](#)
- [Auswählen von Gruppen für einen Auditbericht, 222](#)
- [Auswählen von Rollen für einen Auditbericht, 222](#)

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.

Berechtigungs Pfad

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 **Berichtsausgabeformat** 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 **Berichtsausgabeformat** 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

Befehlszeilenberechtigungen

Dieser Anhang umfasst die folgenden Themen:

- [infacmd as Befehle, 224](#)
- [infacmd cluster-Befehle, 225](#)
- [infacmd dis-Befehle, 226](#)
- [infacmd dp-Befehle, 228](#)
- [infacmd es-Befehle, 228](#)
- [infacmd ipc Befehlsprogramme, 228](#)
- [infacmd isp-Befehle, 228](#)
- [infacmd mas-Befehle, 238](#)
- [infacmd mi-Befehle, 239](#)
- [infacmd mrs Befehlsprogramme, 239](#)
- [infacmd ms-Befehle, 241](#)
- [infacmd tools-Befehle, 242](#)
- [infacmd ps Befehlsprogramme, 242](#)
- [infacmd pwx-Befehle, 243](#)
- [infacmd rms-Befehle, 244](#)
- [infacmd rtm Befehlsprogramme, 245](#)
- [infacmd sch-Befehle, 245](#)
- [infacmd sql - Befehle, 246](#)
- [infacmd wfs-Befehle, 247](#)
- [pmcmd-Befehle, 247](#)
- [pmrep Befehlsprogramme, 250](#)

infacmd as Befehle

Um *infacmd as* Befehle auszuführen, müssen die Benutzer über eines der gelisteten Sets von Domänenberechtigungen, Analyst-Dienst Berechtigungen und Domänenobjektberechtigungen verfügen.

Die folgende Tabelle enthält eine Auflistung der erforderlichen Berechtigungen für *infacmd* as Befehle:

infacmd as Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
CreateAuditTables	Domänen-Administration	Dienst verwalten	Domäne oder Knoten, auf der/dem der Analyst-Dienst ausgeführt wird
CreateService	Domänen-Administration	Dienst verwalten	Domäne oder Knoten, auf der/dem der Analyst-Dienst ausgeführt wird
DeleteAuditTables	Domänen-Administration	Dienst verwalten	Domäne oder Knoten, auf der/dem der Analyst-Dienst ausgeführt wird
ListServiceOptions	-	-	Analyst-Dienst
ListServiceProcessOptions	-	-	Analyst-Dienst
UpdateServiceOptions	Domänen-Administration	Dienst verwalten	Domäne oder Knoten, auf der/dem der Analyst-Dienst ausgeführt wird
UpdateServiceProcessOptions	Domänen-Administration	Dienst verwalten	Domäne oder Knoten, auf der/dem der Analyst-Dienst ausgeführt wird

infacmd cluster-Befehle

Zum Ausführen von *infacmd cluster*-Befehlen muss der Benutzer über einen der aufgelisteten Sätze an Domänen- und Cluster-Konfigurationsberechtigungen verfügen.

In der folgenden Tabelle werden die erforderlichen Rechte und Berechtigungen für *infacmd cluster*-Befehle aufgelistet:

infacmd cluster-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für...
clearConfigurationProperties	Domänenverwaltung	Verbindungen verwalten	Schreiben in Cluster-Konfiguration
createConfiguration	Domänenverwaltung	Verbindungen verwalten	Schreiben in Cluster-Konfigurationen
deleteConfiguration	Domänenverwaltung	Verbindungen verwalten	Schreiben in Cluster-Konfigurationen

infacmd cluster-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für...
exportConfiguration mit reaktiven Eigenschaften	-	-	Schreiben in Cluster-Konfiguration
exportConfiguration ohne reaktive Eigenschaften	-	-	Lesen in Cluster-Konfigurationen
listAssociatedConnections	-	-	-
listConfigurations	-	-	-
listConfigurationGroupPermissions	-	-	-
listConfigurationProperties	-	-	Lesen in Cluster-Konfigurationen
listConfigurationSets	-	-	Lesen in Cluster-Konfigurationen
listConfigurationUserPermissions	-	-	-
refreshConfiguration	Domänenverwaltung	Verbindungen verwalten	Schreiben in Cluster-Konfigurationen
setConfigurationPermissions	-	-	Gewähren in Cluster-Konfiguration
setConfigurationProperties	Domänenverwaltung	Verbindungen verwalten	Schreiben in Cluster-Konfigurationen

infacmd dis-Befehle

Um *infacmd dis*-Befehle ausführen zu können, benötigt der Benutzer eine der aufgeführten Gruppen von Domänenberechtigungen, Berechtigungen für Datenintegrationsdienste und Domänenobjektberechtigungen.

Aus der folgenden Tabelle gehen die erforderlichen Berechtigungen für *infacmd dis* Befehle hervor:

infacmd dis-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für...
BackupApplication	Anwendungsadministration	Anwendungen verwalten	Anwendung
CancelDataObjectCacheRefresh	-	-	-
CreateService	Domänen-Administration	Dienste verwalten	Domäne oder Knoten, auf der/dem der Datenintegrationsdienst ausgeführt wird

infacmd dis-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für...
DeployApplication	Anwendungsadministratio n	Anwendungen verwalten	Anwendung
ListApplicationObjects	–	–	–
ListApplications	–	–	–
ListComputeOptions	Domänen-Administration	Dienste verwalten	Datenintegrationsdienst
ListDataObjectOptions	–	–	–
ListServiceOptions	Domänen-Administration	Dienste verwalten	Datenintegrationsdienst
ListServiceProcessOptions	Domänen-Administration	Dienste verwalten	Datenintegrationsdienst
PurgeDataObjectCache	–	–	–
RefreshDataObjectCache	–	–	–
RenameApplication	Anwendungsadministratio n	Anwendungen verwalten	Anwendung
RestoreApplication	Anwendungsadministratio n	Anwendungen verwalten	Anwendung
StartApplication	Anwendungsadministratio n	Anwendungen verwalten	Anwendung
StopApplication	Anwendungsadministratio n	Anwendungen verwalten	Anwendung
stopBlazeService	Anwendungsadministratio n	Anwendungen verwalten	Anwendung
UndeployApplication	Anwendungsadministratio n	Anwendungen verwalten	Anwendung
UpdateApplication	Anwendungsadministratio n	Anwendungen verwalten	Anwendung
UpdateApplicationOptions	Anwendungsadministratio n	Anwendungen verwalten	Anwendung
UpdateDataObjectOptions	Anwendungsadministratio n	Anwendungen verwalten	–
UpdateComputeOptions	Domänen-Administration	Dienste verwalten	Datenintegrationsdienst
UpdateServiceOptions	Domänen-Administration	Dienste verwalten	Datenintegrationsdienst
UpdateServiceProcessOpti ons	Domänen-Administration	Dienste verwalten	Datenintegrationsdienst

infacmd dp-Befehle

Benutzer müssen native Benutzer sein oder über Administratorrechte verfügen, um die folgenden infacmd dp-Befehle auszuführen:

- startSparkJobServer
- stopSparkJobServer

infacmd es-Befehle

Einem Benutzer muss die Administratorrolle für die Domäne zugewiesen sein, damit er folgende infacmd es-Befehle ausführen kann:

- ListServiceOptions
- UpdateServiceOptions
- UpdateSMTPOptions

infacmd ipc Befehlsprogramme

Um ein *infacmd ipc*-Befehlsprogramm auszuführen, muss der Benutzer eine der aufgelisteten Berechtigungen für die Model Repository-Objekte besitzen.

Die nachstehende Tabelle für die erforderlichen Berechtigungen für die *infacmd isp* Befehlsprogramme auf:

infacmd ipc-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für...
ExportToPC	-	-	Lesen in dem Ordner, in dem die Referenztabellen für den Export erstellt werden
genReuseReportFromPC	Tools	Repository Manager öffnen	-

infacmd isp-Befehle

Um die *infacmd isp*-Befehle auszuführen, müssen die Benutzer eine der aufgeführten Zusammenstellungen für Domänenberechtigungen, Dienstberechtigungen, Domänenobjektberechtigungen und Verbindungsberechtigungen besitzen.

Die nachstehende Tabelle für die erforderlichen Berechtigungen für die *infacmd isp*-Befehle auf:

infacmd isp-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
AddAlertUser (für andere Benutzer)	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
AddAlertUser (für Ihr Benutzerkonto)	-	-	-
AddConnectionPermissions	-	-	Verbindung zuweisen
AddDomainLink*	-	-	-
AddDomainNode	Domänenverwaltung	Knoten und Gitter verwalten	Domäne und Knoten
AddGroupPrivilege	Sicherheitsverwaltung	Berechtigungen und Rollen gewähren	Domäne, Metadata Manager-Dienst, Modellrepository-Dienst oder PowerCenter-Repository-Dienst.
AddLicense	Domänenverwaltung	Dienste verwalten	Domäne oder übergeordneter Ordner
AddNodeResource	Domänenverwaltung	Knoten und Gitter verwalten	Knoten
AddRolePrivilege	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
AddServiceLevel*	-	-	-
AddUserToGroup	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
AssignGroupPermission (in Anwendungsdiensten oder Lizenzobjekten)	Domänenverwaltung	Dienste verwalten	Anwendungsdienst oder Lizenzobjekt
AssignGroupPermission (in der Domäne)*	-	-	-
AssignGroupPermission (in Ordnern)	Domänenverwaltung	Domänenordner verwalten	Ordner
AssignGroupPermission (auf Knoten und Gittern)	Domänenverwaltung	Knoten und Gitter verwalten	Knoten oder Gitter
AssignGroupPermission (in Betriebssystemprofilen)*	-	-	-
AssignISTOMMSERVICE	Domänenverwaltung	Dienste verwalten	Metadata Manager-Dienst
AssignLicense	Domänenverwaltung	Dienste verwalten	Lizenzobjekt und Anwendungsdienst

infacmd isp-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
AssignRSToWShubService	Domänenverwaltung	Dienste verwalten	PowerCenter-Repository-Dienst und Webdienst-Hub
AssignRoleToGroup	Sicherheitsverwaltung	Berechtigungen und Rollen gewähren	Domäne, Metadata Manager-Dienst, Modellrepository-Dienst oder PowerCenter-Repository-Dienst.
AssignRoleToUser	Sicherheitsverwaltung	Berechtigungen und Rollen gewähren	Domäne, Metadata Manager-Dienst, Modellrepository-Dienst oder PowerCenter-Repository-Dienst.
AssignUserPermission (in Anwendungsdiensten oder Lizenzobjekten)	Domänenverwaltung	Dienste verwalten	Anwendungsdienst oder Lizenzobjekt
AssignUserPermission (in der Domäne)*	-	-	-
AssignUserPermission (in Ordnern)	Domänenverwaltung	Domänenordner verwalten	Ordner
AssignUserPermission (auf Knoten und Gittern)	Domänenverwaltung	Knoten und Gitter verwalten	Knoten oder Gitter
AssignUserPermission (in Betriebssystemprofilen)*	-	-	-
AssignUserPrivilege	Sicherheitsverwaltung	Berechtigungen und Rollen gewähren	Domäne, Metadata Manager-Dienst, Modellrepository-Dienst oder PowerCenter-Repository-Dienst.
AssignedToLicense	Domänenverwaltung	Dienste verwalten	Lizenzobjekt und Anwendungsdienst
ConvertLogFile	-	-	Domäne oder Anwendungsdienst
CreateConnection*	-	-	-
CreateFolder	Domänenverwaltung	Domänenordner verwalten	Domäne oder übergeordneter Ordner
CreateGrid	Domänenverwaltung	Knoten und Gitter verwalten	Domäne oder übergeordneter Ordner und einem Gitter zugewiesene Knoten

infacmd isp-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
CreateGroup	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
CreateIntegrationService	Domänenverwaltung	Dienste verwalten	Domäne oder übergeordneter Ordner, Knoten oder Gitter, auf dem der PowerCenter-Integrationsdienst ausgeführt wird, Lizenzobjekt und zugehöriger PowerCenter-Repository-Dienst
CreateMMService	Domänenverwaltung	Dienste verwalten	Domäne oder übergeordneter Ordner, Knoten, auf dem der Metadata Manager-Dienst ausgeführt wird, Lizenzobjekt und zugehöriger PowerCenter-Integrationsdienst und PowerCenter-Repository-Dienst
CreateOSProfile*	-	-	-
CreateRepositoryService	Domänenverwaltung	Dienste verwalten	Domäne oder übergeordneter Ordner, Knoten, auf dem der PowerCenter-Repository-Dienst ausgeführt wird, und Lizenzobjekt
CreateRole	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
CreateSAPBWService	Domänenverwaltung	Dienste verwalten	Domäne oder übergeordneter Ordner, Knoten oder Gitter, auf dem der SAP BW-Dienst ausgeführt wird, Lizenzobjekt und zugehöriger PowerCenter-Integrationsdienst
CreateUser	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-

infacmd isp-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
CreateWSHubService	Domänenverwaltung	Dienste verwalten	Domäne oder übergeordneter Ordner, Knoten oder Gitter, auf dem der Webdienst-Hub ausgeführt wird, Lizenzobjekt und zugehöriger PowerCenter-Repository-Dienst
DisableNodeResource	Domänenverwaltung	Knoten und Gitter verwalten	Knoten
DisableService (für Metadata Manager-Dienst)	Domänenverwaltung	Dienstausführung verwalten	Metadata Manager-Dienst und zugehöriger PowerCenter-Integrationsdienst und PowerCenter-Repository-Dienst
DisableService (für alle anderen Anwendungsdienste)	Domänenverwaltung	Dienstausführung verwalten	Anwendungsdienst
DisableServiceProcess	Domänenverwaltung	Dienstausführung verwalten	Anwendungsdienst
DisableUser	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
EditUser	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
EnableNodeResource	Domänenverwaltung	Knoten und Gitter verwalten	Knoten
EnableService (für Metadata Manager-Dienst)	Domänenverwaltung	Dienstausführung verwalten	Metadata Manager-Dienst und zugehöriger PowerCenter-Integrationsdienst und PowerCenter-Repository-Dienst
EnableService (für alle anderen Anwendungsdienste)	Domänenverwaltung	Dienstausführung verwalten	Anwendungsdienst
EnableServiceProcess	Domänenverwaltung	Dienstausführung verwalten	Anwendungsdienst
EnableUser	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
ExportDomainObjects (für Verbindungen)	Domänenverwaltung	Verbindungen verwalten	In Verbindungen lesen

infacmd isp-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
ExportDomainObjects (für Benutzer, Gruppen und Rollen)	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
ExportUsersAndGroups	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
GetFolderInfo	-	-	Ordner
GetLastError	-	-	Anwendungsdienst
GetLog	-	-	Domäne oder Anwendungsdienst
GetNodeName	-	-	Knoten
GetServiceOption	-	-	Anwendungsdienst
GetServiceProcessOption	-	-	Anwendungsdienst
GetServiceProcessStatus	-	-	Anwendungsdienst
GetServiceStatus	-	-	Anwendungsdienst
GetSessionLog	Laufzeitobjekte	Überwachen	Im Repository-Ordner lesen
GetWorkflowLog	Laufzeitobjekte	Überwachen	Im Repository-Ordner lesen
Hilfe	-	-	-
ImportDomainObjects (für Verbindungen)	Domänenverwaltung	Verbindungen verwalten	In Verbindungen schreiben
ImportDomainObjects (für Benutzer, Gruppen und Rollen)	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
ImportUsersAndGroups	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
ListAlertUsers	-	-	Domäne
ListAllGroups	-	-	-
ListAllRoles	-	-	-
ListAllUsers	-	-	-
ListConnectionOptions	-	-	In Verbindung lesen
ListConnectionPermissions	-	-	-
ListConnectionPermissions nach Gruppe	-	-	-

infacmd isp-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
ListConnectionPermissions nach Benutzer	-	-	-
ListConnections	-	-	-
ListDomainLinks	-	-	Domäne
ListDomainOptions	-	-	Domäne
ListFolders	-	-	Ordner
ListGridNodes	-	-	-
ListGroupPermissions	-	-	-
ListGroupPrivilege	Sicherheitsverwaltung	Berechtigungen und Rollen gewähren	Domäne, Metadata Manager-Dienst, Modellrepository-Dienst oder PowerCenter-Repository-Dienst.
ListGroupsForUser	-	-	Domäne
ListLDAPConnectivity	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
ListLicenses	-	-	Lizenzobjekte
ListNodeOptions	-	-	Knoten
ListNodeResources	-	-	Knoten
ListNodes	-	-	-
ListPlugins	-	-	-
ListRepositoryLDAPConfiguration	-	-	Domäne
ListRolePrivileges	-	-	-
ListSMTPOptions	-	-	Domäne
ListSecurityDomains	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
ListServiceLevels	-	-	Domäne
ListServiceNodes	-	-	Anwendungsdienst
ListServicePrivileges	-	-	-
ListServices	-	-	-

infacmd isp-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
ListUserPermissions	-	-	-
ListUserPrivilege	Sicherheitsverwaltung	Berechtigungen und Rollen gewähren	Domäne, Metadata Manager-Dienst, Modellrepository-Dienst oder PowerCenter-Repository-Dienst.
MoveFolder	Domänenverwaltung	Domänenordner verwalten	Ursprungs- und Zielordner
MoveObject (für Anwendungsdienste oder Lizenzobjekte)	Domänenverwaltung	Dienste verwalten	Ursprungs- und Zielordner
MoveObject (für Knoten oder Gitter)	Domänenverwaltung	Knoten und Gitter verwalten	Ursprungs- und Zielordner
Ping	-	-	-
PurgeLog*	-	-	-
RemoveAlertUser (für andere Benutzer)	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
RemoveAlertUser (für Ihr Benutzerkonto)	-	-	-
RemoveConnection	-	-	In Verbindung schreiben
RemoveConnectionPermissions	-	-	Verbindung zuweisen
RemoveDomainLink*	-	-	-
RemoveFolder	Domänenverwaltung	Domänenordner verwalten	Domänenordner oder übergeordneter Ordner und zu entfernender Ordner
RemoveGrid	Domänenverwaltung	Knoten und Gitter verwalten	Domäne oder übergeordneter Ordner und Gitter
RemoveGroup	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
RemoveGroupPrivilege	Sicherheitsverwaltung	Berechtigungen und Rollen gewähren	Domäne, Metadata Manager-Dienst, Modellrepository-Dienst oder PowerCenter-Repository-Dienst.
RemoveLicense	Domänenverwaltung	Dienste verwalten	Domäne oder übergeordneter Ordner und Lizenzobjekt

infacmd isp-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
RemoveNode	Domänenverwaltung	Knoten und Gitter verwalten	Domäne oder übergeordneter Ordner und Knoten
RemoveNodeResource	Domänenverwaltung	Knoten und Gitter verwalten	Knoten
RemoveOSProfile*	-	-	-
RemoveRole	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
RemoveRolePrivilege	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
RemoveService	Domänenverwaltung	Dienste verwalten	Domäne oder übergeordneter Ordner und Anwendungsdienst
RemoveServiceLevel*	-	-	-
RemoveUser	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
RemoveUserFromGroup	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
RemoveUserPrivilege	Sicherheitsverwaltung	Berechtigungen und Rollen gewähren	Domäne, Metadata Manager-Dienst, Modellrepository-Dienst oder PowerCenter-Repository-Dienst.
RenameConnection	-	-	In Verbindung schreiben
ResetPassword (für andere Benutzer)	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
ResetPassword (für Ihr Benutzerkonto)	-	-	-
RunCUPProfile	Domänenverwaltung	Knoten und Gitter verwalten	Knoten
SetConnectionPermission	-	-	Verbindung zuweisen
SetLDAPConnectivity	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	-
SetRepositoryLDAPConfiguration	-	-	Domäne
ShowLicense	-	-	Lizenzobjekt

infacmd isp-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
ShutdownNode	Domänenverwaltung	Knoten und Gitter verwalten	Knoten
SwitchToGatewayNode*	-	-	-
SwitchToWorkerNode*	-	-	-
UnAssignISMMService	Domänenverwaltung	Dienste verwalten	PowerCenter-Integrationsdienst und Metadata Manager-Dienst
UnAssignRoleFromGroup	Sicherheitsverwaltung	Berechtigungen und Rollen gewähren	Domäne, Metadata Manager-Dienst, Modellrepository-Dienst oder PowerCenter-Repository-Dienst.
UnAssignRoleFromUser	Sicherheitsverwaltung	Berechtigungen und Rollen gewähren	Domäne, Metadata Manager-Dienst, Modellrepository-Dienst oder PowerCenter-Repository-Dienst.
UnassignLicense	Domänenverwaltung	Dienste verwalten	Lizenzobjekt und Anwendungsdienst
UnassignRSWSHubService	Domänenverwaltung	Dienste verwalten	PowerCenter-Repository-Dienst und Webdienst-Hub
UnassociateDomainNode	Domänenverwaltung	Knoten und Gitter verwalten	Knoten
UpdateConnection	-	-	In Verbindung schreiben
UpdateDomainOptions*	-	-	-
UpdateFolder	Domänenverwaltung	Domänenordner verwalten	Ordner
UpdateGatewayInfo*	-	-	-
UpdateGrid	Domänenverwaltung	Knoten und Gitter verwalten	Gitter und Knoten
UpdateIntegrationService	Domänenverwaltung	Dienste verwalten	PowerCenter-Integrationsdienst
UpdateLicense	Domänenverwaltung	Dienste verwalten	Lizenzobjekt
UpdateMMService	Domänenverwaltung	Dienste verwalten	Metadata Manager-Dienst
UpdateNodeOptions	Domänenverwaltung	Knoten und Gitter verwalten	Knoten

infacmd isp-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
UpdateNodeRole	Domänenverwaltung	Knoten und Gitter verwalten	Knoten
UpdateOSProfile	Sicherheitsverwaltung	Benutzer, Gruppen und Rollen verwalten	Betriebssystemprofil
UpdateRepositoryService	Domänenverwaltung	Dienste verwalten	PowerCenter-Repository-Dienst
UpdateSAPBWService	Domänenverwaltung	Dienste verwalten	SAP BW-Dienst
UpdateSMTPOptions*	-	-	-
UpdateServiceLevel*	-	-	-
UpdateServiceProcess	Domänenverwaltung	Dienste verwalten	PowerCenter-Integrationsdienst Jeder dem PowerCenter-Integrationsdienst hinzugefügte Knoten
UpdateWSHubService	Domänenverwaltung	Dienste verwalten	Webdienst-Hub
generateHadoopConnectionFromHiveConection	-	-	-
listMonitoringOptions	Überwachung	Überwachungskonfiguration	Domäne
purgeMonitoringData	Überwachung	Überwachungskonfiguration	Domäne
updateMonitoringOptions	Überwachung	Überwachungskonfiguration	Domäne
<i>*Um diese Befehle ausführen zu können, muss den Benutzern die Administratorrolle für die Domäne zugewiesen werden.</i>			

infacmd mas-Befehle

Um *infacmd mas*-Befehle, ausführen zu können, benötigt der Benutzer eine der aufgeführten Gruppen von Domänenberechtigungen, Berechtigungen für Metadaten-Zugriffsdienste und Domänenobjektberechtigungen.

Die nachstehende Tabelle führt die erforderlichen Rechte und Berechtigungen für die *infacmd mas*-Befehle auf:

infacmd dis-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für...
CreateService	Domänenverwaltung	Dienste verwalten	Domäne oder Knoten, wo der Metadaten-Zugriffsdienst ausgeführt wird
ListServiceOptions	Domänenverwaltung	Dienste verwalten	Metadaten-Zugriffsdienst
ListServiceProcessOptions	Domänenverwaltung	Dienste verwalten	Metadaten-Zugriffsdienst
UpdateServiceOptions	Domänenverwaltung	Dienste verwalten	Metadaten-Zugriffsdienst
UpdateServiceProcessOptions	Domänenverwaltung	Dienste verwalten	Metadaten-Zugriffsdienst

infacmd mi-Befehle

Zur Ausführung der folgenden infacmd mi-Befehle muss Benutzern im Massenerfassungsdienst die Administratorrolle zugewiesen werden:

- clearSamlConfig
- updateSamlConfig

infacmd mrs Befehlsprogramme

Um ein *infacmd mrs*-Befehlsprogramm ausführen zu können, muss der Benutzer über einen der aufgelisteten Sätze an Profil- und Domänenobjektberechtigungen verfügen.

Benutzer können für eigene Objekte die folgenden Befehle ausführen, die auf die Sperrung und Versionierung von Vorgängen bezogen sind. Die Ausführung der Befehle für Objekte, die andere Benutzer besitzen, ist die Berechtigung „Verwalten von teambasierter Entwicklung“ erforderlich:

- CheckInObject
- ListCheckedOutObjects
- ListLockedObjects
- UndoCheckout
- UnlockObject

Die nachstehende Tabelle führt die erforderlichen Berechtigungen für die *infacmd mrs* Befehlsprogramme auf:

Befehl <i>infacmd mrs</i>	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für...
BackupContents	Domänen-Administration	Dienst verwalten	Domäne oder Knoten, auf dem der Modellrepository-Dienst ausgeführt wird
CheckInObject	Domänen-Administration	Verwalten von teambasierter Entwicklung	Der Modellrepository-Dienst
CreateContents	Domänen-Administration	Dienst verwalten	Domäne oder Knoten, auf dem der Modellrepository-Dienst ausgeführt wird
CreateFolder	Domänen-Administration	Für Developer Tool: - Zugriff auf Developer Für Analyst Tool: - Zugriff auf Analyst - Zugriff auf Entdeckungs-Arbeitsbereich	Der Modellrepository-Dienst
CreateProject	Domänen-Administration	Erstellen, Bearbeiten und Löschen von Projekten	Der Modellrepository-Dienst
CreateService	Domänen-Administration	Dienst verwalten	Domäne oder Knoten, auf dem der Modellrepository-Dienst ausgeführt wird
DeleteContents	Domänen-Administration	Dienst verwalten	Domäne oder Knoten, auf dem der Modellrepository-Dienst ausgeführt wird
DeleteFolder	Domänen-Administration	Für Developer Tool: - Zugriff auf Developer Für Analyst Tool: - Zugriff auf Analyst - Zugriff auf Entdeckungs-Arbeitsbereich	Der Modellrepository-Dienst
DeleteProject	Domänen-Administration	Erstellen, Bearbeiten und Löschen von Projekten	Der Modellrepository-Dienst
ListBackupFiles	Domänen-Administration	Dienst verwalten	Domäne oder Knoten, auf dem der Modellrepository-Dienst ausgeführt wird
ListCheckedOutObjects	Domänen-Administration	Verwalten von teambasierter Entwicklung	Der Modellrepository-Dienst
ListFolders	Domänen-Administration	Dienst verwalten	Domäne oder Knoten, auf dem der Modellrepository-Dienst ausgeführt wird
ListLockedObjects	Domänen-Administration	Verwalten von teambasierter Entwicklung	Der Modellrepository-Dienst

Befehl infacmd mrs	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für...
ListProjects	Domänen-Administration	Für Developer Tool: - Zugriff auf Developer Für Analyst Tool: - Zugriff auf Analyst - Zugriff auf Entdeckungs-Arbeitsbereich	Domäne oder Knoten, auf dem der Modellrepository-Dienst ausgeführt wird
ListServiceOptions	–	–	Der Modellrepository-Dienst
ListServiceProcessOptions	–	–	Der Modellrepository-Dienst
PopulateVCS	Domänen-Administration	Verwalten von teambasierter Entwicklung	Der Modellrepository-Dienst
ReassignCheckedOutObject	Domänen-Administration	Verwalten von teambasierter Entwicklung	Der Modellrepository-Dienst
RebuildDependencyGraph	–	–	Der Modellrepository-Dienst
RenameFolder	Domänen-Administration	Für Developer Tool: - Zugriff auf Developer Für Analyst Tool: - Zugriff auf Analyst - Zugriff auf Entdeckungs-Arbeitsbereich	Der Modellrepository-Dienst
RestoreContents	Domänen-Administration	Dienst verwalten	Domäne oder Knoten, auf dem der Modellrepository-Dienst ausgeführt wird
UndoCheckout	Domänen-Administration	Verwalten von teambasierter Entwicklung	Der Modellrepository-Dienst
UnlockObject	Domänen-Administration	Verwalten von teambasierter Entwicklung	Der Modellrepository-Dienst
UpdateServiceOptions	Domänen-Administration	Dienst verwalten	Der Modellrepository-Dienst
UpdateServiceProcessOptions	Domänen-Administration	Dienst verwalten	Der Modellrepository-Dienst
UpgradeContents	Verwaltung des Modellrepository-Diensts	Dienst verwalten	Der Modellrepository-Dienst

infacmd ms-Befehle

Um ein *infacmd ms*-Befehlsprogramm auszuführen, muss der Benutzer eine der aufgelisteten Berechtigungen für das Domänenobjekt besitzen.

Die nachstehende Tabelle führt die erforderlichen Berechtigungen für die *infacmd ms* Befehlsprogramme auf:

infacmd ms-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für...
deleteMappingPersistedOutputs	-	-	Ausführen in der Anwendung
getRequestLog	-	-	-
listMappingParams	-	-	-
listMappingPersistedOutputs	-	-	Anzeigen in der Anwendung
listMappings	-	-	-
runMapping	-	-	Ausführen auf Verbindungsobjekten, die von Mappings benutzt werden

infacmd tools-Befehle

Um *infacmd tools*-Befehle auszuführen, muss der Benutzer eine der aufgelisteten Berechtigungen für die Modellrepository-Objekte besitzen.

In der nachstehenden Tabelle sind die erforderlichen Berechtigungen für die *infacmd tools*-Befehle aufgeführt:

infacmd tools-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für...
ExportObjects	-	-	Lesen im Projekt
ImportObjects	-	-	Schreiben in Projekt

infacmd ps Befehlsprogramme

Um *infacmd ps*-Befehle ausführen zu können, müssen Benutzer über einen der aufgeführten Sätze an Profilberechtigungen und Berechtigungen für Domänenobjekte verfügen.

Die nachstehende Tabelle führt die erforderlichen Berechtigungen für die *infacmd ps* Befehlsprogramme auf:

infacmd ps Befehlsprogramm	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
CreateWH	-	-	-
DropWH	-	-	-
Ausführen	-	-	Lesen in Projekt Quellverbindungsobjekt ausführen
Liste	-	-	Lesen in Projekt
Löschen	-	-	Lesen und Schreiben in Ordner

infacmd pwx-Befehle

Um *infacmd pwx*-Befehle auszuführen, müssen Benutzer einen der aufgeführten Sätze von PowerExchange-Anwendungsdienstberechtigungen besitzen.

Die nachstehende Tabelle führt die erforderlichen Berechtigungen für die *infacmd pwx* Befehlsprogramme auf:

infacmd pwx-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für...
CloseForceListener	Verwaltungsbefehle	closeforce	-
CloseListener	Verwaltungsbefehle	Schließen	-
CondenseLogger	Verwaltungsbefehle	Kondensieren	-
CreateListenerService	Domänenverwaltung	Dienst verwalten	Domäne oder Knoten, auf dem der PowerExchange-Anwendungsdienst ausgeführt wird
CreateLoggerService	Domänenverwaltung	Dienst verwalten	Domäne oder Knoten, auf dem der PowerExchange-Anwendungsdienst ausgeführt wird
DisplayAllLogger	Informationsbefehle	displayall	-
DisplayCPULogger	Informationsbefehle	displaycpu	-
DisplayEventsLogger	Informationsbefehle	displayevents	-

infacmd pwx-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für...
DisplayMemoryLogger	Informationsbefehle	displaymemory	-
DisplayRecordsLogger	Informationsbefehle	displayrecords	-
DisplayStatusLogger	Informationsbefehle	displaystatus	-
FileSwitchLogger	Verwaltungsbefehle	fileswitch	-
ListTaskListener	Informationsbefehle	listtask	-
ShutDownLogger	Verwaltungsbefehle	shutdown	-
StopTaskListener	Verwaltungsbefehle	stoptask	-
UpdateListenerService	Domänenverwaltung	Dienst verwalten	Domäne oder Knoten, auf dem der PowerExchange-Anwendungsdienst ausgeführt wird
UpdateLoggerService	Domänenverwaltung	Dienst verwalten	Domäne oder Knoten, auf dem der PowerExchange-Anwendungsdienst ausgeführt wird

infacmd rms-Befehle

Um *infacmd rms*-Befehle ausführen zu können, muss der Benutzer eine der aufgelisteten Berechtigungen und Rechte für die Domäne besitzen

Die nachstehende Tabelle führt die erforderlichen Berechtigungen für die *infacmd rms*-Befehle auf:

infacmd rms-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
ListComputeNodeAttributes	Domänen-Administration	-	Ressourcenmanager-Dienst
ListServiceOptions	Domänen-Administration	-	Ressourcenmanager-Dienst
SetComputeNodeAttributes	Domänen-Administration	Dienste verwalten	Ressourcenmanager-Dienst
UpdateServiceOptions	Domänen-Administration	Dienste verwalten	Ressourcenmanager-Dienst

infacmd rtm Befehlsprogramme

Um ein *infacmd rtm*-Befehlsprogramm auszuführen, muss der Benutzer eines der aufgelisteten Sets an Profil- und Domänenobjektberechtigungen des Modellrepository-Diensts besitzen.

Die nachstehende Tabelle führt die erforderlichen Berechtigungen für die *infacmd rtm* Befehlsprogramme auf:

infacmd rtm Befehlsprogramme	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
Deployimport	-	-	-
Exportieren	-	-	Lesen in Projekten, die Referenztabellen für den Export enthalten.
Importieren	-	-	Lesen und Schreiben in dem Projekt, in die die Referenztabellen importiert werden.

infacmd sch-Befehle

Um *infacmd sch*-Befehle ausführen zu können, muss der Benutzer eine der aufgelisteten Berechtigungen besitzen.

Die nachstehende Tabelle führt die erforderlichen Berechtigungen für die *infacmd sch*-Befehle auf:

infacmd sch-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
CreateSchedule	Scheduler-Berechtigungen	Zeitplan erstellen	Scheduler-Dienst
DeleteSchedule	Scheduler-Berechtigungen	Zeitplan löschen	Scheduler-Dienst
ListSchedule	Scheduler-Berechtigungen	Zeitpläne anzeigen	Scheduler-Dienst
ListServiceOptions	Domäneberechtigungen	Dienste verwalten	Scheduler-Dienst
ListServiceProcessOptions	Domäneberechtigungen	Dienste verwalten	Scheduler-Dienst
PauseAll	Scheduler-Berechtigungen	Zeitplan bearbeiten	Scheduler-Dienst
PauseSchedule	Scheduler-Berechtigungen	Zeitplan bearbeiten	Scheduler-Dienst
ResumeAll	Scheduler-Berechtigungen	Zeitplan bearbeiten	Scheduler-Dienst
ResumeSchedule	Scheduler-Berechtigungen	Zeitplan bearbeiten	Scheduler-Dienst
UpdateSchedule	Scheduler-Berechtigungen	Zeitplan bearbeiten	Scheduler-Dienst
UpdateService	Domäneberechtigungen	Dienste verwalten	Scheduler-Dienst

infacmd sch-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
UpdateServiceProcess	Domäneberechtigungen	Dienste verwalten	Scheduler-Dienst
Upgrade	Domäneberechtigungen	Dienste verwalten	Scheduler-Dienst

infacmd sql - Befehle

Um *infacmd sql*-Befehle ausführen zu können, müssen Benutzer über einen der aufgeführten Sätze an Domänenberechtigungen, Datenintegrationsdienst und Berechtigungen für Domänenobjekte verfügen.

Die folgende Tabelle listet die erforderlichen Berechtigungen für die *infacmd sql*-Befehle auf:

infacmd sql - Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
ExecuteSQL	-	-	Basierend auf Objekten, auf die Sie in Ihrer SQL-Anweisung zugreifen möchten
ListColumnPermissions	-	-	-
ListSQLDataServiceOptions	-	-	-
ListSQLDataServicePermissions	-	-	-
ListSQLDataServices	-	-	-
ListStoredProcedurePermissions	-	-	-
ListTableOptions	-	-	-
ListTablePermissions	-	-	-
PurgeTableCache	-	-	-
RefreshTableCache	-	-	-
RenameSQLDataService	Anwendungsadministration	Anwendungen verwalten	-
SetColumnPermissions	-	-	Gewähren für das Objekt
SetSQLDataServicePermissions	-	-	Gewähren für das Objekt
SetStoredProcedurePermissions	-	-	Gewähren für das Objekt

infacmd sql - Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung für
SetTablePermissions	-	-	Gewähren für das Objekt
StartSQLDataService	Anwendungsadministration	Anwendungen verwalten	-
StopSQLDataService	Anwendungsadministration	Anwendungen verwalten	-
UpdateColumnOptions	Anwendungsadministration	Anwendungen verwalten	-
UpdateSQLDataServiceOptions	Anwendungsadministration	Anwendungen verwalten	-
UpdateTableOptions	Anwendungsadministration	Anwendungen verwalten	-

infacmd wfs-Befehle

Zum Ausführen von infacmd wfs-Befehlen benötigen Benutzer keine Berechtigungen.

pmcmd-Befehle

Um *pmcmd*-Befehle auszuführen zu können, müssen Benutzer über die aufgeführten Sätze an Berechtigungen für PowerCenter-Repository-Dienst und PowerCenter Repository-Objekte verfügen.

Wenn der PowerCenter-Integrationsdienst im abgesicherten Modus läuft, müssen die Benutzer über die Administrator-Rolle für den zugehörige PowerCenter-Repository-Dienst verfügen, um folgende Befehle ausführen zu können:

- aborttask
- abortworkflow
- getrunningsessionsdetails
- getservicedetails
- getsessionstatistics
- gettaskdetails
- getworkflowdetails
- recoverworkflow
- scheduleworkflow
- starttask
- startworkflow

- stoptask
- stopworkflow
- unscheduleworkflow

Die folgende Tabelle listet die erforderlichen Berechtigungen für die *pmcmd*-Befehle auf:

pmcmd-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung
aborttask (vom eigenen Benutzerkonto gestartet)	-	-	Lesen und Ausführen des Ordners
aborttask (von anderen Benutzern gestartet)	Laufzeitobjekte	Ausführung verwalten	Lesen und Ausführen des Ordners
abortworkflow (vom eigenen Benutzerkonto gestartet)	-	-	Lesen und Ausführen des Ordners
abortworkflow (von anderen Benutzern gestartet)	Laufzeitobjekte	Ausführung verwalten	Lesen und Ausführen des Ordners
Verbinden	-	-	-
Trennen	-	-	-
Beenden	-	-	-
getrunningsessionsdetails	Laufzeitobjekte	Überwachen	-
getservicedetails	Laufzeitobjekte	Überwachen	Lesen in Ordner
getserviceproperties	-	-	-
getsessionstatistics	Laufzeitobjekte	Überwachen	Lesen in Ordner
gettaskdetails	Laufzeitobjekte	Überwachen	Lesen in Ordner
getworkflowdetails	Laufzeitobjekte	Überwachen	Lesen in Ordner
Hilfe	-	-	-
pingservice	-	-	-
recoverworkflow (vom eigenen Benutzerkonto gestartet)	Laufzeitobjekte	Ausführen	Lesen und Ausführen des Ordners Lesen und Ausführen in Verbindungsobjekten Berechtigung für Betriebssystemprofil (falls zutreffend)
recoverworkflow (von anderen Benutzern gestartet)	Laufzeitobjekte	Ausführung verwalten	Lesen und Ausführen des Ordners Lesen und Ausführen in Verbindungsobjekten Berechtigung für Betriebssystemprofil (falls zutreffend)

pmcmd-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung
scheduleworkflow	Laufzeitobjekte	Ausführung verwalten	Lesen und Ausführen des Ordners Lesen und Ausführen in Verbindungsobjekten Berechtigung für Betriebssystemprofil (falls zutreffend)
setfolder	-	-	Lesen in Ordner
setnowait	-	-	-
setwait	-	-	-
showsettings	-	-	-
starttask	Laufzeitobjekte	Ausführen	Lesen und Ausführen des Ordners Lesen und Ausführen in Verbindungsobjekten Berechtigung für Betriebssystemprofil (falls zutreffend)
startworkflow	Laufzeitobjekte	Ausführen	Lesen und Ausführen des Ordners Lesen und Ausführen in Verbindungsobjekten Berechtigung für Betriebssystemprofil (falls zutreffend)
stoptask (vom eigenen Benutzerkonto gestartet)	-	-	Lesen und Ausführen des Ordners
stoptask (von anderen Benutzern gestartet)	Laufzeitobjekte	Ausführung verwalten	Lesen und Ausführen des Ordners
stopworkflow (vom eigenen Benutzerkonto gestartet)	-	-	Lesen und Ausführen des Ordners
stopworkflow (von anderen Benutzern gestartet)	Laufzeitobjekte	Ausführung verwalten	Lesen und Ausführen des Ordners
unscheduleworkflow	Laufzeitobjekte	Ausführung verwalten	Lesen und Ausführen des Ordners
unsetfolder	-	-	Lesen in Ordner
Version	-	-	-
waittask	Laufzeitobjekte	Überwachen	Lesen in Ordner
waitworkflow	Laufzeitobjekte	Überwachen	Lesen in Ordner

pmrep Befehlsprogramme

Benutzer müssen über die Berechtigung "Repository Manager öffnen" verfüge, um *pmrep*-Befehle ausführen zu können, mit Ausnahme der folgenden Befehle:

- Ausführen
- Erstellen
- Wiederherstellen
- Upgrade
- Version
- Hilfe

Um *pmrep*-Befehle auszuführen zu können, müssen Benutzer über einen der aufgeführten Sätze an Domänenberechtigungen und Berechtigungen für PowerCenter-Repository-Dienst, Domänenberechtigungen und Berechtigungen für Model Repository-Objekte verfügen.

Benutzer müssen Objekteigentümer sein oder über die Administrator-Rolle für den PowerCenter-Repository-Dienst verfügen, um die folgenden Befehle ausführen zu können:

- AssignPermission
- ChangeOwner
- CreateQuery
- DeleteConnection
- DeleteDeploymentGroup
- DeleteFolder
- DeleteLabel
- DeleteQuery
- ModifyFolder (zum Ändern des Eigentümers, Konfigurieren von Berechtigungen, Freigeben des Ordners oder Bearbeiten von Ordernamen oder Beschreibungen)

Die folgende Tabelle listet die erforderlichen Berechtigungen für die *pmrep*-Befehle auf:

pmrep-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung
AddToDeploymentGroup	Globale Objekte	Bereitstellungsgruppe n verwalten	Lesen in ursprünglichem Ordner Lesen und Schreiben in Bereitstellungsgruppe
ApplyLabel	-	-	Lesen in Ordner Lesen und Ausführen in Beschriftung
AssignPermission	-	-	-
BackUp	Domänenverwaltung	Dienste verwalten	Berechtigung für PowerCenter-Repository-Dienst
ChangeOwner	-	-	-

pmrep-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung
CheckIn (für eigene Auscheck-Vorgänge)	Designobjekte	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner
CheckIn (für eigene Auscheck-Vorgänge)	Quellen und Ziele	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner
CheckIn (für eigene Auscheck-Vorgänge)	Laufzeitobjekte	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner
CheckIn (für Auscheck-Vorgänge Dritter)	Designobjekte	Versionen verwalten	Lesen und Schreiben in Ordner
CheckIn (für Auscheck-Vorgänge Dritter)	Quellen und Ziele	Versionen verwalten	Lesen und Schreiben in Ordner
CheckIn (für Auscheck-Vorgänge Dritter)	Laufzeitobjekte	Versionen verwalten	Lesen und Schreiben in Ordner
CleanUp	-	-	-
ClearDeploymentGroup	Globale Objekte	Bereitstellungsgruppen verwalten	Lesen und Schreiben in Bereitstellungsgruppe
Connect	-	-	-
Erstellen	Domänenverwaltung	Dienste verwalten	Berechtigung für PowerCenter-Repository-Dienst
CreateConnection	Globale Objekte	Verbindungen erstellen	-
CreateDeploymentGroup	Globale Objekte	Bereitstellungsgruppen verwalten	-
CreateFolder	Ordner	Erstellen	-
CreateLabel	Globale Objekte	Beschriftungen erstellen	-
CreateQuery	Globale Objekte	Anfragen erstellen	-
Delete	Domänenverwaltung	Dienste verwalten	Berechtigung für PowerCenter-Repository-Dienst
DeleteConnection	-	-	-
DeleteDeploymentGroup	-	-	-
DeleteFolder	-	-	-
DeleteLabel	-	-	-
DeleteObject	Designobjekte	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner

pmrep-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung
DeleteObject	Quellen und Ziele	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner
DeleteObject	Laufzeitobjekte	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner
DeleteQuery	-	-	-
DeployDeploymentGroup	Globale Objekte	Bereitstellungsgruppe n verwalten	Lesen in ursprünglichem Ordner Lesen und Schreiben in Zielordner Lesen und Schreiben in Bereitstellungsgruppe
DeployFolder	Ordner	Kopieren in ursprüngliches Repository Erstellen in Ziel-Repository	Lesen in Ordner
ExecuteQuery	-	-	Lesen und Ausführen in Abfragen
Exit	-	-	-
FindCheckout	-	-	Lesen in Ordner
GetConnectionDetails	-	-	In Verbindung lesen object
Hilfe	-	-	-
KillUserConnection	Domänenverwaltung	Dienste verwalten	Berechtigung für PowerCenter-Repository-Dienst
ListConnections	-	-	In Verbindung lesen object
ListObjectDependencies	-	-	Lesen in Ordner
ListObjects	-	-	Lesen in Ordner
ListTablesBySess	-	-	Lesen in Ordner
ListUserConnections	Domänenverwaltung	Dienste verwalten	Berechtigung für PowerCenter-Repository-Dienst
ModifyFolder (zum Ändern des Eigentümers, Konfigurieren von Berechtigungen, Freigeben des Ordners oder Bearbeiten von Ordernamen oder Beschreibungen)	-	-	-
ModifyFolder (zum Ändern des Status)	Ordner	Versionen verwalten	Lesen und Schreiben in Ordner

pmrep-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung
Benachrichtigen	Domänenverwaltung	Dienste verwalten	Berechtigung für PowerCenter-Repository-Dienst
ObjectExport	-	-	Lesen in Ordner
ObjectImport	Designobjekte	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner
ObjectImport	Quellen und Ziele	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner
ObjectImport	Laufzeitobjekte	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner
PurgeVersion	Designobjekte	Versionen verwalten	Lesen und Schreiben in Ordner Lesen, Schreiben und Ausführen von Abfragen, wenn Sie einen Abfragenamen angeben
PurgeVersion	Quellen und Ziele	Versionen verwalten	Lesen und Schreiben in Ordner Lesen, Schreiben und Ausführen von Abfragen, wenn Sie einen Abfragenamen angeben
PurgeVersion	Laufzeitobjekte	Versionen verwalten	Lesen und Schreiben in Ordner Lesen, Schreiben und Ausführen von Abfragen, wenn Sie einen Abfragenamen angeben
PurgeVersion (zum Löschen von Objekten auf Ordnebene)	Ordner	Versionen verwalten	Lesen und Schreiben in Ordner
PurgeVersion (zum Löschen von Objekten auf Repository-Ebene)	Domänenverwaltung	Dienste verwalten	Berechtigung für PowerCenter-Repository-Dienst
Register	Domänenverwaltung	Dienste verwalten	Berechtigung für PowerCenter-Repository-Dienst
RegisterPlugin	Domänenverwaltung	Dienste verwalten	Berechtigung für PowerCenter-Repository-Dienst
Wiederherstellen	Domänenverwaltung	Dienste verwalten	Berechtigung für PowerCenter-Repository-Dienst
RollbackDeployment	Globale Objekte	Bereitstellungsgruppen verwalten	Lesen und Schreiben in Zielordner
Ausführen	-	-	-
ShowConnectionInfo	-	-	-

pmrep-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung
SwitchConnection	Laufzeitobjekte	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner Lesen in Verbindungsobjekten
TruncateLog	Laufzeitobjekte	Ausführung verwalten	Lesen und Ausführen des Ordners
UndoCheckout (für eigene Auscheck-Vorgänge)	Designobjekte	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner
UndoCheckout (für eigene Auscheck-Vorgänge)	Quellen und Ziele	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner
UndoCheckout (für eigene Auscheck-Vorgänge)	Laufzeitobjekte	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner
UndoCheckout (für Auscheck-Vorgänge Dritter)	Designobjekte	Versionen verwalten	Lesen und Schreiben in Ordner
UndoCheckout (für Auscheck-Vorgänge Dritter)	Quellen und Ziele	Versionen verwalten	Lesen und Schreiben in Ordner
UndoCheckout (für Auscheck-Vorgänge Dritter)	Laufzeitobjekte	Versionen verwalten	Lesen und Schreiben in Ordner
Unregister	Domänenverwaltung	Dienste verwalten	Berechtigung für PowerCenter-Repository-Dienst
UnregisterPlugin	Domänenverwaltung	Dienste verwalten	Berechtigung für PowerCenter-Repository-Dienst
UpdateConnection	-	-	Lesen und Schreiben in Verbindungsobjekten
UpdateEmailAddr	Laufzeitobjekte	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner
UpdateSeqGenVals	Designobjekte	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner
UpdateSrcPrefix	Laufzeitobjekte	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner
UpdateStatistics	Domänenverwaltung	Dienste verwalten	Berechtigung für PowerCenter-Repository-Dienst
UpdateTargPrefix	Laufzeitobjekte	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner
Upgrade	Domänenverwaltung	Dienste verwalten	Berechtigung für PowerCenter-Repository-Dienst
Validate	Designobjekte	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner

pmrep-Befehl	Berechtigungsgruppe	Name der Berechtigung	Berechtigung
Validate	Laufzeitobjekte	Erstellen, Bearbeiten und Löschen	Lesen und Schreiben in Ordner
Version	-	-	-

ANHANG B

Benutzerdefinierte Rollen

Dieser Anhang umfasst die folgenden Themen:

- [Benutzerdefinierte Rolle für den Analyst-Dienst, 256](#)
- [Benutzerdefinierte Rollen für den Metadata Manager-Dienst, 257](#)
- [Benutzerdefinierte Rolle für den Operator, 259](#)
- [PowerCenter-Repository-Dienst - Benutzerdefinierte Rollen, 260](#)
- [Benutzerdefinierte Rollen für den Test Data Manager, 261](#)

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 Arbeitsbereich	Arbeitsbereich „Glossar“

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“.

Metadata Manager – Erweiterter Benutzer

Die folgende Tabelle enthält die die Standardberechtigungen, die der benutzerdefinierten Rolle "Metadata Manager - Erweiterter Benutzer" zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Katalog	<ul style="list-style-type: none">- 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	<ul style="list-style-type: none">- Ressource anzeigen- Ressource laden- Zeitpläne verwalten- Metadaten bereinigen- Ressource verwalten
Modell	<ul style="list-style-type: none">- Modell anzeigen- Modell verwalten- Modelle exportieren/importieren
Sicherheit	Katalogberechtigungen verwalten

Metadata Manager – Standardbenutzer

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Metadata Manager – Standardbenutzer“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Katalog	<ul style="list-style-type: none">- Herkunft anzeigen- Zugehörige Kataloge anzeigen- Katalog anzeigen- Beziehungen anzeigen- Kommentare anzeigen- Links anzeigen
Modell	Modell anzeigen

Metadata Manager – Fortgeschrittener Benutzer

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Metadata Manager – Fortgeschrittener Benutzer“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Katalog	<ul style="list-style-type: none">- 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	<ul style="list-style-type: none">- Ressource anzeigen- Ressource laden
Modell	Modell anzeigen

Benutzerdefinierte Rolle für den Operator

Die benutzerdefinierte Rolle für den Operator umfasst Berechtigungen für die Verwaltung, Planung und Überwachung von Anwendungsdiensten.

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Operator“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Anwendungsadministration	Anwendungen verwalten
Domänen-Administration	Dienstausführung verwalten
Verwaltung des Modellrepository-Diensts	Verwalten von teambasierter Entwicklung
Überwachen	<p>Die Überwachen-Berechtigungsgruppe enthält die folgenden Berechtigungen:</p> <ul style="list-style-type: none">- Ansicht: Jobs von anderen Benutzern anzeigen- Ansicht: Statistiken anzeigen- Ansicht: Berichte anzeigen- Zugriffsüberwachung: Zugriff über Analyst Tool- Zugriffsüberwachung: Zugriff über Developer Tool- Zugriffsüberwachung: Zugriff über Administrator Tool- Aktionen für Jobs durchführen <p>Hinweis: In einer Domäne, die die Kerberos-Authentifizierung verwendet, müssen Benutzer auch über die Administratorrolle für den Modellrepository-Dienst verfügen, der für die Überwachung konfiguriert wurde.</p>
Scheduler	<p>Die Scheduler-Berechtigungsgruppe enthält die folgenden Berechtigungen:</p> <ul style="list-style-type: none">- Geplante Jobs verwalten: Zeitplan erstellen- Geplante Jobs verwalten: Zeitplan löschen- Geplante Jobs verwalten: Zeitplan bearbeiten- Geplante Jobs verwalten: Zeitpläne anzeigen
Tools	Zugriff auf Informatica Administrator

PowerCenter-Repository-Dienst - Benutzerdefinierte Rollen

Die benutzerdefinierten Rollen des PowerCenter-Repository-Diensts umfassen den PowerCenter-Verbindungsadministrator, PowerCenter-Entwickler, PowerCenter-Operator und PowerCenter-Repository-Ordneradministrator.

PowerCenter – Verbindungsadministrator

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

PowerCenter – Entwickler

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „PowerCenter – Entwickler“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Tools	<ul style="list-style-type: none">- Designer öffnen- Workflow Manager öffnen- Workflow Monitor öffnen
Designobjekte	<ul style="list-style-type: none">- Erstellen, Bearbeiten und Löschen- Versionen verwalten
Quellen und Ziele	<ul style="list-style-type: none">- Erstellen, Bearbeiten und Löschen- Versionen verwalten
Laufzeitobjekte	<ul style="list-style-type: none">- Erstellen, Bearbeiten und Löschen- Ausführen- Versionen verwalten- Überwachen

PowerCenter – Operator

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „PowerCenter – Operator“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Tools	Workflow Monitor öffnen
Laufzeitobjekte	<ul style="list-style-type: none">- Ausführen- Ausführung verwalten- Überwachen

PowerCenter-Repository-Ordneradministrator

Die folgende Tabelle enthält die die Standardberechtigungen, die der benutzerdefinierten Rolle "PowerCenter - Repository-Ordneradministrator" zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Tools	Repository Manager öffnen
Ordner	<ul style="list-style-type: none">- Kopieren- Erstellen- Versionen verwalten
Globale Objekte	<ul style="list-style-type: none">- Bereitstellungsgruppen verwalten- Bereitstellungsgruppen werden ausgeführt- Beschriftungen erstellen- Berechtigung zum Erstellen von Anfragen

Benutzerdefinierte Rollen für den Test Data Manager

Zu den benutzerdefinierten Rollen des Test Data Manager gehören der Testdaten-Administrator, Testdatenentwickler, Testdaten-Projekt-DBA, Testdaten-Projektentwickler, Testdaten-Projekteigentümer, Testdaten-Risikomanager und Test-Techniker.

Testdaten-Administrator

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Testdaten-Administrator“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Projekte	Projekt prüfen
Verwaltung	<ul style="list-style-type: none">- Verbindungen anzeigen- Verbindungen verwalten- Einstellungen verwalten

Testdatenentwickler

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Testdaten-Entwickler“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Richtlinien	<ul style="list-style-type: none">- Richtlinien anzeigen- Richtlinien verwalten
Datendomänen	<ul style="list-style-type: none">- Datendomänen anzeigen- Datendomänen verwalten
Projekte	Projekt prüfen

Testdaten-Projekt-DBA

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Testdaten-Projekt-DBA“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Projekte	<ul style="list-style-type: none">- Projekt anzeigen- Projekt ausführen- Projekt überwachen- Projekt prüfen
Verwaltung	<ul style="list-style-type: none">- Verbindungen anzeigen- Verbindungen verwalten

Testdaten-Projektentwickler

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Testdaten-Projektentwickler“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Richtlinien	Richtlinien anzeigen
Datendomänen	Datendomänen anzeigen
Projekte	<ul style="list-style-type: none">- Projekt anzeigen- Projekt ermitteln- Projekt ausführen- Projekt überwachen- Projekt prüfen- Metadaten importieren
Datenmaskierung	<ul style="list-style-type: none">- Datenmaskierung anzeigen- Datenmaskierung verwalten

Berechtigungsgruppe	Name der Berechtigung
Datenteilmenge	<ul style="list-style-type: none"> - Datenteilmenge anzeigen - Datenteilmenge verwalten
Verwaltung	<ul style="list-style-type: none"> - Verbindungen anzeigen - Verbindungen verwalten

Testdaten-Projekteigentümer

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Testdaten-Projekteigentümer“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Richtlinien	Richtlinien anzeigen
Datendomänen	Datendomänen anzeigen
Projekte	<ul style="list-style-type: none"> - Projekt anzeigen - Projekt verwalten - Projekt ermitteln - Projekt ausführen - Projekt überwachen - Projekt prüfen - Metadaten importieren
Datenmaskierung	<ul style="list-style-type: none"> - Datenmaskierung anzeigen - Datenmaskierung verwalten
Datenteilmenge	<ul style="list-style-type: none"> - Datenteilmenge anzeigen - Datenteilmenge verwalten
Verwaltung	<ul style="list-style-type: none"> - Verbindungen anzeigen - Verbindungen verwalten

Testdaten-Risikomanager

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Testdaten-Risikomanager“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Richtlinien	Richtlinien anzeigen
Datendomänen	Datendomänen anzeigen
Projekte	Projekt prüfen

Testdaten-Spezialist

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Testdaten-Spezialist“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Richtlinien	Richtlinien anzeigen
Datendomänen	<ul style="list-style-type: none">- Datendomänen anzeigen- Datendomänen verwalten
Projekte	<ul style="list-style-type: none">- Projekt anzeigen- Projekt verwalten- Projekt ermitteln- Projekt ausführen- Projekt überwachen- Projekt prüfen- Metadaten importieren
Datenmaskierung	<ul style="list-style-type: none">- Datenmaskierung anzeigen- Datenmaskierung verwalten
Datenteilmenge	<ul style="list-style-type: none">- Datenteilmenge anzeigen- Datenteilmenge verwalten
Verwaltung	<ul style="list-style-type: none">- Verbindungen anzeigen- Verbindungen verwalten

Test-Techniker

Die folgende Tabelle enthält die Standardberechtigungen, die der benutzerdefinierten Rolle „Test-Techniker“ zugewiesen sind:

Berechtigungsgruppe	Name der Berechtigung
Projekte	<ul style="list-style-type: none">- Projekt anzeigen- Projekt überwachen

INDEX

A

- Administrator
 - Rolle [189](#)
- Administratoren
 - Anwendungs-Client [127](#)
 - Domäne [126](#)
 - Standard [126](#)
- Analyst-Dienst
 - benutzerdefinierte Rollen [256](#)
 - Berechtigungen [160](#)
- ändern
 - Passwort für Benutzerkonto [122](#)
- Anmeldeaktivität
 - Anzeigen [133](#)
- Anwendung
 - Berechtigungen [207](#)
- Anwendungsdienste
 - Autorisierung [116](#)
 - Benutzersynchronisation [116](#)
 - Berechtigungen [199](#)
- Arbeitsablauf
 - Berechtigungen [207](#)
 - Geerbte Berechtigungen [207](#)
- as
 - Berechtigungen per Befehl [224](#)
- Auditberichte
 - Beschreibung [217](#)
 - für Benutzer [221](#), [222](#)
 - für Gruppen [222](#)
 - Übersicht [121](#)
- Authentifizierung
 - Kerberos [21](#)
 - LDAP [21](#), [27](#), [116](#)
 - Nativ [20](#), [116](#)
 - Service Manager [116](#)
- Autorisierung
 - Anwendungsdienste [116](#)
 - Datenintegrationsdienst [116](#)
 - Metadata Manager-Dienst [116](#)
 - Modellrepository-Dienst [116](#)
 - PowerCenter-Repository-Dienst [116](#)
 - Service Manager [116](#)

B

- Befehlszeilenprogramme
 - Berechtigungen [224](#)
- Benutzer
 - Berechtigungen, zuweisen [192](#)
 - Gruppen zuweisen [129](#)
 - gültiger Name [128](#)
 - Rollen, zuweisen [192](#)
 - Synchronisation [116](#)
 - Systemspeicher [132](#)

- Benutzer (*Fortsetzung*)
 - Übersicht [119](#)
 - Ungültige Zeichen [128](#)
 - verwalten [128](#)
 - Vielzahl von [132](#)
- Benutzeraktivitätsprotokolle
 - Aktivitätscodes [134](#)
 - Ausgabeformate [133](#)
 - convertUserActivityLog [133](#)
 - getUserActivityLog [133](#)
- Benutzerbeschreibung
 - Ungültige Zeichen [128](#)
- benutzerdefinierte Rollen
 - Analyst-Dienst [256](#)
 - Operator [259](#)
- Benutzerdefinierte Rollen
 - bearbeiten [191](#)
 - Benutzern und Gruppen zuweisen [192](#)
 - Berechtigungen, zuweisen [191](#)
 - Beschreibung [189](#), [190](#)
 - erstellen [191](#)
 - löschen [192](#)
 - Metadata Manager-Dienst [257](#)
 - PowerCenter-Repository-Dienst [260](#)
- Benutzerkonten
 - aktivieren [130](#)
 - Ändern des Passworts [122](#)
 - beim Installieren erstellte [126](#)
 - Standard [126](#)
 - Übersicht [126](#)
- Benutzersicherheit
 - Beschreibung [115](#)
- Berechtigungen
 - Aktiv [198](#)
 - Analyst-Dienst [160](#)
 - Anwendung [207](#)
 - Anwendungsdienste [199](#)
 - Arbeiten mit Berechtigungen [197](#)
 - Arbeitsablauf [207](#)
 - as Befehle [224](#)
 - Befehlszeilenprogramme [224](#)
 - Beschreibung [150](#), [197](#)
 - Betriebssystemprofile [199](#), [202](#)
 - Cluster-Befehle [225](#)
 - Content-Management-Dienst [162](#)
 - Datenintegrationsdienst [162](#)
 - Designobjekte [172](#)
 - Direkt [198](#)
 - dis-Befehle [226](#)
 - Domäne [152](#)
 - Domänen-Tools [159](#)
 - Domänenobjekte [199](#)
 - Domänenverwaltung [153](#)
 - es-Befehle [228](#)
 - Fehlerbehebung [194](#)
 - Geerbt [198](#)

Berechtigungen (Fortsetzung)

- geerbte [193](#)
- Gitter [199](#)
- globale PowerCenter-Objekte [180](#)
- Informatica Cloud-Verwaltung [160](#)
- ipc Befehle [228](#)
- isp Befehle [228](#)
- Knoten [199](#)
- Laufzeitobjekte [176](#)
- Lizenzen [199](#)
- Mapping [207](#)
- mas-Befehle [238](#)
- Metadata Manager Service [163](#)
- Modellrepository-Dienst [168](#)
- MRS-Befehle [239](#)
- ms Befehle [241](#)
- Ordner [170, 199](#)
- pmcmd-Befehle [247](#)
- pmrep-Befehle [250](#)
- PowerCenter Repository Service [169](#)
- PowerCenter Repository Service-Tools [170](#)
- PowerExchange Listener Service [183](#)
- PowerExchange Logger Service [183](#)
- ps Befehl [242](#)
- pwx - Befehle [243](#)
- Quellen [174](#)
- rms-Befehle [244](#)
- rtm Befehlsprogramme [245](#)
- sch-Befehle [245](#)
- Scheduler-Dienst [184](#)
- Sicherheits-Administration [152](#)
- sql-Befehle [246](#)
- SQL-Datendienst [209](#)
- Suchfilter [199](#)
- Targets [174](#)
- tools-Befehle [242](#)
- Typen [198](#)
- Überwachen [158](#)
- Verbindungen [204](#)
- Virtuelle gespeicherte Prozedur [209](#)
- Virtuelle Tabelle [209](#)
- Virtuelles Schema [209](#)
- Web-Dienst [213](#)
- Web-Dienst-Operation [213](#)
- wfs-Befehle [247](#)
- zuweisen [192](#)
- Berechtigungsgruppe „Cloud-Verwaltung“
 - Domäne [160](#)
- Berechtigungsgruppe „Domänenverwaltung“
 - Beschreibung [153](#)
- Berechtigungsgruppe „Laden“
 - Beschreibung [166](#)
- Berechtigungsgruppe durchsuchen
 - Beschreibung [164](#)
- Berechtigungsgruppe für globale Objekte
 - Beschreibung [180](#)
- Berechtigungsgruppe Sicherheitsverwaltung
 - Beschreibung [152](#)
- Berechtigungsgruppen
 - Beschreibung [151](#)
 - Designobjekte [172](#)
 - Domänenverwaltung [153](#)
 - durchsuchen [164](#)
 - Globale Objekte [180](#)
 - Informatica Cloud-Verwaltung [160](#)
 - Laden [166](#)
 - Laufzeitobjekte [176](#)
 - Modell [167](#)

Berechtigungsgruppen (Fortsetzung)

- Ordner [170](#)
- Quellen und Targets [174](#)
- Sicherheit [167](#)
- Sicherheits-Administration [152](#)
- Tools [159, 170](#)
- Überwachen [158](#)
- Bereitstellungsgruppen
 - Berechtigungen für PowerCenter [180](#)
- Beschriftungen
 - Berechtigungen für PowerCenter [180](#)
- Betriebssystemprofil
 - bearbeiten [139](#)
 - Eigenschaften, Datenintegrationsdienst [139, 141](#)
 - Eigenschaften, Metadaten-Zugriffsdienst [143](#)
 - Eigenschaften, PowerCenter-Integrationsdienst [139](#)
 - Erstellen [143](#)
 - löschen [146](#)
 - Standard [145](#)
- Betriebssystemprofile
 - Berechtigungen [199, 202](#)
 - Übersicht [120](#)

C

- Cacerts, Truststore-Datei [32](#)
- Chiffre-Suites
 - Konfigurieren [100](#)
- Client-Konfiguration
 - sichere Domäne [90](#)
- Cluster
 - Berechtigungen nach Befehl [225](#)
 - Rechte nach Befehl [225](#)
- Content-Management-Dienst
 - Berechtigungen [162](#)
- convertUserActivityLog
 - Benutzeraktivitätsprotokolle [133](#)

D

- Datenintegrationsdienst
 - Autorisierung [116](#)
 - Berechtigungen [162](#)
- Designobjekt-Berechtigungsgruppe
 - Beschreibung [172](#)
- Designobjekte
 - Berechtigungen [172](#)
 - Beschreibung [172](#)
- Dienstmanager
 - Single Sign-On [116](#)
- Direkte Berechtigung
 - Beschreibung [198](#)
- dis
 - Berechtigungen nach Befehl [226](#)
 - Rechte nach Befehl [226](#)
- Domäne
 - Administrationsberechtigungen [153](#)
 - Administrator [126](#)
 - Administratorrolle [189](#)
 - Benutzer mit Berechtigungen [194](#)
 - Benutzersicherheit [123](#)
 - Benutzersynchronisation [116](#)
 - Berechtigungen [152](#)
 - Sicherheitsverwaltungsberechtigungen [152](#)
- Domänenadministrator
 - Beschreibung [126](#)

Domänenberechtigungen
Aktiv [198](#)
Direkt [198](#)
Geerbt [198](#)
Domänenobjekte
Berechtigungen [199](#)

E

Effektive Berechtigung
Beschreibung [198](#)
es
Berechtigungen nach Befehl [228](#)
Rechte nach Befehl [228](#)

F

Filter
getUserActivityLog [134](#)

G

Geerbte Berechtigung
Beschreibung [198](#)
geerbte Berechtigungen
Beschreibung [193](#)
getUserActivityLog
Benutzeraktivitätsprotokolle [133](#)
Filter [134](#)
Gitter
Berechtigungen [199](#)
globale Objekte
Berechtigungen für PowerCenter [180](#)
Gruppe "Jeder"
Beschreibung [125](#)
Gruppen
Berechtigungen, zuweisen [192](#)
gültiger Name [137](#)
Rollen, zuweisen [192](#)
Standard "Jeder" [125](#)
Synchronisation [116](#)
übergeordnete Gruppe [137](#)
Übersicht [118](#)
Ungültige Zeichen [137](#)
verwalten [137](#)
Gruppenbeschreibung
Ungültige Zeichen [137](#)
gültiger Name
Benutzerkonto [128](#)
Gruppen [137](#)

I

Identitäts-Provider
Für Single Sign-On konfigurieren [73](#)
Informatica Administrator
Navigator [118](#)
Registerkarten, anzeigen [114](#)
Sicherheitsseite [117](#)
Suche wird ausgeführt [117](#)
Übersicht [114](#)
Informatica Analyst
Administrator [127](#)

Informatica Developer
Administrator [127](#)
Informatica-Domäne
Benutzer, verwalten [128](#)
Benutzersicherheit [123](#)
Berechtigungen [123](#)
ipc
Berechtigungen nach Befehl [228](#)
Rechte nach Befehl [228](#)
isp
Berechtigungen nach Befehl [228](#)
Rechte nach Befehl [228](#)

K

Kerberos-Authentifizierung
Bereichsübergreifende Authentifizierung [37](#)
Beschreibung [21](#)
Dienstprinzipalkonten [43](#)
Dienstprinzipalname [44](#)
keytab [44](#)
Knotenebene [39](#)
LDAP-Synchronisierung [61](#)
Prozessebene [39](#)
SPN-Keytab-Formatdatei [48](#)
Übersicht [34, 35](#)
Keytool-Dienstprogramm [32](#)
Knoten
Berechtigungen [199](#)
Konten
Ändern des Passworts [122](#)
Kontoverwaltung
Übersicht [120](#)

L

Laufzeitobjekte
Berechtigungen [176](#)
Beschreibung [176](#)
Laufzeitobjekte-Berechtigungsgruppe
Beschreibung [176](#)
LDAP-Authentifizierung
Azure Active Directory [26](#)
Beschreibung [21, 116](#)
einrichten [27](#)
Selbstsigniertes SSL-Zertifikat [32](#)
Unterstützte Verzeichnisdienste [25](#)
verschachtelte Gruppen [32](#)
Verzeichnisdienste [27](#)
LDAP-Benutzer
aktivieren [130](#)
Importieren [27](#)
verwalten [128](#)
zu Gruppen zuweisen [130](#)
LDAP-Gruppen
Importieren [27](#)
verwalten [137](#)
LDAP-Konfigurationen
Löschen [33](#)
LDAP-Sicherheitsdomäne
Beschreibung [21](#)
LDAP-Verzeichnisdienst
verschachtelte Gruppen [32](#)
Lizenzen
Berechtigungen [199](#)

M

- Mapping
 - Berechtigungen [207](#)
 - Geerbte Berechtigungen [207](#)
- mas
 - Berechtigungen nach Befehl [238](#)
 - Rechte nach Befehl [238](#)
- Metadata Manager
 - Administrator [127](#)
- Metadata Manager Service
 - Berechtigungen [163](#)
- Metadata Manager-Dienst
 - Autorisierung [116](#)
 - Benutzer mit Berechtigungen [194](#)
 - Benutzerdefinierte Rollen [257](#)
 - Benutzersynchronisation [116](#)
- Metadata Manager-Dienst-Berechtigungen
 - Berechtigungsgruppe „Laden“ [166](#)
 - Berechtigungsgruppe durchsuchen [164](#)
 - Modell-Berechtigungsgruppe [167](#)
 - Sicherheitsberechtigungsgruppe [167](#)
- Metadaten von Referenztabelle bearbeiten
 - Berechtigung [162](#)
- Modell-Berechtigungsgruppe
 - Beschreibung [167](#)
- Modellrepository-Dienst
 - Autorisierung [116](#)
 - Benutzer mit Berechtigungen [194](#)
 - Benutzersynchronisation [116](#)
 - Berechtigungen [168](#)
- MRS
 - Berechtigungen nach Befehl [239](#)
 - Rechte nach Befehl [239](#)
- ms
 - Berechtigungen nach Befehl [241](#)
 - Rechte nach Befehl [241](#)

N

- native Authentifizierung
 - Beschreibung [20](#)
- Native Authentifizierung
 - Beschreibung [116](#)
- Native Benutzer
 - aktivieren [130](#)
 - bearbeiten [129](#)
 - Gruppen zuweisen [129](#)
 - hinzufügen [128](#)
 - löschen [131](#)
 - Passwörter [128](#)
 - verwalten [128](#)
- native Gruppen
 - bearbeiten [137](#)
 - Benutzer, zuordnen [129](#)
 - hinzufügen [137](#)
 - in eine andere Gruppe verschieben [138](#)
 - löschen [138](#)
 - verwalten [137](#)
- Native Sicherheitsdomäne
 - Beschreibung [20](#)
- Navigator
 - Sicherheitsseite [118](#)

O

- Objektanfragen
 - Berechtigungen für PowerCenter [180](#)
- operating system profile
 - managing [138](#)
- Operator}
 - benutzerdefinierte Rollen [259](#)
- Ordner
 - Berechtigungen [170](#), [199](#)
- Ordnerberechtigungsgruppe
 - Beschreibung [170](#)

P

- Passwort
 - Ändern für ein Benutzerkonto [122](#)
- Passwörter
 - Ändern für Standardadministrator [126](#)
 - Anforderungen [128](#)
 - Native Benutzer [128](#)
- pmcmd
 - Berechtigungen nach Befehl [247](#)
 - Berechtigungen per Befehl [247](#)
- pmrep
 - Berechtigungen nach Befehl [250](#)
 - Rechte nach Befehl [250](#)
- PowerCenter Client
 - Administrator [127](#)
- PowerCenter Repository Service
 - Berechtigungen [169](#)
- PowerCenter Sicherheit
 - verwalten [117](#)
- PowerCenter-Repository-Dienst
 - Administratorrolle [189](#)
 - Autorisierung [116](#)
 - Benutzer mit Berechtigungen [194](#)
 - Benutzerdefinierte Rollen [260](#)
 - Benutzersynchronisation [116](#)
- PowerExchange Listener Service
 - Berechtigungen [183](#)
- PowerExchange Logger Service
 - Berechtigungen [183](#)
- ps
 - Berechtigungen per Befehl [242](#)
- pxw
 - Berechtigungen nach Befehl [243](#)

Q

- Quell- und Target-Berechtigungsgruppe
 - Beschreibung [174](#)
- Quellen
 - Berechtigungen [174](#)

R

- Referenztabelle erstellen
 - Berechtigung [162](#)
- rms
 - Berechtigungen nach Befehl [244](#)
 - Rechte nach Befehl [244](#)
- Rollen
 - Administrator [189](#)
 - benutzerdefiniert [190](#)

Rollen (Fortsetzung)

- Beschreibung [152](#)
- Fehlerbehebung [194](#)
- Übersicht [119](#)
- verwalten [189](#)
- zuweisen [192](#)

rtm

- Berechtigungen per Befehl [245](#)

S

sch

- Berechtigungen nach Befehl [245](#)
- Rechte nach Befehl [245](#)

Scheduler-Dienst

- Berechtigungen [184](#)

Security Assertion Markup Language (SAML)

- Anforderungssignierung [75](#), [76](#)
- Assertion, signiert oder verschlüsselt [75](#)
- auf Gateway-Knoten aktivieren [74](#)
- in Domäne aktivieren [74](#)
- signierte Antwort [75](#), [77](#)
- Unterstützung für [69](#)
- verschlüsselte Assertion [77](#)

Service Manager

- Authentifizierung [116](#)
- Autorisierung [116](#)

sichere Domäne

- Client-Konfiguration [90](#)

Sicherheit

- Berechtigungen [123](#), [150](#), [152](#)
- Passwörter [128](#)
- Rollen [152](#)

Sicherheit auf Spaltenlevel

- Einschränken von Spalten [212](#)

Sicherheitsberechtigungsgruppe

- Beschreibung [167](#)

Sicherheitsdomäne

- Nativ [20](#)

Sicherheitsdomänen

- LDAP [21](#)
- Löschen einer LDAP [33](#)

Sicherheitsseite

- Informatica Administrator [117](#)
- Navigator [118](#)

single sign-on

- Übersicht [69](#)

Single Sign-On

- Beschreibung [116](#)
- Konfigurieren [72](#)

sql

- Berechtigungen nach Befehl [246](#)
- Berechtigungen per Befehl [246](#)

SQL-Datendienst

- Berechtigungen [209](#)
- Berechtigungstypen [209](#)
- Geerbte Berechtigungen [209](#)

SSL-Zertifikat

- LDAP-Authentifizierung [32](#)

Standardadministrator

- ändern [126](#)
- Beschreibung [126](#)
- Passwörter, ändern [126](#)

Suchbereich

- Informatica Administrator [117](#)

Suchfilter

- Berechtigungen [199](#)

Synchronisation

- Benutzer [116](#)
- LDAP-Benutzer [27](#)

Systemdefinierte Rollen

- Administrator [189](#)
- Benutzern und Gruppen zuweisen [192](#)
- Beschreibung [189](#)

Systemspeicher

- Vergrößern [132](#)

T

Targets

- Berechtigungen [174](#)

Test Data Manager

- Administrator [127](#)

Tools

- Berechtigungen nach Befehl [242](#)
- Rechte nach Befehl [242](#)

Tools-Berechtigungsgruppe

- Domäne [159](#)
- PowerCenter-Repository-Dienst [170](#)

U

übergeordnete Gruppen

- Beschreibung [137](#)

Überwachen-Berechtigungsgruppe

- Domäne [158](#)

Umgebungsvariablen

- INFA_TRUSTSTORE [90](#)
- INFA_TRUSTSTORE_PASSWORD [90](#)

UpdateColumnOptions

- Ersetzen von Spaltenwerten [212](#)

V

Verbindungen

- Berechtigungen [204](#)
- Berechtigungstypen [204](#)
- Standardberechtigungen [204](#)

Verbindungsobjekte

- Berechtigungen für PowerCenter [180](#)

verschachtelte Gruppen

- LDAP-Authentifizierung [32](#)
- LDAP-Verzeichnisdienst [32](#)

Virtuelle gespeicherte Prozedur

- Berechtigungen [209](#)
- Geerbte Berechtigungen [209](#)

Virtuelle Tabelle

- Berechtigungen [209](#)
- Geerbte Berechtigungen [209](#)

Virtuelles Schema

- Berechtigungen [209](#)
- Geerbte Berechtigungen [209](#)

W

Web Dienst

- Berechtigungstypen [214](#)

Web-Dienst

- Berechtigungen [213](#)

Web-Dienst-Operation

- Berechtigungen [213](#)

Webdienstressource
Berechtigungen [213](#)

wfs
Berechtigungen per Befehl [247](#)