



Informatica®
10.5.9

Administratorhandbuch

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

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

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

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

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

Informatica-Produkte unterliegen einer Gewährleistung gemäß den Geschäftsbedingungen der Vereinbarungen, unter denen sie bereitgestellt werden. INFORMATICA STELLT DIE INFORMATIONEN IN DIESEM DOKUMENT OHNE MÄNGELGEWÄHR UND OHNE AUSDRÜCKLICHE ODER STILLSCHWEIGENDE GEWÄHRLEISTUNG JEDLICHER 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.

Inhalt

Einleitung	15
Informatica-Ressourcen.	15
Informatica Network.	15
Informatica-Wissensdatenbank.	15
Informatica-Dokumentation.	16
Informatica-Produktverfügbarkeitsmatrizen.	16
Informatica Velocity.	16
Informatica Marketplace.	16
Informatica – Weltweiter Kundensupport.	16
 Kapitel 1: Grundlagen zu den Domänen.....	 17
Grundlagen zu den Domänen - Übersicht.	17
Knoten.	18
Dienstmanager.	19
Anwendungsdienste.	20
Analyst-Dienst.	21
Content-Managementdienst.	22
Data Integration Service.	23
E-Mail-Dienst.	23
Metadaten-Zugriffsdienst.	23
Metadata Manager Service.	24
Modellrepository-Dienst.	24
PowerCenter Integration Service.	24
PowerCenter-Repository-Dienst.	25
PowerExchange Listener Service.	25
PowerExchange Logger Service.	25
Ressourcenmanager-Dienst.	25
SAP BW Service.	26
Scheduler-Dienst.	26
Web Services Hub.	26
Hohe Verfügbarkeit.	26
Informatica-Datennutzungsrichtlinie.	26
Konfigurieren der Informatica-DiscoveryIQ Proxy-Details.	27
Deaktivieren der Informatica-Datennutzung.	27
 Kapitel 2: Eigenes Konto verwalten.....	 28
Eigenes Konto verwalten - Übersicht.	28
Passwortverwaltung.	28
Ändern Ihres Passwortes..	29
Einstellungen.	29

Informatica Network-Anmeldedaten.	30
Informatica Network-Anmeldedaten eingeben.	30
Suchen der Informatica-Wissensdatenbank.	30
Kapitel 3: Informatica Administrator.	31
Verwenden von Informatica Administrator - Übersicht.	31
Anmelden beim Informatica Administrator.	32
Informatica Administrator-URL.	33
Fehlerbehebung bei der Anmeldung bei Informatica Administrator.	33
Registerkarte „Verwalten“.	33
Registerkarte „Verwalten“ - Ansicht „Domäne“.	34
Detailbereich.	36
Ressourcennutzungsanzeigen.	37
Registerkarte „Verwalten“ - Ansicht „Dienste und Knoten“.	38
Navigatorsuche.	39
Domäne.	40
Ordner.	41
Anwendungsdienste.	41
Systemdienste.	45
Knoten.	47
Gitter.	47
Lizenzen.	47
Registerkarte „Verwalten“ – Verbindungsansicht.	48
Registerkarte „Verwalten“ - Ansicht „Pläne“.	49
Registerkarte „Überwachen“.	49
Registerkarte „Überwachen“ - Ansicht „Übersichtsstatistik“.	51
Registerkarte „Überwachen“ - Ansicht „Ausführungsstatistiken“.	52
Ansichten in der Ansicht „Ausführungsstatistiken“.	53
Statistiken in der Ansicht „Ausführungsstatistiken“.	55
Berichte in der Ansicht „Ausführungsstatistiken“.	55
Ansicht „Übersichtsstatistik“.	58
Ansicht „Detaillierte Statistiken“.	58
Registerkarte "Protokolle".	59
Registerkarte Berichte.	59
Registerkarte Sicherheit.	60
Der Suchbereich.	60
Der Sicherheits-Navigator.	60
Gruppen.	61
Benutzer.	61
Rollen.	62
Betriebssystemprofile.	62
LDAP-Konfiguration.	63
Kontoverwaltung.	63

Auditberichte.	63
Dienststatus.	64
Prozessstatus.	64
Jobstatus.	66
Barrierefreiheit von Informatica Administrator - Übersicht.	67
Tastenkombinationen.	67
Kapitel 4: Verwenden der Domänenansicht.	69
Über die Ansicht „Domäne“.	69
Abhängigkeitsgrafik.	70
Anzeigen von Abhängigkeiten für Anwendungsdienste, Knoten und Gitter	70
Wiederherstellen bzw. Deaktivieren von nachgelagerten Diensten.	71
Befehlshistorie.	72
Ansicht „Historie“.	73
Anzeigen der Historie.	74
Anzeigen von Ereignissen.	75
Kapitel 5: Domänenverwaltung.	76
Domänenverwaltung - Übersicht.	76
Alarmverwaltung.	77
Konfigurieren der SMTP-Einstellungen.	77
Alarmer abbonieren.	78
Alarmer anzeigen.	79
Ordnerverwaltung.	79
Erstellen eines Ordners.	80
Objekte in einen Ordner verschieben.	80
Entfernen eines Ordners	80
Domänensicherheitsmanagement.	81
Sicherheitsverwaltung für Benutzer.	81
Anwendungsdienstverwaltung.	82
Aktivieren und Deaktivieren von Diensten und Dienstprozessen.	82
Dienstprozesse anzeigen.	83
Konfigurieren des Neustarts für Dienstprozesse.	83
Anwendungsdienste entfernen.	84
Problembehebung für Anwendungsdienste.	84
Gateway-Konfiguration.	84
Konfigurieren von Gateway- und Worker-Knoten.	85
Domänenkonfigurationsverwaltung.	85
Sichern der Domänenkonfiguration.	86
Wiederherstellen der Domänen-Konfiguration.	86
Migrieren der Domänen-Konfiguration.	87
Aktualisieren der Domänenkonfigurationsdatenbankverbindung.	89
Umbenennen der Domäne.	90

Herunterfahren einer Domäne.	91
Domäneneigenschaften.	91
Allgemeine Eigenschaften.	92
Datenbankeigenschaften.	93
Gateway-Konfigurationseigenschaften.	93
Dienstebenenverwaltung.	94
SMTP-Konfiguration.	95
Benutzerdefinierte Eigenschaften für die Domäne.	96

Kapitel 6: Knoten..... 97

Knoten – Übersicht.	97
Knotentypen.	98
Gateway-Knoten.	98
Worker-Knoten.	98
Beispiel: Domäne mit mehreren Knoten.	98
Knotenrollen.	99
Dienstrolle.	99
Berechnungsrolle.	100
Aktualisieren der Knotenrolle.	100
Anzeigen von Prozessen auf einem Knoten mit Dienstrolle.	101
Definieren und Hinzufügen von Knoten.	101
Hinzufügen von Knoten zur Domäne.	102
Konfigurieren der Knoteneigenschaften.	103
Herunterfahren und Neustarten des Knotens.	106
Herunterfahren eines Knotens über das Administrator tool.	106
Starten oder Anhalten eines Knotens unter Windows.	106
Einen Knoten unter UNIX starten und anhalten.	106
Entfernen der Knotenzuordnung.	107
Entfernen eines Knotens.	107

Kapitel 7: Hohe Verfügbarkeit..... 108

Hohe Verfügbarkeit - Übersicht.	108
Belastbarkeit.	109
Belastbarkeit der Anwendungs-Clients.	109
Anwendungsdienst-Belastbarkeit.	110
Knoten-Belastbarkeit.	111
Beispielkonfiguration für ein Belastbarkeits-Timeout.	111
Neustart und Failover.	112
Domänen-Failover.	113
Anwendungsdienst - Neustart und Failover.	113
Wiederherstellung.	114
Konfiguration für einen hochverfügbare Domäne.	115
Konfiguration der Belastbarkeit für Anwendungsdienste.	116

Failover-Konfiguration für einen Anwendungsdienst.	117
Konfiguration für Failover und Wiederherstellung des PowerCenter-Integrationsdienstes. . . .	117
Konfiguration der Belastbarkeit für Befehlszeilenprogramme.	118
Domänen-Failover-Konfiguration.	119
Konfiguration des Knoten-Neustarts.	119
Oracle RAC-Datenbank-Failover.	119
Netzwerk, hohe Verfügbarkeit.	120

Kapitel 8: Verbindungen..... 121

Verbindungen - Übersicht.	121
Verbindungsverwaltung.	121
Erstellen einer Verbindung.	122
Aktualisieren der Verbindungsliste.	123
Anzeigen einer Verbindung.	123
Konfigurieren des Pooling für eine Verbindung.	123
Bearbeiten und Testen einer Verbindung.	124
Löschen einer Verbindung.	124
Pass-Through-Sicherheit.	125
Pass-Through-Sicherheit mit Datenobjekt-Zwischenspeicherung.	125
Pass-Through-Sicherheit hinzufügen	126
Poolingeigenschaften in Verbindungsobjekten.	126

Kapitel 9: Verbindungseigenschaften..... 128

Verbindungseigenschaften – Übersicht.	129
Adabas-Verbindungseigenschaften.	130
Amazon Redshift-Verbindungseigenschaften.	132
Amazon S3-Verbindungseigenschaften.	136
Eigenschaften der Blockchain-Verbindung.	139
Cassandra-Verbindungseigenschaften.	140
Confluent-Kafka-Verbindung.	142
Allgemeine Eigenschaften.	143
Eigenschaften des Confluent-Kafka-Brokers.	143
SSL-Eigenschaften	144
Erstellen einer Confluent-Kafka-Verbindung mit infacmd.	144
Databricks-Verbindungseigenschaften.	145
Greenplum-Verbindungseigenschaften.	147
Google Analytics-Verbindungseigenschaften.	148
Google BigQuery-Verbindungseigenschaften.	149
Verbindungsmodi.	151
Google Cloud Spanner-Verbindungseigenschaften.	152
Google Cloud Storage-Verbindungseigenschaften.	152
Google PubSub-Verbindungseigenschaften.	153
Hadoop-Verbindungseigenschaften.	154

Eigenschaften des Hadoop-Clusters.	155
Allgemeine Eigenschaften.	158
Eigenschaften des Ablehnungsverzeichnisses.	160
Blaze-Konfiguration.	160
Spark-Konfiguration.	162
HBase-Verbindungseigenschaften.	163
HDFS- oder ViewFS-Verbindungseigenschaften.	163
HBase-Verbindungseigenschaften für MapR-DB.	165
Hive-Verbindungseigenschaften.	166
HTTP-Verbindungseigenschaften.	170
Eigenschaften von IBM DB2-Verbindungen.	172
Eigenschaften von IBM DB2 for i5/OS-Verbindungen.	175
Eigenschaften von IBM DB2 for z/OS-Verbindungen.	179
IMS-Verbindungseigenschaften.	182
Eigenschaften der JDBC-Verbindung.	185
Eigenschaften der JDBC V2-Verbindung.	187
Eigenschaften der JD Edwards EnterpriseOne-Verbindung.	190
Kafka-Verbindungseigenschaften.	191
Allgemeine Eigenschaften.	192
Eigenschaften des Kafka-Brokers.	192
SSL-Eigenschaften.	193
Erstellen einer Kafka-Verbindung mit infacmd.	194
Kudu-Verbindungseigenschaften	194
Eigenschaften der LDAP-Verbindung.	195
Eigenschaften der Microsoft Azure Blob Storage-Verbindung.	196
Microsoft Azure Cosmos DB SQL API-Verbindungseigenschaften.	198
Eigenschaften der Microsoft Azure Data Lake Storage Gen1-Verbindung.	198
Eigenschaften der Microsoft Azure Data Lake Storage Gen2-Verbindung.	200
Eigenschaften der Microsoft Azure SQL Data Warehouse-Verbindung.	201
MS SQL Server-Verbindungseigenschaften.	203
Eigenschaften von Netezza-Verbindungen.	207
Eigenschaften von OData-Verbindungen.	208
ODBC-Verbindungseigenschaften.	209
Eigenschaften für Oracle-Verbindungen.	211
Salesforce-Verbindungseigenschaften.	214
Eigenschaften der Salesforce Marketing Cloud-Verbindung.	215
SAP-Verbindungseigenschaften.	217
Eigenschaften sequenzieller Verbindungen.	219
Snowflake-Verbindungseigenschaften.	222
Verbindungseigenschaften des parallelen Teradata-Transporters.	223
Tableau-Verbindungseigenschaften.	225
Tableau V3-Verbindungseigenschaften.	226

Streaming-Verbindungseigenschaften für Twitter.	228
VSAM-Verbindungseigenschaften.	229
Verbindungseigenschaften von Webdiensten.	231
Bezeichnereigenschaften in Datenbankverbindungen.	233
Reguläre Bezeichner.	233
Begrenzte Bezeichner.	233
Bezeichnereigenschaften.	234
Kapitel 10: Pläne.	236
Zeitpläne - Übersicht.	236
Erstellen und Bearbeiten von Zeitplänen.	236
Erstellen eines Zeitplans.	237
Bearbeiten eines Zeitplans.	239
Anhalten und Fortsetzen eines Zeitplans.	239
Entfernen von Jobs aus einem Zeitplan.	240
Löschen eines Zeitplans.	240
Kapitel 11: Exportieren und Importieren von Domänenobjekten.	241
Export und Import von Domänenobjekten - Übersicht	241
Exportprozess.	242
Regeln und Richtlinien für das Exportieren von Domänenobjekten.	242
Domänenobjekte anzeigen.	242
Darstellbare Domänenobjektnamen.	243
Importprozess.	244
Regeln und Richtlinien für den Import von Domänenobjekten.	244
Konfliktlösung.	244
Kapitel 12: Lizenzverwaltung.	246
Lizenzverwaltung - Übersicht.	246
Lizenzvalidierung.	247
Lizenzierungsprotokollereignisse.	247
Lizenzverwaltungstasks.	247
Arten von Lizenzschlüsseln.	248
Originalschlüssel.	248
Inkrementelle Schlüssel.	248
Ein Lizenzobjekt erstellen.	249
Eine Lizenz einem Dienst zuweisen.	250
Regeln und Richtlinien zum Zuweisen von Lizenzen an einen Dienst.	250
Entfernen eine Lizenz von einem Anwendungsdienst.	251
Aktualisieren einer Lizenz.	251
Entfernen einer Lizenz.	252
Lizenzeigenschaften.	252
Lizenzdetails.	253

Unterstützte Plattformen.	254
Repositorys.	254
Dienstoptionen.	254
Verbindungen.	255
Metadaten austausch-Optionen.	255
Kapitel 13: Überwachung.	256
Überwachen - Übersicht.	256
Konfigurieren der Überwachung.	257
Schritt 1. Überwachungseinstellungen konfigurieren.	258
Schritt 2. Konfigurieren der Ansichten „Berichte“ und „Statistiken“.	259
Optimieren der Überwachungsleistung.	260
Übersichtsstatistik.	261
Anzeigen der Übersichtsstatistik.	262
Data Integration Services überwachen	262
Eigenschaftensicht für einen Datenintegrationsdienst.	263
Berichtsansicht für einen Data Integration Service.	263
Überwachen von Ad-hoc-Jobs.	263
Anzeigen von Protokollen für einen Ad-hoc-Job.	267
Abbrechen eines Ad-hoc-Jobs.	267
Anzeigen der Übersichtsstatistik für einen Ad-hoc-Job.	267
Anzeigen von detaillierten Statistiken für einen Ad-hoc-Job.	268
Überwachen von Mapping-Audits.	268
Überwachen von Anwendungen.	269
Eigenschaftensicht für eine Anwendung.	269
Berichtsansicht einer Anwendung.	269
Überwachen bereitgestellter Zuordnungsjobs.	269
Logs für einen bereitgestellten Mapping-Job anzeigen.	270
Bereitgestellten Zuordnungsjob erneut ausgeben.	270
Bereitgestellten Mapping-Job abbrechen.	271
Anzeigen der Übersichtsstatistik für einen bereitgestellten Mapping-Job.	271
Anzeigen von detaillierten Statistiken für einen bereitgestellten Mapping-Job.	271
Anzeigen der Job-Statistiken für bereitgestellte Mappings mit dem REST Operations Hub-Dienst.	272
Logische Datenobjekte überwachen.	272
Eigenschaftensicht für ein logisches Datenobjekt.	272
Ansicht "Cache-Aktualisierungsdurchläufe" für ein logisches Datenobjekt.	273
Logs für Datenobjekt-Cache-Aktualisierungsdurchläufe.	273
SQL-Datendienste überwachen.	273
Eigenschaftensicht für einen SQL-Datendienst.	274
Verbindungsansicht für einen SQL Data Service.	274
Anfrageansicht eines SQL-Datendienstes.	275
Virtuelle Tabellen für einen SQL-Datendienst anzeigen.	275

Berichtsansicht eines SQL-Datendienstes.	276
Web-Dienste überwachen.	276
Eigenschaftenansicht für einen Web-Dienst.	277
Berichtsansicht eines Web-Dienstes.	277
Ansicht „Operationen“ für einen REST- oder SOAP-Webdienst.	277
Anfrageansicht eines Webdienstes.	278
Überwachen von Arbeitsabläufen.	278
Arbeitsablaufgrafik	278
Anzeigen von Arbeitsablaufobjekten.	279
Arbeitsablaufstatus.	280
Arbeitsablaufobjektstatus.	282
Arbeitselementstatus der Mapping-Aufgabe.	283
Abbrechen eines Arbeitsablaufs.	283
Arbeitsablaufwiederherstellung.	284
Arbeitsablaufprotokolle.	285
Jobstatus nach dem Neustart oder Failover des Anwendungsdiensts.	286
Überwachen eines Ordners von Objekten.	287
Anzeigen des Kontexts eines Objekts.	287
Konfigurieren des benutzerdefinierten Filters für Datum und Uhrzeit.	288
Konfigurieren des benutzerdefinierten Filters für abgelaufene Zeit.	288
Konfigurieren des benutzerdefinierten Filters Mehrfachauswahl.	288
Kapitel 14: Log-Verwaltung.	289
Protokollverwaltung - Übersicht.	289
Architektur des Protokollmanagers.	290
Log-Ereignisse der PowerCenter-Sitzung und des Arbeitsablaufs.	290
Job-Protokollereignisse des Datenintegrationsdiensts.	291
Protokollmanager-Wiederherstellung.	291
Fehlersuche für den Log Manager.	292
Protokollspeicherort.	292
Systemprotokolle.	293
Log-Verwaltung - Konfiguration.	293
Bereinigen von Log-Ereignissen.. . . .	294
Zeitzone.	295
Log-Management-Eigenschaften konfigurieren.	295
Die Registerkarte Logs.	295
Anzeigen von Protokollereignissen.	296
Konfigurieren von Log-Spalten.	297
Speichern von Log-Ereignissen.	298
Exportieren von Log-Ereignissen.	298
Fehlerprotokoll im Administrator Tool.	300
Protokollereignisse.	300
Protokollereignisse - Komponenten.	301

Domänenprotokollereignisse.	302
Log-Ereignisse im Analyst Service.	303
Protokollereignisse des Data Integration Service.	303
Log-Ereignisse des Listener Service.	303
Logger Service Konfigurationseigenschaften.	303
Protokollereignisse des Modellrepository-Dienst.	304
Benutzerdefinierte Rollen für den Metadata Manager Service.	304
Log-Ereignisse des PowerCenter Integration Service.	304
Log-Ereignisse des PowerCenter Repository Service.	304
Protokollereignisse des Ressourcenmanager-Diensts.	305
Log-Ereignisse des SAP BW Service.	305
Protokollereignisse des Scheduler-Diensts.	305
Log-Ereignisse des Web Services Hub.	306
Protokollereignisse der Benutzeraktivität.	306
Mapping-Aufgabenprotokolle.	307

Kapitel 15: Domänenberichte..... 308

Domänenberichte - Übersicht.	308
Lizenzverwaltungsbericht.	308
Lizenzierung.	309
CPU-Zusammenfassung.	310
CPU-Detail.	310
Repository-Zusammenfassung.	311
Benutzerzusammenfassung.	311
Benutzerdetail.	312
Hardwarekonfiguration.	312
Knotenkonfiguration.	313
Lizenzierte Optionen.	313
Lizenzverwaltungsbericht ausführen.	314
Lizenzverwaltungsbericht in einer E-Mail verschicken.	315
Web Services-Bericht.	315
Über den Web-Dienste-Bericht.	315
Allgemeine Eigenschaften und Zusammenfassung für den Web Services Hub.	317
Historienstatistik-Tabelle für Web Services.	318
Laufzeitstatistiken für Web Services.	318
Web-Dienst-Eigenschaften.	319
Top IP-Adressen des Web-Dienstes.	319
Historienstatistik-Tabelle für Web-Dienst.	320
Ausführen des Web Services Report.	320
Web Services Report für einen sicheren Web Services Hub ausführen.	321

Kapitel 16: Knotendiagnostiken..... 323

Knotendiagnostiken - Übersicht.	323
---	-----

Informatica-Netzwerk-Anmeldung.	324
Anmelden beim Informatica-Netzwerk.	324
Generieren der Knotendiagnostik.	325
Knotendiagnostiken herunterladen.	326
Knotendiagnostiken hochladen.	326
Knotendiagnostik analysieren.	327
Fehlerbehebungsmöglichkeiten erkennen.	328
Identifizieren von Empfehlungen.	328
Kapitel 17: Informationen zur Globalisierung.	329
Globalisierung - Übersicht.	329
Unicode.	330
Mit einem Unicode PowerCenter Repository arbeiten.	330
Gebietsschemata.	331
Systemgebietsschema.	332
Benutzerschema.	332
Eingabe-Gebietsschema.	332
Datenverschiebungsmodi.	332
Zeichendatenverschiebungs-Modes.	333
Ändern der Datenverschiebungsmodi.	333
Codepages - Übersicht.	334
UNIX Codepages.	335
Windows Codepages.	336
Auswählen einer Codepage.	336
Codepage-Kompatibilität.	336
Codepage der Domänenkonfigurationsdatenbank.	338
Codepage des Administrator Tools.	338
Codepage des PowerCenter Client.	338
Codepage des PowerCenter Integration Service-Prozesses.	339
PowerCenter Repository-Codepage.	339
Codepage für Metadaten Manager-Repository.	340
PowerCenter-Quell-Codepage.	340
PowerCenter-Target-Codepage.	341
Befehlszeilenprogramm-Codepages.	341
Codepage-Kompatibilität - Zusammenfassung.	342
Codepage-Validierung.	344
Entspannte Codepage-Validierung.	345
Konfigurieren des PowerCenter Integration Service.	346
Kompatible Quell- und Target-Codepages auswählen.	346
Fehlerbehebung für Codepage-Lockerung.	346
PowerCenter Codepage-Umwandlung.	347
Auswählen von Zeichen für PowerCenter Repository Metadaten.	347
Fallstudie: ISO 8859-1 Datenverarbeitung.	348

ISO 8859-1 Umgebung konfigurieren.	348
Fallstudie: Verarbeiten von Unicode UTF-16LE Daten.	351
UTF-16LE Umgebung konfigurieren.	351
Kapitel 18: Verwalten von Verteilungspaketen.	354
Verwaltung von Verteilungspaketen – Übersicht.	354
Vorbereitungen.	354
Installieren oder Entfernen von Verteilungspaketen im Konsolenmodus.	355
Installieren oder Entfernen von Verteilungspaketen im automatischen Modus.	356
Nach der Installation.	357
Anhang A: Codepages.	358
Unterstützte Codepages für Anwendungsdienste.	358
Unterstützte Codepages für Quellen und Ziele.	360
Anhang B: Benutzerdefinierte Rollen.	371
Benutzerdefinierte Rolle für den Analyst-Dienst.	371
Benutzerdefinierte Rollen für den Metadata Manager-Dienst.	372
Benutzerdefinierte Rolle für den Operator.	374
PowerCenter-Repository-Dienst - Benutzerdefinierte Rollen.	375
Benutzerdefinierte Rollen für den Test Data Manager.	376
Anhang C: Konnektivität der Informatica-Plattform.	380
Konnektivität der Informatica-Plattform - Übersicht.	380
Domänen-Konnektivität.	381
Model Repository-Konnektivität.	382
PowerCenter-Konnektivität.	383
Repository Service-Konnektivität.	385
Integration Service-Konnektivität.	385
PowerCenter Client-Konnektivität.	387
Metadata Manager-Dienst-Verbindung.	388
Native Konnektivität.	388
ODBC-Konnektivität.	388
JDBC-Konnektivität.	389
Anhang D: Konfigurieren des Webbrowsers.	390
Konfigurieren des Webbrowsers.	390
Index.	391

Einleitung

Verwenden Sie das *Informatica® Administrator-Handbuch*, um Informationen zur Anmeldung beim Administrator Tool zu erhalten und sich mit der Benutzeroberfläche vertraut zu machen. Informieren Sie sich über die Konfiguration, Verwaltung und Überwachung der Informatica-Domäne. Das Handbuch befasst sich unter anderem mit der Domänenarchitektur und den zugehörigen Komponenten, wie z. B. Knoten, Diensten, Hochverfügbarkeit, Verbindungen und Überwachung.

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

Grundlagen zu den Domänen

Dieses Kapitel umfasst die folgenden Themen:

- [Grundlagen zu den Domänen - Übersicht, 17](#)
- [Knoten, 18](#)
- [Dienstmanager, 19](#)
- [Anwendungsdienste, 20](#)
- [Hohe Verfügbarkeit, 26](#)
- [Informatica-Datennutzungsrichtlinie, 26](#)

Grundlagen zu den Domänen - Übersicht

Informatica verfügt über eine dienstorientierte Architektur, die die Fähigkeit zur Skalierung von Diensten und zum gemeinsamen Nutzen von Ressourcen über mehrere Rechner aufweist. Die Funktionalität der hohen Verfügbarkeit minimiert Dienstausschfallzeiten aufgrund unerwarteter Ausfälle und geplanter Wartung in der Informatica-Umgebung.

Die Informatica-Domäne stellt die grundlegende Verwaltungseinheit in Informatica dar. Die Domäne unterstützt die Verwaltung der verteilten Dienste. Eine Domäne ist eine Zusammenstellung von Knoten und Diensten, die Sie auf der Grundlage des Verwaltungseigentumsverhältnisses in Ordnern gruppieren können.

Ein Knoten entspricht der logischen Darstellung eines einzelnen Computers in einer Domäne. Ein Knoten in der Domäne fungiert als Gateway für Dienstanforderungen von Clients und leitet sie an den entsprechenden Dienst und Knoten weiter. Dienste und Prozesse laufen auf Knoten in einer Domäne. Die Verfügbarkeit eines Dienstes oder Prozesses auf einem Knoten hängt davon ab, wie Sie den Dienst und den Knoten konfigurieren.

Zu den Diensten für die Domäne gehören der Dienstmanager und eine Reihe von Anwendungsdiensten:

- **Dienstmanager.** Ein Dienst, der auf jedem Knoten in der Domäne ausgeführt wird, um alle Domänenvorgänge zu verwalten. Der Dienstmanager führt Domänenfunktionen aus, wie beispielsweise Authentifizierung, Autorisierung oder Protokollierung. Zudem startet der Dienstmanager die Anwendungsdienste, die für die Ausführung auf dem jeweiligen Knoten konfiguriert wurden.
- **Anwendungsdienste** Dienste, die serverbasierte Funktionalität darstellen, wie z. B. der Modellrepository-Dienst und der Datenintegrationsdienst. Die Anwendungsdienste, die auf einem Knoten laufen, hängen davon ab, wie Sie die Dienste konfigurieren.

Der Dienstmanager und die Anwendungsdienste steuern die Sicherheit. Der Dienstmanager verwaltet die Benutzer und Gruppen, die sich bei den Anwendungs-Clients anmelden können, und authentifiziert die Benutzer, die sich bei den Anwendungs-Clients anmelden. Der Dienstmanager und die Anwendungsdienste autorisieren Benutzeranfragen von Anwendungs-Clients.

Informatica Administrator (das Administrator Tool) umfasst die administrativen Aufgaben für Domänenobjekte, wie Dienste, Knoten, Lizenzen und Gitter. Sie verwalten die Domäne und die Sicherheit der Domäne mithilfe des Administrator tool.

Wenn Sie über die Option für hohe Verfügbarkeit verfügen, können Sie Dienste skalieren und einzelne Ausfallstellen (Single Points of Failure) für Dienste beseitigen. Dienste können, trotz temporärer Netzwerk- oder Hardware-Ausfälle, weiterhin ausgeführt werden.

Knoten

Ein Knoten entspricht einer logischen Darstellung eines einzelnen Computers in einer Domäne. Fügen Sie während der Installation die Installationsmaschine als Knoten zur Domäne hinzu. Sie können einer Domäne mehrere Knoten hinzufügen.

Jeder Knoten in der Domäne führt den Dienstmanager aus, der die Domänenfunktionen auf dem jeweiligen Knoten verwaltet. Zudem unterstützt der Dienstmanager die auf dem Knoten ausgeführten Anwendungsdienste. Die Domänenfunktionen und Dienste, die ein Knoten ausführt, sind abhängig von den folgenden Knotenkonfigurationen:

Knotentyp

Der Knotentyp legt fest, ob der Knoten als Gateway-Knoten oder als Worker-Knoten dient, und bestimmt die Domänenfunktionen, die der Knoten ausführt. Einer der Gateway-Knoten dient als Master-Gateway-Knoten für die Domäne. Der Master-Gateway-Knoten empfängt Dienstanfragen von Clients und leitet diese an den entsprechenden Dienst und Knoten weiter. Ein Worker-Knoten ist ein Knoten, der nicht als Gateway konfiguriert ist. Bei der ersten Installation der Informatica-Dienste erstellen Sie einen Gateway-Knoten und die Informatica-Domäne. Beim Installieren der Informatica-Dienste auf anderen Computern erstellen Sie weitere Gateway-Knoten oder Worker-Knoten, die Sie zur Domäne hinzufügen.

Knotenrolle

Die Knotenrolle gibt den Zweck des Knotens an. Ein Knoten mit der Dienstrolle kann Anwendungsdienste ausführen. Ein Knoten mit der Berechnungsrolle kann Berechnungen durchführen, die von Remote-Anwendungsdiensten angefragt werden. Ein Knoten mit beiden Rollen kann Anwendungsdienste ausführen und lokal Berechnungen für diese Dienste durchführen. Standardmäßig sind für alle Gateway- und Worker-Knoten sowohl die Dienst- als auch die Berechnungsrolle aktiviert. Wenn ein Knoten einem Datenintegrationsdienst-Gitter zugewiesen wird, können Sie die Knotenrolle bei Bedarf aktualisieren. Aktivieren Sie nur die Dienstrolle, wenn der Knoten den Datenintegrationsdienst-Prozess ausführen soll. Aktivieren Sie nur die Berechnungsrolle, wenn der Knoten Datenintegrationsdienst-Mappings ausführen soll.

Sie können Alarme abonnieren, um Benachrichtigungen über Knotenereignisse zu erhalten, wie z. B. Knotenfehler oder die Wahl eines Master-Gateways. Zudem können Sie Knotendiagnostiken generieren und in den Configuration Support Manager hochladen sowie Informationen über verfügbare EBF-Dateien und Informatica-Empfehlungen anzeigen.

Dienstmanager

Der Dienstmanager ist ein Dienst, der alle Domänenoperationen verwaltet. Er wird innerhalb der Informatica-Dienste ausgeführt. Er läuft als Dienst unter Windows und als Dämon unter UNIX. Beim Starten der Informatica-Dienste wird auch der Dienstmanager gestartet.

Der Dienstmanager wird auf jedem Knoten in der Domäne ausgeführt. Wenn der Dienstmanager nicht läuft, ist der Knoten nicht verfügbar.

Der Dienstmanager läuft auf allen Knoten in der Domäne, um die Domäne und Anwendungsdienste zu unterstützen:

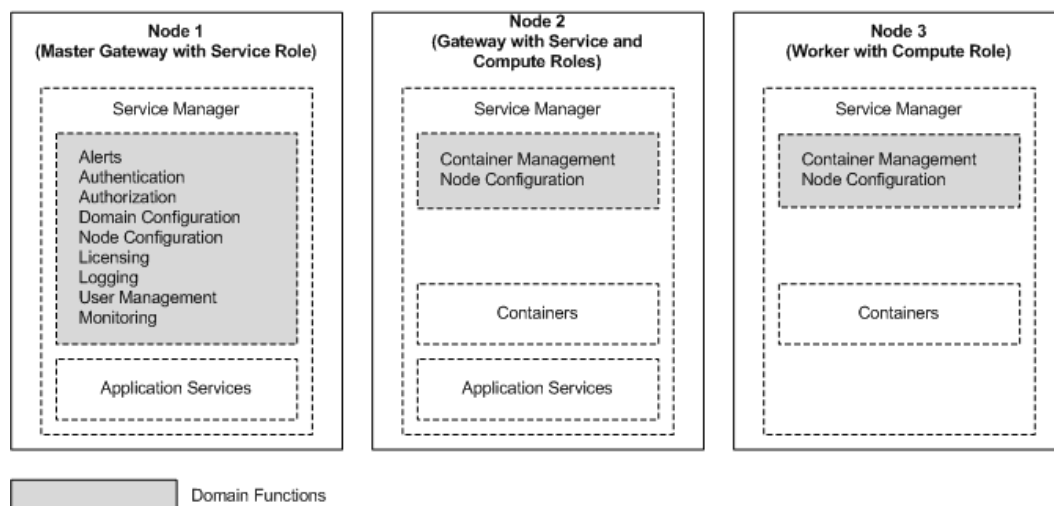
- **Domänen-Support.** Der Dienstmanager führt auf jedem Knoten Funktionen aus, um die Domäne zu unterstützen. Die Funktionen, die der Dienstmanager auf einem Knoten ausführt, variieren je nach Typ und Rolle des Knotens. Zum Beispiel führt der Dienstmanager, der auf dem Master-Gateway-Knoten läuft, alle Domänenfunktionen auf diesem Knoten aus. Der Dienstmanager, der auf einem anderen Knotentyp läuft, führt auf diesem Knoten eingeschränkte Domänenfunktionen aus.
- **Anwendungsdienst-Support.** Wenn ein Knoten über die Dienstrolle verfügt, startet der Dienstmanager die zur Ausführung auf diesem Knoten konfigurierten Anwendungsdienste. Er startet und stoppt Dienste und Dienstprozesse entsprechend den Anfragen von Clients. Außerdem leitet er Dienstanfragen an Anwendungsdienste weiter. Der Dienstmanager verwendet TCP/IP für die Kommunikation mit den Anwendungsdiensten.

In der nachstehenden Tabelle sind die vom Dienstmanager ausgeführten Domänenfunktionen beschrieben:

Funktion	Beschreibung
Alarmverwaltung	Der Dienstmanager sendet Alarme an abonnierte Benutzer. Sie können Alarme abonnieren, um über Knotenfehler, die Wahl eines Master-Gateways oder über Dienstprozess-Failover für Dienste auf der Domäne benachrichtigt zu werden. Wenn Sie Alarme abonnieren, erhalten Sie Benachrichtigungs-E-Mails. Die Alarmverwaltung findet auf dem Master-Gateway-Knoten statt.
Authentifizierung	Der Dienstmanager authentifiziert Benutzer, die sich bei Anwendungs-Clients anmelden. Die Authentifizierung findet auf dem Master-Gateway-Knoten statt.
Autorisierung	Der Dienstmanager autorisiert Benutzeranforderungen für Domänenobjekte anhand der Berechtigungen und Rollen, die dem Benutzer zugewiesen sind. Anfragen für Domänenobjekte können über das Administrator Tool gestellt werden. Die Domänenautorisierung findet auf dem Master-Gateway-Knoten statt.
Containerverwaltung	Wenn einem Knoten die Berechnungsrolle zugewiesen wurde, verwaltet der Dienstmanager die Container auf dem Knoten. Ein Container ist eine Zuweisung von Speicher- und CPU-Ressourcen. Ein Anwendungsdienst verwendet die Container, um Berechnungen auf dem Knoten remote durchzuführen. Beispiel: Ein Datenintegrationsdienst, der auf einem Gitter ausgeführt wird, kann ein Mapping innerhalb eines Containers auf einem Knoten mit Berechnungsrolle remote ausführen. Die Containerverwaltung findet auf einem beliebigen Knoten mit der Berechnungsrolle statt.
Domänenkonfiguration	Der Dienstmanager verwaltet die Metadaten der Domänenkonfiguration. Die Domänenkonfiguration findet auf dem Master-Gateway-Knoten statt.
Knotenkonfiguration	Der Dienstmanager verwaltet die Metadaten der Knotenkonfiguration in der Domäne. Die Knotenkonfiguration findet auf allen Knoten der Domäne statt.

Funktion	Beschreibung
Lizenzierung	Der Dienstmanager registriert Lizenzinformationen und überprüft diese beim Ausführen der Anwendungsdienste. Die Lizenzierung findet auf dem Master-Gateway-Knoten statt.
Protokollierung	Der Dienstmanager sammelt Protokollereignisse von jedem Dienst in der Domäne und stellt diese zur Verfügung. Um die Protokollierungsfunktion durchzuführen, führt der Dienstmanager einen Protokollmanager und einen Protokollagenten aus. Der Protokollmanager wird auf dem Master-Gateway-Knoten ausgeführt. Der Protokollagent wird auf allen Knoten ausgeführt, auf denen Sitzungen und Arbeitsabläufe des PowerCenter®-Integrationsdiensts sowie Datenintegrationsdienst-Jobs ausgeführt werden.
Benutzerverwaltung	Der Dienstmanager authentifiziert native und LDAP-Benutzer und Gruppen, die sich bei Anwendungs-Clients anmelden. Darüber hinaus verwaltet er die Erstellung von Rollen sowie die Zuweisung von Rollen und Berechtigungen zu nativen und LDAP-Benutzern und -Gruppen. Die Benutzerverwaltung findet auf dem Master-Gateway-Knoten statt.
Überwachung	Der Dienstmanager sorgt für das Beibehalten, Aktualisieren, Abrufen und Veröffentlichen von Laufzeitstatistiken für Integrationsobjekte im Überwachungsmodellrepository. Der Dienstmanager speichert die Überwachungskonfigurationsdetails im Domänenkonfigurations-Repository. Die Überwachung findet auf dem Master-Gateway-Knoten statt.

Die folgende Abbildung zeigt, wo der Dienstmanager Domänenfunktionen ausführt:



Anwendungsdienste

Bei Anwendungsdiensten handelt es sich um serverbasierte Funktionen.

Anwendungsdienste umfassen Dienste, die Sie erstellen, und Systemdienste, die bei Erstellung der Domäne für Sie erstellt werden. Ein Systemdienst kann in der Domäne eine einzelne Instanz haben.

Anwendungsdienste umfassen folgende Dienste:

- Analyst-Dienst
- Content-Managementdienst
- Datenintegrationsdienst
- Metadaten-Zugriffsdienst
- Metadata Manager-Dienst
- Modellrepository-Dienst
- PowerCenter-Integrationsdienst
- PowerCenter-Repository-Dienst
- PowerExchange®-Listenerdienst
- PowerExchange-Protokollierungsdienst
- Ressourcenmanager-Dienst
- SAP BW-Dienst
- Scheduler-Dienst
- Test Data Manager-Dienst
- Webdienst-Hub

Beim Konfigurieren eines Anwendungsdienstes benennen Sie einen Knoten, auf dem der Dienstprozess ausgeführt werden soll. Wenn der Dienstprozess ausgeführt wird, weist der Dienstmanager eine Portnummer in dem Portnummernbereich zu, der dem Knoten zugeordnet wurde.

Der Dienstprozess ist die Laufzeitdarstellung eines auf einem Knoten ausgeführten Dienstes. Wie viele Prozesse gleichzeitig ausgeführt werden können, richtet sich nach dem Diensttyp. So kann der PowerCenter-Integrationsdienst bei Ausführung auf einem Gitter beispielsweise mehrere Dienstprozesse gleichzeitig ausführen.

Haben Sie die Hochverfügbarkeitsoption, können Sie einen Dienst auf mehreren Knoten ausführen. Geben Sie an, auf welchem Primärknoten der Dienst laufen soll. Alle übrigen Knoten sind Backup-Knoten für den Dienst. Steht der Primärknoten nicht zur Verfügung, wird der Dienst auf einem Backup-Knoten ausgeführt. Sie können Alarmmeldungen abonnieren, um bei einem Dienstprozess-Failover eine Benachrichtigung zu erhalten.

Falls Sie nicht über die Hochverfügbarkeitsoption verfügen sollten, konfigurieren Sie einen Dienst für die Ausführung auf einem Knoten. Wenn Sie den Dienst mehreren Knoten zuweisen, wird der Dienst nicht gestartet.

Analyst-Dienst

Der Analyst-Dienst ist ein Anwendungsdienst, der die Anwendung Informatica Analyst in der Informatica-Domäne ausführt. Der Analyst-Dienst verwaltet die Verbindungen zwischen den Dienstkomponenten und den Benutzern, die sich beim Analyst Tool anmelden. Der Analyst-Dienst stellt eine Verbindung zu einem Datenintegrationsdienst, einem Modellrepository-Dienst, einem Metadata Manager- und einem Suchdienst her.

Der Analyst-Dienst gibt auch die folgenden Verzeichnisse und Datenbankverbindungen an:

- Verzeichnis des Einfachdatei-Cache
- Netzwerkverzeichnis für Einfachdateien
- Verzeichnis der Business Glossary-Exportdatei
- Audit-Datenbank der Ausnahmeverwaltung

Wenn Sie den Analyst-Dienst konfigurieren, verbinden Sie ihn mit einem Datenintegrationsdienst, um Profile, Scorecards und Mapping-Spezifikationen auszuführen. Sie können den Analyst-Dienst auch mit einem Datenintegrationsdienst verbinden, der Arbeitsabläufe zum Erstellen von Human-Tasks ausführt. Verbinden Sie den Analyst-Dienst mit einem Modellrepository-Dienst, um ein Modellrepository anzugeben.

Verbinden Sie den Analyst-Dienst mit einem Metadata Manager-Dienst, um Datenherkunftsvorgänge für Scorecards im Analyst-Tool durchzuführen. Verbinden Sie den Analyst-Dienst mit einem Suchdienst, um Suchoperationen im Analyst-Tool zu verwalten.

Geben Sie ein Cache-Verzeichnis für Einfachdateien zum Speichern von temporären Daten an. Einfachdateien an, die von Ihnen hochgeladen werden. Geben Sie ein Unternehmensglossarverzeichnis zum Speichern temporärer Dateien an, die Sie aus Business Glossary exportieren.

Geben Sie ein Einfachdatei-Netzwerkverzeichnis an, damit Sie Einfachdateien mithilfe der Netzwerkpfadoptio n im Analyst Tool importieren können.

Geben Sie eine Datenbank als Ausnahmeverwaltungs-Audit-Datenbank an, um einen Audit-Trail für alle Human-Task-Vorgänge in eine einzige Datenbank zu schreiben. Wenn Sie die Datenbank angeben, geben Sie auch das Schema für die Audit-Tabellen an. Die Datenbank speichert Audit-Daten für jede Arbeit, die Benutzer in Human-Task-Instanzen im Analyst Tool ausführen und die vom Analyst-Dienst verwaltet werden. Wenn Sie keine Datenbank und kein Schema angeben, schreibt der Analyst-Dienst Audit-Daten für jede Human-Task-Instanz in die Datenbank, in der die Human-Task-Daten gespeichert sind.

Content-Managementdienst

Der Content-Managementdienst ist ein Anwendungsdienst für die Verwaltung von Referenzdaten. Der Dienst stellt die Referenzdateneigenschaften für den Datenintegrationsdienst und das Developer Tool zur Verfügung. Der Dienst generiert auch Mapplets anhand der Regelspezifikationen. Sie können Regelspezifikationen erstellen und Mapplets aus Regelspezifikationen im Analyst Tool generieren.

Der Content-Managementdienst muss verfügbar sein, wenn Sie die folgenden Ressourcen verwenden:

Adressreferenzdaten

Der Content-Managementdienst verwaltet Konfigurationsinformationen für Adressreferenzdaten. Der Datenintegrationsdienst wendet die Konfigurationsinformationen bei der Ausführung einer Zuordnung an, die die Adressreferenzdaten liest.

Identitätspopulationsdateien

Der Content-Managementdienst verwaltet die Liste der Populationsdateien auf dem Knoten. Der Datenintegrationsdienst wendet die Populationskonfiguration bei der Ausführung einer Zuordnung an, die die Populationsdateien liest.

Probabilistische Modelldateien und Klassifizierermode lldateien

Der Content-Managementdienst speichert die Speicherorte sämtlicher probabilistischer Modelldateien und Klassifizierermode lldateien auf dem Knoten. Der Content-Managementdienst verwaltet außerdem den Kompilierungsstatus jedes Modells.

Referenztabellen

Der Content-Managementdienst gibt die Datenbank an, in der Datenwerte für die Referenztabellenobjekte im zugeordneten Modellrepository gespeichert werden.

Regelspezifikationen

Der Content-Managementdienst generiert Mapplets aus Regelspezifikationen. Der Analyst-Dienst wählt einen Content-Managementdienst aus, um die Mapplets zu generieren. Das Analyst Tool verwendet die Modellrepository-Dienstkonfiguration, um den Content-Managementdienst auszuwählen.

Data Integration Service

Der Data Integration Service ist ein Anwendungsdienst, der Datenintegrationsaufgaben für Informatica Analyst, Informatica Developer und externe Clients übernimmt. Zu den Datenintegrationsaufgaben gehören die Datenvorschau, die Ausführung von Profilen, SQL-Datendiensten, Web-Diensten und Mappings.

Wenn Sie einen Befehl aus der Befehlszeile oder einem externen Client ausgegeben haben, um SQL-Datendienste und Mappings in einer Anwendung auszuführen, sendet der Befehl die Anfrage an den Data Integration Service.

Sie können den Datenintegrationsdienst zur Ausführung auf den folgenden Domänenobjekten konfigurieren:

Auf Knoten

Falls Ihre Lizenz hohe Verfügbarkeit umfasst, können Sie den Dienst so konfigurieren, dass er auf mehreren Knoten ausgeführt wird. Standardmäßig wird der Dienst auf dem Primärknoten ausgeführt. Steht der Primärknoten nicht zur Verfügung, wird der Dienst auf einem Backup-Knoten ausgeführt. Wenn der Dienstprozess fehlschlägt oder der Knoten nicht mehr verfügbar ist, führt der Dienst ein Failover auf einen anderen Knoten aus. Falls Ihre Lizenz keine hohe Verfügbarkeit umfasst, können Sie den Dienst so konfigurieren, dass er auf einem Knoten ausgeführt wird.

In einem Gitter

Falls Ihre Lizenz Gitter umfasst, können Sie den Dienst zur Ausführung in einem Gitter konfigurieren. Ein Gitter ist ein Alias, das einer Gruppe von Knoten zugewiesen ist. Der Datenintegrationsdienst sendet Jobs an die verfügbaren Knoten, die dem Gitter zugewiesen sind. Wenn der Datenintegrationsdienst in einem Gitter ausgeführt wird, bleibt der Dienst verfügbar, falls ein Dienstprozess fehlschlägt oder ein Knoten nicht mehr verfügbar ist.

E-Mail-Dienst

Der E-Mail-Dienst ist ein Systemdienst, der E-Mail-Benachrichtigungen für Unternehmensglossare, Scorecards und Arbeitsabläufe verwaltet.

Aktivieren Sie den E-Mail-Dienst, damit Benutzer E-Mail-Benachrichtigungen konfigurieren können.

Die E-Mail-Dienst sendet E-Mails für die folgenden Benachrichtigungen:

- Business Glossary-Benachrichtigungen.
- Scorecard-Benachrichtigungen.
- Arbeitsablaufbenachrichtigungen. Zu den Arbeitsablaufbenachrichtigungen gehören E-Mails, die aus Human- und Benachrichtigungsaufgaben in Arbeitsabläufen gesendet werden, die der Datenintegrationsdienst ausführt.

Sie können den Dienst für die Ausführung auf mehreren Knoten konfigurieren. Geben Sie an, auf welchem Primärknoten der Dienst laufen soll. Alle übrigen Knoten fungieren als Sicherungsknoten für den Dienst. Steht der Primärknoten nicht zur Verfügung, wird der Dienst auf einem Sicherungsknoten ausgeführt.

Metadaten-Zugriffsdienst

Der Metadaten-Zugriffsdienst ist ein vom Benutzer verwalteter Dienst, der dem Developer Tool den Zugriff auf Hadoop-Verbindungsinformationen ermöglicht, um Metadaten zu importieren und in der Vorschau anzuzeigen.

Der Metadaten-Zugriffsdienst enthält Informationen über den Dienstprinzipalnamen (Service Principal Name, SPN) sowie Keytab-Informationen, wenn der Hadoop-Cluster Kerberos-Authentifizierung verwendet. Sie können einen oder mehrere Metadaten-Zugriffsdienste auf einem Knoten erstellen. Je nach Lizenz kann der Metadaten-Zugriffsdienst hoch verfügbar sein.

HBase-, HDFS-, Hive- und MapR-DB-Verbindungen verwenden den Metadaten-Zugriffsdienst, wenn Sie ein Objekt aus einem Hadoop-Cluster importieren. Die Google Cloud Storage-Verbindung verwendet den Metadaten-Zugriffsdienst zum Importieren von Metadaten von Dateien in Google Cloud Storage. Erstellen und konfigurieren Sie einen Metadaten-Zugriffsdienst, bevor Sie Google Cloud Storage-, HBase-, HDFS-, Hive- und MapR-DB-Verbindungen erstellen.

Metadata Manager Service

Der Metadata Manager Service ist ein Anwendungsdienst, der die Metadata Manager-Anwendung ausführt und die Verbindungen zwischen den Metadata Manager-Komponenten verwaltet.

Mit Metadata Manager werden Metadaten von unterschiedlichen Metadaten-Repositories durchsucht und analysiert. Sie können Metadaten aus folgenden Quellen laden, durchsuchen und analysieren: Anwendungen, Business Intelligence, Data Integration, Data Modelling und aus relationalen Metadatenquellen.

Der Metadata Manager Service lässt sich für die Ausführung auf nur einem Knoten konfigurieren. Der Metadata Manager Service ist kein Dienst mit hoher Verfügbarkeit. Dennoch können Sie mehrere Metadata Manager Services auf demselben Knoten ausführen.

Modellrepository-Dienst

Der Modellrepository-Dienst verwaltet das Modellrepository. Im Modellrepository werden die von Informatica-Produkten erstellten Metadaten in einer relationalen Datenbank gespeichert, um die Zusammenarbeit zwischen den Produkten zu ermöglichen. Informatica Developer, Informatica Analyst, der Datenintegrationsdienst und das Administrator Tool speichern Metadaten im Modellrepository.

Sie können ein Modellrepository als Überwachungsmodellrepository konfigurieren. Anschließend können Sie einen Überwachungsmodellrepository-Dienst für das Überwachungsmodellrepository einrichten. Der Überwachungsmodellrepository-Dienst überwacht Statistiken für Datenintegrationsdienstjobs. Sie konfigurieren den Überwachungsmodellrepository-Dienst in den Domäneneigenschaften.

Erstellen Sie je einen Modellrepository-Dienst pro Modellrepository. Wenn Sie einen Modellrepository-Dienst erstellen, können Sie ein Modellrepository erstellen oder ein vorhandenes Modellrepository verwenden. Sie können mehrere Modellrepository-Dienste auf demselben Knoten ausführen.

PowerCenter Integration Service

Der PowerCenter Integration Service führt PowerCenter-Sitzungen und -Arbeitsabläufe aus. Bei der Konfiguration des PowerCenter Integration Service können Sie angeben, wo er ausgeführt werden soll:

- Auf einem Gitter. Wenn Sie den Dienst so konfigurieren, dass er auf einem Gitter ausgeführt wird, kann er auf mehreren Knoten gleichzeitig laufen. Der PowerCenter Integration Service sendet Tasks an die verfügbaren Knoten, die dem Gitter zugeordnet sind. Wenn Sie nicht über die Option für hohe Verfügbarkeit verfügen, schlägt der Task fehl, wenn einer der Dienstprozesse oder Knoten nicht mehr verfügbar ist. Wenn Sie über die Option für hohe Verfügbarkeit verfügen, stehen Failover und Wiederherstellung zur Verfügung, wenn einer der Dienstprozesse oder Knoten nicht mehr verfügbar ist.
- Auf Knoten. Wenn Sie über die Option für hohe Verfügbarkeit verfügen, können Sie den Dienst so konfigurieren, dass er auf mehreren Knoten läuft. Standardmäßig läuft er auf dem primären Knoten. Wenn der primäre Knoten nicht verfügbar ist, wird er auf einem Backup-Knoten ausgeführt. Wenn der Dienstprozess fehlschlägt oder der Knoten nicht mehr verfügbar ist, wechselt der Dienst auf einen anderen Knoten. Wenn Sie nicht über die Option für hohe Verfügbarkeit verfügen, können Sie den Dienst so konfigurieren, dass er auf einem Knoten läuft.

PowerCenter-Repository-Dienst

Der PowerCenter-Repository-Dienst verwaltet das PowerCenter-Repository. Er ruft Metadaten ab, fügt sie in die PowerCenter-Repository-Datenbanktabellen ein und aktualisiert sie. Wenn der Dienstprozess fehlschlägt oder die Knoten nicht verfügbar sind, ist der Dienst nicht mehr verfügbar.

Wenn Sie die Option hohe Verfügbarkeit verwenden, können Sie den Dienst so konfigurieren, dass er auf den Primär- oder Backup-Knoten ausgeführt wird. Standardmäßig wird der Dienstprozess auf einem Primärknoten ausgeführt. Wenn der Dienstprozess fehlschlägt, startet ein neuer Prozess auf demselben Knoten. Steht der Knoten nicht mehr zur Verfügung, startet der Dienstprozess auf einem der Backup-Knoten.

PowerExchange Listener Service

Der PowerExchange Listener Service ist ein Anwendungsdienst, der das PowerExchange Listener verwaltet. Der PowerExchange Listener verwaltet die Kommunikation zwischen einem PowerCenter oder PowerExchange Client und einer Datenquelle bei der Datenbestandsverschiebung und der Erfassung von Datenänderungen. Der PowerCenter Integration Service verbindet sich über den Listener Service mit PowerExchange Listener. Um einen Dienst zu verwalten und die Dienst-Logs anzuzeigen, verwenden Sie das Administrator Tool.

Wenn Sie die Option der hohen Verfügbarkeit im PowerCenter verwenden, können Sie den Listener Service auf mehreren Knoten ausführen. Wenn der Listener Service-Prozess auf dem Primärknoten fehlschlägt, wird er auf den Backup-Knoten verlagert.

PowerExchange Logger Service

Der Logger Service ist ein Anwendungsdienst, der den PowerExchange Logger für Linux, UNIX und Windows verwaltet. Der PowerExchange Logger erfasst Änderungsdaten von einer Datenquelle und schreibt die Daten in Log-Dateien des PowerExchange Loggers. Um den Dienst zu verwalten und die Dienst-Logs anzuzeigen, verwenden Sie das Administrator Tool.

Wenn Sie die Option der hohen Verfügbarkeit im PowerCenter verwenden, können Sie den Logger Service auf mehreren Knoten ausführen. Wenn der Logger Service-Prozess auf dem Primärknoten fehlschlägt, wird er auf den Backup-Knoten verlagert.

Ressourcenmanager-Dienst

Der Ressourcenmanager-Dienst ist ein Systemdienst, der Rechenressourcen in der Domäne verwaltet und Jobs versendet, um optimale Leistungs- und Skalierbarkeitsergebnisse zu erzielen. Der Ressourcenmanager-Dienst sammelt Informationen über Knoten mit der Berechnungsrolle. Der Dienst gleicht die Jobanforderungen mit der Ressourcenverfügbarkeit ab und ermittelt so den besten Berechnungsknoten für die Ausführung des Jobs.

Der Ressourcenmanager-Dienst kommuniziert mit Berechnungsknoten in einem Datenintegrationsdienstgitter. Aktivieren Sie den Ressourcenmanager-Dienst, wenn Sie ein Datenintegrationsdienstgitter für die Ausführung von Jobs in separaten Remoteprozessen konfigurieren.

Sie können den Dienst für die Ausführung auf mehreren Knoten konfigurieren. Geben Sie an, auf welchem Primärknoten der Dienst laufen soll. Alle übrigen Knoten sind Backup-Knoten für den Dienst. Steht der Primärknoten nicht zur Verfügung, wird der Dienst auf einem Backup-Knoten ausgeführt.

SAP BW Service

Der SAP BW Service wartet auf RFC Abfragen von einem SAP NetWeaver BI und initiiert Arbeitsabläufe, die aus dem SAP NetWeaver BI extrahieren oder dorthin laden. Der SAP BW Service ist nicht hoch verfügbar. Sie können ihn so konfigurieren, dass er auf einem Knoten ausgeführt wird.

Scheduler-Dienst

Der Scheduler-Dienst ist ein Systemdienst, der Zeitpläne für Profile, Scorecards, bereitgestellte Zuordnungen und bereitgestellte Arbeitsabläufe verwaltet.

Aktivieren Sie den Scheduler-Dienst zum Erstellen, Verwalten und Ausführen von Zeitplänen.

Sie können den Dienst für die Ausführung auf mehreren Knoten konfigurieren. Geben Sie an, auf welchem Primärknoten der Dienst laufen soll. Alle übrigen Knoten sind Backup-Knoten für den Dienst. Steht der Primärknoten nicht zur Verfügung, wird der Dienst auf einem Backup-Knoten ausgeführt.

Web Services Hub

Der Web Services Hub erhält Anfragen vom Web-Dienst-Client und stellt die PowerCenter-Arbeitsabläufe als Services bereit. Der Web Services Hub lässt sich nicht auf assoziierten Dienstprozessen ausführen. Er wird innerhalb der Dienstverwaltung ausgeführt.

Hohe Verfügbarkeit

Die hohe Verfügbarkeit ist eine Option, die einen einzelnen Fehlerpunkt in einer Domäne entfernt und eine minimale Dienstunterbrechung im Falle eines Fehlers gewährleistet. Die hohe Verfügbarkeit besteht aus zwei Komponenten:

- Belastbarkeit. Darunter wird die Fähigkeit eine Anwendung verstanden, vorübergehende Netzwerkfehler zu tolerieren bis entweder das Belastbarkeits-Timeout abgelaufen ist, oder der externe Systemfehler behoben wurde.
- Failover. Darunter wird die Migration eines Anwendungsdienstes oder einer Task auf einen andern Knoten verstanden, wenn der Knoten, der den Dienstprozess ausführt, un erreichbar geworden ist.
- Wiederherstellung. Dies ist die automatische Vervollständigung einer Task, nachdem ein Dienst unterbrochen worden ist. Die automatische Wiederherstellung steht für die Tasks des PowerCenter Integration Service und des PowerCenter Repository Service zur Verfügung. Sie können die Arbeitsabläufe und Sitzungen des PowerCenter Integration Service aber auch manuell wiederherstellen. Die manuelle Wiederherstellung ist jedoch nicht Teil der hohen Verfügbarkeit.

Informatica-Datennutzungsrichtlinie

Informatica DiscoveryIQ ist ein Produktnutzungs-Toolkit in der Informatica-Domäne, das Routineberichte über Datennutzung und Systemstatistiken an Informatica sendet.

Nach der Installation und Konfiguration der Informatica-Domäne lädt Informatica DiscoveryIQ alle 15 Minuten Daten an Informatica hoch. Danach sendet die Domäne alle paar Tage Daten an Informatica. Datensammlung

und -upload sind standardmäßig aktiviert. Sie können angeben, dass keine Nutzungsstatistiken an Informatica gesendet werden.

Wenn das Netzwerk, auf dem die Informatica-Dienste installiert sind, für die Kommunikation mit dem externen Netzwerk einen Proxy-Server benötigt, konfigurieren Sie die Proxy-Details.

Mit Informatica DiscoveryIQ ist es für Informatica möglich, den Zustand Ihrer Umgebung durch Analyse der Systemstatistiken und Domänenberichte zu überprüfen. Sie erhalten von Informatica basierend auf den Berichten Informationen über bewährte Methoden und Empfehlungen, um Probleme auf der Domäne zu lösen. Die Nutzungsstatistiken ermöglichen Informatica einen proaktiven Einblick in Produktimplementierungen.

Informatica DiscoveryIQ sendet die folgenden Daten an Informatica:

- Details zum Betriebssystem
- CPU-Informationen
- Seriennummer des Informatica-Lizenzschlüssels
- Gateway-Informationen
- Domänenoptionen
- Knotenoptionen
- Anwendungsdienstoptionen

Konfigurieren der Informatica-DiscoveryIQ Proxy-Details

Konfigurieren Sie die Proxyserver-Details, wenn das Netzwerk, auf dem Informatica-Dienste installiert sind, einen Proxyserver zur Kommunikation mit dem externen Netzwerk verwendet.

1. Klicken Sie im Überschriftsbereich des Administrator-Tools auf **Verwalten > DiscoveryIQ Proxy Details**.
2. Geben Sie die Domäne, Hostname und Portnummer des Proxyservers ein.
3. Geben Sie den Benutzernamen und Passwort ein, um eine Verbindung zum Proxyserver herzustellen.
4. Klicken Sie auf **OK**, um die Proxyserver-Details zu speichern.

Deaktivieren der Informatica-Datennutzung

Sie können das Hochladen von Nutzungsdaten aus der Informatica-Domäne in das Administrator-Tool deaktivieren.

1. Klicken Sie im Administrator-Tool auf **Hilfe > Info**.
2. Klicken Sie auf **Richtlinie zur Datennutzung**.
3. Löschen Sie **Sammlung von Nutzungsdaten aktivieren**.
4. Klicken Sie auf **OK**.

KAPITEL 2

Eigenes Konto verwalten

Dieses Kapitel umfasst die folgenden Themen:

- [Eigenes Konto verwalten - Übersicht, 28](#)
- [Passwortverwaltung, 28](#)
- [Einstellungen, 29](#)
- [Informatica Network-Anmeldedaten, 30](#)

Eigenes Konto verwalten - Übersicht

Verwalten Sie Ihr Konto, um Ihr Passwort zu ändern oder Benutzereinstellungen zu bearbeiten.

Wenn Sie ein natives Benutzerkonto haben, können Sie Ihr Passwort jederzeit mit der Anwendung "Passwort ändern" ändern. Wenn jemand anderes Ihr Benutzerkonto angelegt hat, ändern Sie Ihr Passwort, wenn Sie sich zum ersten Mal beim Administrator Tool anmelden.

Die Benutzereinstellungen legen fest, welche Optionen bei der Anmeldung im Administrator Tool angezeigt werden. Die Benutzereinstellungen wirken sich nicht auf die Optionen aus, die angezeigt werden, wenn sich ein anderer Benutzer beim Administrator Tool anmeldet.

Sie können Ihre Anmeldedaten für das Informatica Network für Ihr Konto konfigurieren, um über das Administrator Tool auf die Informatica-Wissensdatenbank zuzugreifen.

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**.

Einstellungen

Ihre Einstellungen legen fest, welche Optionen bei der Anmeldung im Administrator Tool angezeigt werden. Ihre Einstellungen wirken sich nicht auf die Optionen aus, die angezeigt werden, wenn sich ein anderer Benutzer beim Administrator Tool anmeldet.

Die folgende Tabelle beschreibt die Optionen, die Sie in Ihren Einstellungen konfigurieren können:

Option	Beschreibung
Alarmer abonnieren	Abonnieren Sie für Domänen- und Dienst-Alarmer. Für Ihr Benutzerkonto muss eine gültige E-Mail-Adresse konfiguriert sein. Standardwert ist „Nein“.
Benutzerdefinierte Eigenschaften anzeigen	Zeigt benutzerdefinierte Eigenschaften im Inhaltsbereich an, wenn Sie auf ein Objekt im Navigator klicken. Mit benutzerdefinierten Eigenschaften konfigurieren Sie das Verhalten von Informatica für besondere Fälle oder zur Leistungssteigerung. Blenden Sie die benutzerdefinierten Eigenschaften aus, um zu vermeiden, dass die Werte versehentlich geändert werden. Verwenden Sie benutzerdefinierte Eigenschaften nur auf Anweisung des globalen Benutzersupports von Informatica.

Um die Einstellungen zu ändern, klicken Sie im Kopfbereich von Administrator Tool auf **Verwaltung > Einstellungen**.

Informatica Network-Anmeldedaten

Sie können Ihre Anmeldedaten für Informatica Network im Administrator Tool eingeben, um über das Administrator Tool auf die Informatica-Wissensdatenbank zuzugreifen.

Sie können auch die Suchergebnisse für eine Fehlermeldung in der Informatica-Wissensdatenbank durch Klicken auf den Fehlermeldungscode im Administrator-Tool anzeigen.

Informatica Network-Anmeldedaten eingeben

Geben Sie Ihre Anmeldedaten für Informatica Network ein, um mit dem Administrator Tool auf die Informatica-Wissensdatenbank zuzugreifen.

1. Klicken Sie auf **Verwalten > Anmeldedaten für Supportportal**.
Daraufhin wird das **Anmeldefenster für Informatica Network** angezeigt.
2. Geben Sie Ihre Anmeldedaten für Informatica Network und die Kundenprojekt-ID ein.
3. Klicken Sie auf **OK**.

Suchen der Informatica-Wissensdatenbank

Sie können direkt über das Administrator-Tool nach Begriffen in der Informatica-Wissensdatenbank suchen.

1. Klicken Sie auf **Hilfe > Wissensdatenbank durchsuchen**.
Das Fenster **Wissensdatenbank durchsuchen** wird angezeigt.
2. Geben Sie den Begriff für die Suche im Textfeld ein.
3. Klicken Sie auf **OK**.
Die Suchergebnisse werden in einem anderen Browserfenster angezeigt.

KAPITEL 3

Informatica Administrator

Dieses Kapitel umfasst die folgenden Themen:

- [Verwenden von Informatica Administrator - Übersicht, 31](#)
- [Anmelden beim Informatica Administrator, 32](#)
- [Registerkarte „Verwalten“, 33](#)
- [Registerkarte „Verwalten“ - Ansicht „Domäne“, 34](#)
- [Registerkarte „Verwalten“ - Ansicht „Dienste und Knoten“, 38](#)
- [Registerkarte „Verwalten“ – Verbindungsansicht, 48](#)
- [Registerkarte „Verwalten“ - Ansicht „Pläne“, 49](#)
- [Registerkarte „Überwachen“, 49](#)
- [Registerkarte „Überwachen“ - Ansicht „Übersichtsstatistik“, 51](#)
- [Registerkarte „Überwachen“ - Ansicht „Ausführungsstatistiken“, 52](#)
- [Registerkarte "Protokolle", 59](#)
- [Registerkarte Berichte, 59](#)
- [Registerkarte Sicherheit, 60](#)
- [Dienststatus, 64](#)
- [Prozessstatus, 64](#)
- [Jobstatus, 66](#)
- [Barrierefreiheit von Informatica Administrator - Übersicht, 67](#)

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.
- **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.

Anmelden beim Informatica Administrator

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

Wenn die Informatica-Domäne in einem Netzwerk mit Kerberos-Authentifizierung ausgeführt wird, müssen Sie den Browser so konfigurieren, dass der Zugriff auf die Informatica-Webanwendungen möglich ist. Fügen Sie in Microsoft Internet Explorer, Microsoft Edge und Google Chrome die URL der Informatica-Webanwendung zur Liste der vertrauenswürdigen Sites hinzu. Fügen Sie in Safari das Zertifikat der Informatica-Webanwendung zum Schlüsselbund hinzu. Wenn Sie Chrome Version 86.0.42x oder höher unter Windows verwenden, müssen Sie auch die Richtlinien `AuthServerWhitelist` und `AuthNegotiateDelegateWhitelist` festlegen.

1. Starten Sie Microsoft Internet Explorer oder Google Chrome.
2. Geben Sie in der **Adresszeile** die URL für das Administrator Tool ein:
 - Wenn das Administrator Tool nicht für die Verwendung einer sicheren Verbindung konfiguriert wurde, geben Sie die folgende URL ein:

```
http://<fully qualified hostname>:<http port>/administrator/
```

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

```
https://<fully qualified hostname>:<https port>/administrator/
```

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

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

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

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

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

Informatica Administrator-URL

In der URL des Administrator-Tools stellt `<Host>:<Port>` den Hostnamen des Master-Gateway-Knotens und die Portnummer des Administrator-Tools dar.

Den Port für das Administrator-Tool konfigurieren Sie beim Definieren der Domäne. Sie können die Domäne beim Installieren oder durch Ausführen des Befehlszeilenprogramms *infasetup* DefineDomain definieren. Wenn Sie den Domänen-Port anstatt des Administrator-Tool-Ports in die URL eingeben, wird der Browser zum Administrator-Tool-Port weitergeleitet.

Hinweis: Bei einem Failover der Domäne zu einem anderen Master-Gateway-Knoten entspricht der Hostname in der URL des Administrator-Tools dem Hostnamen des gewählten Master-Gateway-Knotens.

Fehlerbehebung bei der Anmeldung bei Informatica Administrator

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

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

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

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

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

Registerkarte „Verwalten“

Auf der Registerkarte **Verwalten** können Sie die Domäne und die in ihr enthaltenen Objekte verwalten.

Welche Inhalte auf der Registerkarte **Verwalten** angezeigt werden und welche Aufgaben Sie darauf ausführen können, hängt von der Ansicht ab, die Sie auswählen. Sie können die folgenden Ansichten auswählen:

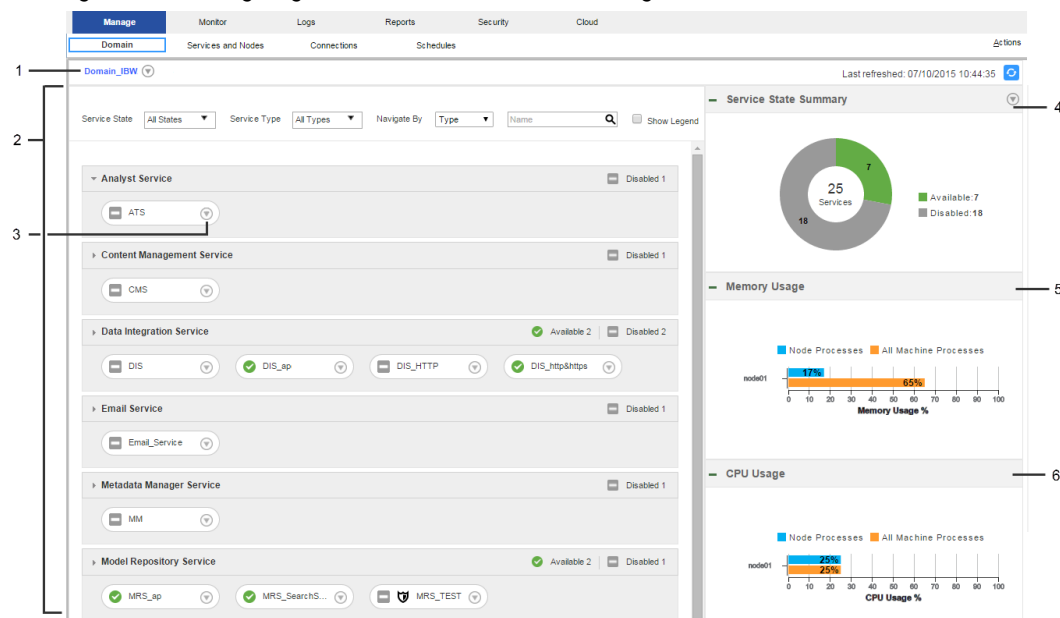
- **Domäne** Zur Anzeige und Verwaltung von Domänenstatus, Ressourcenverbrauch und Ereignissen.
- **Dienste und Knoten** Zur Anzeige und Verwaltung von Anwendungsdiensten und -knoten.

- **Verbindungen** Zur Anzeige und Verwaltung von Verbindungen.
- **Pläne.** Zeigen Sie Zeitpläne für Profile, Scorecards, bereitgestellte Zuordnungen und bereitgestellte Arbeitsabläufe an und verwalten Sie diese.

Registerkarte „Verwalten“ - Ansicht „Domäne“

In der Ansicht **Domäne** wird eine Übersicht der Domäne und ihrer Inhalte angezeigt. Sie können in der Ansicht „Domäne“ den Domänenstatus, den Ressourcenverbrauch und Ereignisse überwachen. Außerdem können Sie Domänenaktionen durchführen, beispielsweise die Aktivierung und Deaktivierung von Diensten.

Die folgende Abbildung zeigt die Ansicht **Domäne** auf der Registerkarte **Verwalten**:



1. Menü „Aktionen“ für Domänen
2. Inhaltsbereich
3. Menü „Aktionen“ für Objekte
4. Dienststatus - Zusammenfassung
5. Speichernutzungsanzeige
6. CPU-Nutzungsanzeige

Die Ansicht **Domäne** enthält folgende Komponenten:

Menü „Aktionen“ für Domänen

Im Menü „Aktionen“ für Domänen können Sie weitere Informationen zur Domäne anzeigen oder die Domäne herunterfahren.

Im Menü „Aktionen“ für Domänen können Sie die folgenden Aufgaben durchführen:

- Eigenschaften anzeigen. Öffnen der Ansicht „Dienste und Knoten“ und Anzeigen der Eigenschaften für die Domäne.
- Verlauf anzeigen. Öffnen der Ansicht „Historie“ und Anzeigen der gestrigen Domänenereignisse.
- Protokolle anzeigen. Öffnen der Registerkarte „Protokolle“ und Anzeigen der gestrigen Dienstmanager-Protokollereignisse.

- Befehlshistorie anzeigen. Öffnen des Bereichs „Befehlshistorie“ und Anzeigen der letzten 50 Dienst-Lebenszyklusbefehle, die im Administrator Tool ausgeführt wurden.
- Domäne herunterfahren.

Inhaltsbereich

Zeigt Domänenobjekte und deren Status an. Zu den Domänenobjekten gehören Dienste, Knoten und Gitter.

In der folgenden Tabelle werden die Methoden zum Anzeigen von Objekten im Inhaltsbereich beschrieben:

Methode	Beschreibung
Dienststatus	Filtern von Diensten nach folgenden Status: - Alle Status - Verfügbar - Nicht verfügbar - Deaktiviert
Diensttyp	Filtern einiger oder aller Dienste in der Domäne.
Navigieren nach	Gruppieren von Objekten nach Knoten, Typ oder Ordner.
Suchen	Suchen anhand des Namens nach einem Objekt. Sie können in diesem Feld das Sternchen (*) als Platzhalterzeichen verwenden.
Legende anzeigen	Anzeigen einer Liste der Statussymbole und Beschreibungen.

Menüs „Aktionen“ für Objekte

Die Objekte im Inhaltsbereich verfügen jeweils über ein Menü „Aktionen“. Über das jeweilige Menü „Aktionen“ können Sie Informationen über Domänenobjekte anzeigen oder gängige Aufgaben ausführen. Welche Informationen Sie anzeigen und welche Aufgaben Sie durchführen können, hängt von dem Objekt ab, das Sie auswählen.

Im Menü „Aktionen“ eines Diensts können Sie die folgenden Aufgaben durchführen:

- Eigenschaften anzeigen. Öffnen der Ansicht „Dienste und Knoten“ und Anzeigen der Eigenschaften für den Dienst.
- Verlauf anzeigen. Öffnen Sie die Ansicht „Historie“ und zeigen Sie die gestrigen Dienstereignisse an.
- Protokolle anzeigen. Öffnen der Registerkarte „Protokolle“ und Anzeigen der gestrigen Dienstprotokollereignisse.
- Abhängigkeiten anzeigen. Öffnen der Abhängigkeitsgrafik und Anzeigen direkter Abhängigkeiten für den Dienst.
- Dienst wiederherstellen.
- Aktivieren bzw. Deaktivieren des Diensts.

Im Menü „Aktionen“ eines Knotens können Sie die folgenden Aufgaben durchführen:

- Eigenschaften anzeigen. Öffnen der Ansicht „Dienste und Knoten“ und Anzeigen der Eigenschaften für den Knoten.
- Verlauf anzeigen. Öffnen der Ansicht „Historie“ und Anzeigen der gestrigen Knotenereignisse.

- Abhängigkeiten anzeigen. Öffnen der Abhängigkeitsgrafik und Anzeigen direkter Abhängigkeiten für den Knoten.
- Knoten herunterfahren

Im Menü „Aktionen“ eines Gitters können Sie die folgenden Aufgaben durchführen:

- Eigenschaften anzeigen. Öffnen der Ansicht „Dienste und Knoten“ und Anzeigen der Eigenschaften für das Gitter.
- Abhängigkeiten anzeigen. Öffnen der Abhängigkeitsgrafik und Anzeigen direkter Abhängigkeiten für das Gitter.

Dienststatus - Zusammenfassung

Ringdiagramm mit der Anzahl der Dienste in der Domäne und deren Status. Wenn Sie im Diagramm auf einen Status klicken, werden im Inhaltsbereich die Dienste mit dem entsprechenden Status angezeigt.

Ressourcennutzungsanzeigen

Balkendiagramme zum Vergleichen der Ressourcennutzung eines Domänenprozesses mit der Ressourcennutzung aller Prozesse auf dem Computer. Die Ansicht „Domäne“ enthält eine Speichernutzungsanzeige und eine CPU-Nutzungsanzeige.

Registerkarte „Verwalten“ - Menü „Aktionen“

Greifen Sie auf die Hilfe für die Ansicht „Domäne“ zu.

Detailbereich

Wenn Sie ein Domänenobjekt auswählen, werden im **Detailbereich** Informationen zu diesem Objekt angezeigt. Welche Informationen angezeigt werden, hängt von dem Objekt ab, das Sie auswählen.

In der folgenden Tabelle werden die Details beschrieben, die je nach dem im Inhaltsbereich ausgewählten Objekt angezeigt werden:

Objekt	Inhalt des Detailbereichs
Knoten	Knotenname und -status. Klicken Sie auf den Namen des Knotens, um die Knoteneigenschaften anzuzeigen.
Dienst	Im Detailbereich werden die folgenden Inhalte für einen Dienst angezeigt: <ul style="list-style-type: none"> - Dienstname und -status. Klicken Sie auf den Namen des Diensts, um die Diensteigenschaften anzuzeigen. - Knoten, auf dem der Dienstprozess ausgeführt wird. Klicken Sie auf den Namen des Knotens, um die Knoteneigenschaften anzuzeigen. - Status des Knotens, auf dem der Dienstprozess ausgeführt wird. - Status des Dienstprozesses.
Dienst, der in einem Gitter ausgeführt wird	Im Detailbereich werden die folgenden Inhalte für einen Dienst angezeigt, der in einem Gitter ausgeführt wird: <ul style="list-style-type: none"> - Dienstname und -status. Klicken Sie auf den Namen des Diensts, um die Diensteigenschaften anzuzeigen. - Knoten im Gitter. Klicken Sie auf den Namen eines Knotens, um die Knoteneigenschaften anzuzeigen. - Status der Knoten, auf denen die Dienstprozesse ausgeführt werden. - Status der Dienstprozesse.

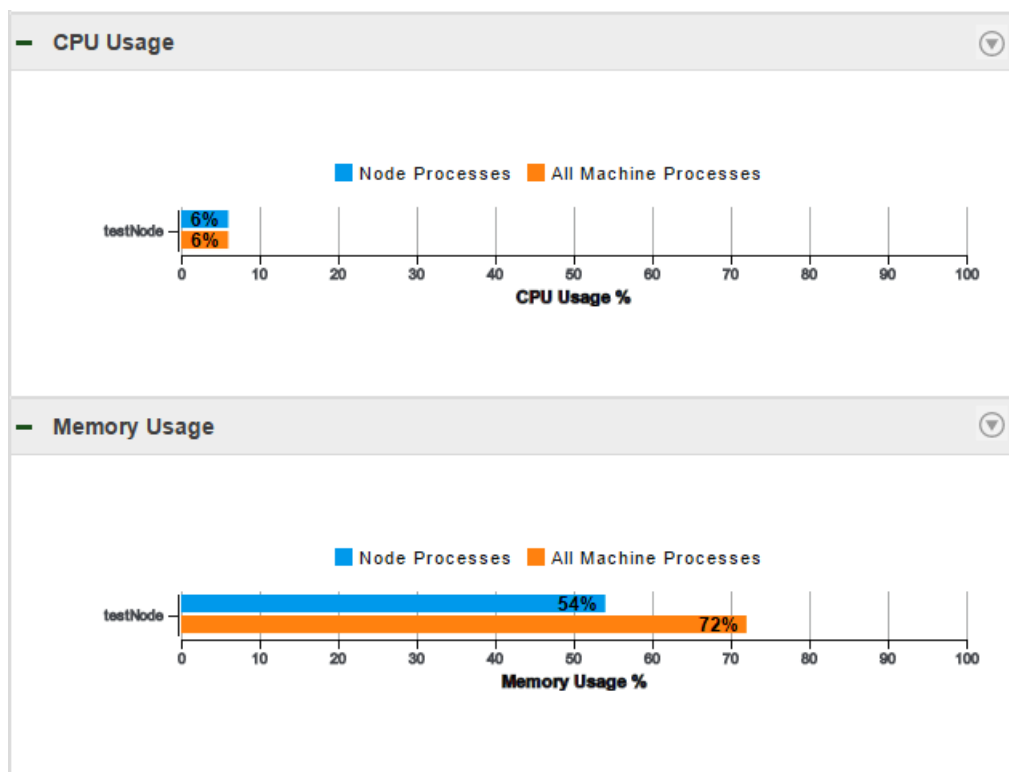
Objekt	Inhalt des Detailbereichs
Dienst im Modus „Hohe Verfügbarkeit“	<p>Im Detailbereich werden die folgenden Inhalte für einen Dienst angezeigt, der hochverfügbar ist:</p> <ul style="list-style-type: none"> - Dienstname und -status. Klicken Sie auf den Namen des Diensts, um die Diensteeigenschaften anzuzeigen. - Knoten, auf denen der Dienst gemäß Konfiguration ausgeführt werden soll. Klicken Sie auf den Namen eines Knotens, um die Knoteneigenschaften anzuzeigen. - Status der Knoten, auf denen die Dienstprozesse ausgeführt werden. - Status des Dienstprozesses auf den Knoten.
Gitter	<p>Im Detailbereich werden die folgenden Inhalte für ein Gitter angezeigt:</p> <ul style="list-style-type: none"> - Gittername und -status. Klicken Sie auf den Gitternamen, um die Gittereigenschaften anzuzeigen. - Knoten im Gitter. Klicken Sie auf den Namen eines Knotens, um die Knoteneigenschaften anzuzeigen. - Status der Knoten, die im Gitter ausgeführt werden.

Ressourcennutzungsanzeigen

Die Ressourcennutzungsanzeigen sind Balkendiagramme zum Vergleichen der Ressourcennutzung für einen Domänenprozess mit der Ressourcennutzung aller Prozesse auf dem Computer. Wählen Sie einen Domänenprozess zum Vergleichen mit allen Prozessen aus. Sie können die aktuelle Nutzungsstatistik oder die Statistik für die vergangenen 60 Minuten anzeigen.

Sie können die Nutzungsstatistik für den Speicher und die CPU anzeigen. Wählen Sie aus, ob Sie die aktuelle Statistik oder Diagramme zur Nutzung für die vergangenen 60 Minuten anzeigen möchten. Klicken Sie auf den Auswahlpfeil und wählen Sie **Aktuell** oder **Trend der letzten Stunde** aus.

Die folgende Abbildung zeigt die aktuelle Ressourcennutzung in einer Domäne mit einem Knoten:



Die in den Diagrammen angezeigten Informationen basieren auf dem von Ihnen ausgewählten Domänenobjekt.

In der folgenden Tabelle werden die Informationen beschrieben, die Sie bei der Auswahl der Domäne bzw. eines Domänenobjekts anzeigen können:

Domänenobjekt	Inhalt der Nutzungsanzeige
Domäne	In den Nutzungsanzeigen werden folgende Inhalte angezeigt: <ul style="list-style-type: none"> - Knoten in der Domäne. - Ressourcennutzung aller Prozesse, die auf den einzelnen Knoten in der Domäne ausgeführt werden. - Ressourcennutzung aller Prozesse, die auf dem Computer ausgeführt werden.
Knoten	In den Nutzungsanzeigen werden folgende Inhalte angezeigt: <ul style="list-style-type: none"> - Der Knoten. - Ressourcennutzung der Prozesse, die auf dem Knoten ausgeführt werden. - Ressourcennutzung aller Prozesse, die auf dem Computer ausgeführt werden.
Dienst	In den Nutzungsanzeigen werden folgende Inhalte angezeigt: <ul style="list-style-type: none"> - Der Knoten, auf dem der Dienstprozess ausgeführt wird. - Ressourcennutzung des Dienstprozesses, der auf dem Knoten ausgeführt wird. - Ressourcennutzung aller Prozesse, die auf dem Computer ausgeführt werden.
Dienst im Modus „Hohe Verfügbarkeit“	In den Nutzungsanzeigen werden folgende Inhalte angezeigt: <ul style="list-style-type: none"> - Den Knoten, auf dem der Dienstprozess ausgeführt wird. - Ressourcennutzung des Dienstprozesses, der auf dem Knoten ausgeführt wird. - Ressourcennutzung aller Prozesse, die auf dem Computer ausgeführt werden.
Dienst, der in einem Gitter ausgeführt wird	In den Nutzungsanzeigen werden folgende Inhalte angezeigt: <ul style="list-style-type: none"> - Alle Knoten, auf denen der Dienstprozess ausgeführt wird. - Ressourcennutzung des Dienstprozesses, der auf dem jeweiligen Knoten ausgeführt wird. - Ressourcennutzung aller Prozesse, die auf dem Computer ausgeführt werden.
Gitter	In den Nutzungsanzeigen werden folgende Inhalte angezeigt: <ul style="list-style-type: none"> - Alle verfügbaren Knoten im Gitter. - Ressourcennutzung aller Prozesse, die auf den einzelnen Knoten in der Domäne ausgeführt werden. - Ressourcennutzung aller Prozesse, die auf dem Computer ausgeführt werden.

Wenn in der Anzeige die Verknüpfung **Weitere anzeigen...** eingeblendet wird, können Sie darauf klicken, um die vollständige Liste der Knoten in der Domäne anzuzeigen. Sie können die Liste nach Knotennamen, Prozessnutzung auf den Knoten oder Prozessnutzung auf dem Computer sortieren. Außerdem können Sie in der Liste nach einem bestimmten Knoten suchen.

Registerkarte „Verwalten“ - Ansicht „Dienste und Knoten“

In der Ansicht **Dienste und Knoten** werden alle in der Domäne definierten Anwendungsdienste und Knoten angezeigt.

Die Ansicht **Dienste und Knoten** hat folgende Komponenten:

Navigator

Wird auf der linken Seite der Registerkarte **Verwalten** angezeigt. Der Navigator zeigt die folgenden Objekttypen an:

- Domäne. Sie können eine Domäne anzeigen, die das höchste Objekt in der Navigator-Hierarchie darstellt.
- Ordner. Ordner sind zum Organisieren von Domänenobjekten im Navigator bestimmt. Wählen Sie einen Ordner aus, um Informationen über den Ordner und die Objekte im Ordner anzuzeigen.
- Anwendungsdienste Ein Anwendungsdienst stellt serverbasierte Funktionalität dar. Wählen Sie einen Anwendungsdienst aus, um Informationen über den Dienst und dessen Prozesse anzuzeigen.
- System_Services. Ein Systemdienst ist ein Anwendungsdienst, der in der Domäne eine einzelne Instanz haben kann. Wählen Sie einen Systemdienst aus, um Informationen über den Dienst und dessen Prozesse anzuzeigen.
- Knoten. Bei einem Knoten handelt es sich um einen Computer in der Domäne. Sie können Dienstprozesse so konfigurieren, dass sie auf Knoten mit der Dienstrolle ausgeführt werden.
- Gitter. Erstellen Sie ein Gitter, um den Data Integration Service oder PowerCenter Integration Service auf mehreren Knoten auszuführen. Wählen Sie ein Gitter, um zu sehen, welche Knoten dem Gitter zugewiesen sind.
- Lizenzen. Erstellen Sie auf der Registerkarte **Verwalten** basierend auf der von Informatica zur Verfügung gestellten Lizenzschlüsseldatei eine Lizenz. Wählen Sie eine Lizenz aus, um zu sehen, welche Dienste der Lizenz zugewiesen sind.

Sie können im Navigator nach Knoten, Diensten und Gittern suchen.

Inhaltsübersicht

Wird auf der rechten Seite der Registerkarte **Verwalten** angezeigt und enthält Informationen über die Domäne oder Domänenobjekte, die Sie im Navigator ausgewählt haben.

Menü "Aktionen" im Navigator

Beim Auswählen der Domäne im Navigator können Sie einen Ordner, einen Dienst, einen Knoten, ein Gitter oder eine Lizenz erstellen.

Wenn Sie ein Domänenobjekt im Navigator auswählen, können Sie das Objekt löschen, es in einen Ordner verschieben, oder das Objekt aktualisieren.

Menü „Aktionen“ auf der Registerkarte „Verwalten“

Wenn Sie die Domäne im Navigator auswählen, können Sie die Domäne herunterfahren oder Protokolle für sie anzeigen.

Wenn Sie einen Knoten im Navigator auswählen, können Sie eine Knotenzuordnung entfernen, den Benchmark des CPU-Profiles neu berechnen oder den Knoten herunterfahren.

Wenn Sie einen Dienst im Navigator auswählen, können Sie den Dienst wiederherstellen oder deaktivieren und Eigenschaften für ihn konfigurieren.

Wenn Sie eine Lizenz im Navigator auswählen, können Sie der Lizenz einen inkrementellen Schlüssel hinzufügen.

Navigatorsuche

Sie können nach Knoten, Anwendungsdiensten und Gittern im Navigator suchen und danach filtern.

Sie können die folgenden Aufgaben im Suchbereich des Navigators ausführen:

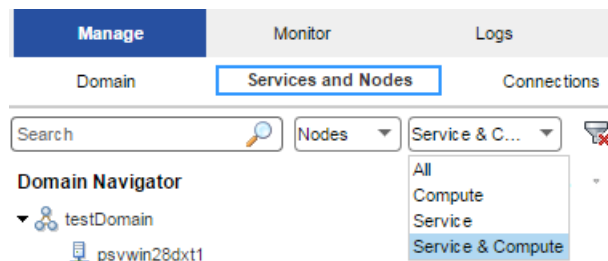
Nach Objektname suchen.

Geben Sie im Suchtextfeld den Namen des Objekts, das Sie suchen möchten, vollständig oder teilweise ein. Im Navigator werden die Suchergebnisse angezeigt.

Nach Objekttyp filtern.

Klicken Sie auf **Filter** und wählen Sie anschließend den Objekttyp aus, nach dem Sie filtern möchten. Wenn Sie nach Knoten filtern, können Sie den Filter nach Knotenrolle weiter einschränken. Wenn Sie nach Diensten filtern, können Sie den Filter nach Diensttyp weiter einschränken. Im Navigator werden die gefilterten Ergebnisse angezeigt.

Die folgende Abbildung zeigt den nach Knoten gefilterten Suchbereich im Navigator mit den Dienst- und Berechnungsrollen:



Filter zurücksetzen.

Klicken Sie auf **Filter zurücksetzen**, um jeglichen Filter und jeglichen eingegebenen Suchtext zu löschen.

Domäne

Sie können auf der Registerkarte **Verwalten** in der Ansicht **Dienste und Knoten** eine Domäne anzeigen. Hierbei handelt es sich um das höchste Objekt in der Navigator-Hierarchie.

Wenn Sie die Domäne im Navigator auswählen, werden im Inhaltsbereich die folgenden Ansichten und Schaltflächen angezeigt:

- Ansicht **Eigenschaften**. Anzeigen oder Bearbeiten der Domänen-Belastbarkeitseigenschaften.
- Ansicht **Ressourcen**. Anzeigen der verfügbaren Ressourcen für jeden Knoten in der Domäne.
- Ansicht **Berechtigungen**. Anzeigen oder Bearbeiten der Gruppen- und Benutzerberechtigungen für die Domäne.
- **Ansicht Diagnostik**. Anzeigen der Knotendiagnostik, Generieren und Hochladen der Knotendiagnostik auf den Customer Support Manager oder Bearbeiten der Anmeldedaten für das Kundenportal.
- Ansicht **Plug-Ins**. In der Domäne registrierte Plug-Ins anzeigen.
- Schaltfläche **Domänenprotokolle anzeigen**. Anzeigen von Protokollen für die Domäne und Dienste in der Domäne.

Im Menü **Aktionen** im Navigator können Sie der Domäne einen Ordner, einen Knoten, ein Gitter, einen Anwendungsdienst oder eine Lizenz hinzufügen.

Im Menü **Aktionen** auf der Registerkarte **Verwalten** können Sie die Domäne herunterfahren, Protokolle anzeigen oder auf die Hilfe für die aktuelle Ansicht zugreifen.

Ordner

Sie können die Ordner in einer Domäne dazu verwenden, die Sicherheit zu organisieren.

Die Ordner können Knoten, Dienste, Gitter, Lizenzen und andere Ordner enthalten.

Wenn Sie im Navigator einen Ordner wählen, wird der Navigator geöffnet und zeigt die Objekte im Ordner an. Der Inhaltsbereich zeigt die folgenden Informationen an:

- Ansicht **Eigenschaften**. Zeigt den Namen und die Beschreibung des Ordners an.
- Ansicht **Berechtigungen**. Dient zum Bearbeiten von Gruppen und Benutzerberechtigungen in dem Ordner.

Im Menü **Aktionen** im Navigator können Sie den Ordner löschen, in einen anderen Ordner verschieben, die Inhalte auf der Registerkarte **Verwalten** aktualisieren oder Hilfe zur aktuellen Registerkarte anzeigen.

Hinweis: Der Ordner System_Services wird bei Erstellung der Domäne für Sie erstellt und enthält alle Systemdienste. Ein Systemdienst ist ein Anwendungsdienst, der in der Domäne eine einzelne Instanz haben kann. Die Eigenschaften oder Inhalte des Ordners System_Services können nicht gelöscht, verschoben oder bearbeitet werden.

Anwendungsdienste

Bei den Anwendungsdiensten handelt es sich um eine Gruppe von Diensten, die serverbasierte Informatica-Funktionalität darstellen.

In der Ansicht **Dienste und Knoten** auf der Registerkarte **Verwalten** können Sie folgende Anwendungsdienste erstellen und verwalten:

Analyst-Dienst

Ausführen von Informatica Analyst in der Informatica-Domäne. Der Analyst-Dienst verwaltet die Verbindungen zwischen Dienstkomponenten und den Benutzern, die sich bei Informatica Analyst anmelden.

Der Analyst-Dienst stellt eine Verbindung zu einem Datenintegrationsdienst, einem Modellrepository-Dienst, einem Metadata Manager- und einem Suchdienst her. Der Analyst-Dienst gibt auch das Einfachdatei-Cache-Verzeichnis und das Einfachdatei-Netzwerkverzeichnis, ein Verzeichnis für Geschäftsglossar-Exportdateien, sowie eine Ausnahmeverwaltungs-Audit-Datenbank an.

Um auf das Analyst Tool zuzugreifen, können Sie den Analyst-Dienst in der Informatica-Domäne erstellen und recyceln. Die können das Analyst Tool aus dem Administrator Tool heraus starten.

Wenn Sie im Navigator einen Analyst-Dienst auswählen, werden in der Inhaltsangabe folgende Informationen angezeigt:

- Ansicht **Eigenschaften**. Anzeigen des Dienststatus und der URL für den Analyst-Dienst. Verwalten allgemeiner und benutzerdefinierter Eigenschaften sowie von Modellrepository-, Datenintegrations-, Human-Task-, Metadata Manager-, Einfachdatei-Cache-, Einfachdatei-Netzwerk-, Geschäftsglossarexport- und Protokollierungseigenschaften.
- Ansicht **Prozesse**. Anzeigen des Status des Dienstprozesses auf jedem Knoten. Anzeigen und Bearbeiten der Dienstprozesseigenschaften für jeden zugewiesenen Knoten.
- Ansicht **Berechtigungen**. Anzeigen und Bearbeiten von Gruppen- und Benutzerberechtigungen im Analyst-Dienst.
- Menü **Aktionen**. Verwalten der Dienst- und Repository-Inhalte.

Content-Managementdienst

Verwaltet Referenzdaten und kompiliert Regelspezifikationen in Mapplets.

Wenn Sie im Navigator einen Content-Managementdienst auswählen, werden in der Inhaltsangabe folgende Informationen eingeblendet:

- Ansicht **Eigenschaften**. Anzeigen des Dienststatus. Verwalten allgemeiner und benutzerdefinierter Eigenschaften sowie von Master-, Datenintegrations-, Modellrepository-, Referenztabellendaten-, temporären Datei- und Protokollierungseigenschaften.
- Ansicht **Prozesse** Anzeigen des Status des Dienstprozesses auf jedem Knoten. Anzeigen und Bearbeiten der Dienstprozesseigenschaften für jeden zugewiesenen Knoten.
- Ansicht **Berechtigungen**. Anzeigen und Bearbeiten von Gruppen- und Benutzerberechtigungen im Content-Managementdienst.
- Menü **Aktionen** Dienstverwaltung.

Datenintegrationsdienst

Der Datenintegrationsdienst führt Datenintegrationsaufgaben für Informatica Analyst, Informatica Developer und externe Clients durch. Bei der Vorschau oder Ausführung von Datenprofilen, SQL-Datendiensten und Mappings im Informatica Analyst oder Informatica Developer überträgt die Anwendung Anfragen zur Ausführung der Datenintegrationsaufgaben zum Datenintegrationsdienst. Wenn Sie einen Befehl aus der Befehlszeile oder einem externen Client zum Ausführen von SQL-Datendiensten und Mappings in einer Anwendung starten, überträgt der Befehl die Anfrage zum Datenintegrationsdienst.

Beim Auswählen eines Datenintegrationsdiensts im Navigator stehen in der Inhaltsangabe folgende Informationen:

- Ansicht **Eigenschaften**. Anzeigen des Dienststatus. Verwalten allgemeiner, Modellrepository-, Protokollierungs-, logischer Datenobjekt- und virtueller Tabellen-Cache-, Profiling-, Datenobjekt-Cache- und benutzerdefinierter Eigenschaften. Einrichten der standardmäßigen Bereitstellungsoption.
- Ansicht **Prozesse** Anzeigen des Status des Dienstprozesses auf jedem Knoten. Anzeigen und Bearbeiten der Dienstprozesseigenschaften für jeden zugewiesenen Knoten.
- Ansicht **Anwendungen**. Starten und Anhalten von Anwendungen und SQL-Datendiensten. Sicherungsanwendungen Verwalten von Anwendungseigenschaften.
- Menü **Aktionen** Verwalten der Dienst- und Repository-Inhalte.

Metadaten-Zugriffsdienst

Ermöglicht dem Developer Tool den Zugriff auf Hadoop-Verbindungsinformationen zum Importieren von Metadaten und Anzeigen dieser Daten in der Vorschau. Beim Importieren eines Datenobjekts sendet das Developer Tool eine Anforderung an den Metadaten-Zugriffsdienst.

Wenn Sie im Navigator einen Metadaten-Zugriffsdienst auswählen, werden in der Inhaltsübersicht folgende Informationen angezeigt:

- Ansicht **Eigenschaften**. Anzeigen des Dienststatus. Verwalten von allgemeinen und benutzerdefinierten Eigenschaften sowie von Ausführungs- und HTTP-Konfigurationseigenschaften.
- Ansicht **Prozesse** Anzeigen des Status des Dienstprozesses auf jedem Knoten. Anzeigen und Bearbeiten der Dienstprozesseigenschaften für jeden zugewiesenen Knoten.
- Ansicht **Berechtigungen**. Anzeigen oder Bearbeiten von Gruppen- und Benutzerberechtigungen im Metadaten-Zugriffsdienst.
- Menü **Aktionen** Dienstverwaltung.

Metadata Manager-Dienst

Der Metadata Manager-Dienst führt die Metadata Manager-Anwendung aus und verwaltet Verbindungen zwischen den Metadata Manager-Komponenten.

Wenn Sie im Navigator einen Metadata Manager-Dienst auswählen, werden in der Inhaltsangabe folgende Informationen angezeigt:

- Ansicht **Eigenschaften**. Anzeigen des Dienststatus und der URL der Metadata Manager-Dienstinstanz. Anzeigen oder Bearbeiten der Metadata Manager Eigenschaften.
- Ansicht **Zugeordnete Dienste**. Anzeigen und Konfigurieren zugehörigen Integration Service für den Metadata Manager-Dienst.
- Ansicht **Berechtigungen**. Anzeigen oder Bearbeiten von Gruppen- und Benutzerberechtigungen im Metadata Manager-Dienst.
- Menü **Aktionen** Verwalten der Dienst- und Repository-Inhalte.

Modellrepository-Dienst

Verwaltet das Modellrepository. Das Modellrepository speichert von Informatica-Produkten (z. B. Informatica Developer, Informatica Analyst, dem Datenintegrationsdienst und Informatica Administrator) erstellte Metadaten. Das Modellrepository ermöglicht die Zusammenarbeit zwischen den Produkten.

Beim Auswählen eines Modellrepository-Dienst im Navigator werden in der Inhaltsübersicht folgende Informationen angezeigt:

- Ansicht **Eigenschaften**. Anzeigen des Dienststatus. Verwalten allgemeiner, Repository-Datenbank-, Such- und benutzerdefinierter Eigenschaften.
- Ansicht **Prozesse**. Anzeigen des Status des Dienstprozesses auf jedem Knoten. Anzeigen und Bearbeiten der Dienstprozesseigenschaften für jeden zugewiesenen Knoten.
- Menü **Aktionen**. Verwalten der Dienst- und Repository-Inhalte.

Sie können ein Modellrepository als Überwachungsmodellrepository konfigurieren. Sie können einen Überwachungsmodellrepository-Dienst auf Domänenebene konfigurieren, um mehrere Datenintegrationsdienste und die Objekte zu überwachen, die vom Datenintegrationsdienst ausgeführt werden.

PowerCenter-Integrationsdienst

Ausführen von PowerCenter-Sitzungen und -Arbeitsabläufen. Wählen Sie einen PowerCenter-Integrationsdienst im Navigator aus, um auf Informationen über den Dienst zugreifen zu können.

Beim Auswählen eines PowerCenter-Integrationsdiensts im Navigator werden in der Inhaltsübersicht folgende Informationen angezeigt:

- Ansicht **Eigenschaften**. Anzeigen des Dienststatus. Anzeigen oder Bearbeiten der Eigenschaften des Integration Service.
- Ansicht **Zugeordnetes Repository**. Anzeigen oder Bearbeiten des zum Integration Service gehörenden Repository.
- Ansicht **Prozesse**. Anzeigen des Status des Dienstprozesses auf jedem Knoten. Anzeigen oder Bearbeiten der Dienstprozesseigenschaften für jeden zugewiesenen Knoten.
- Ansicht **Berechtigungen**. Anzeigen oder Bearbeiten von Gruppen- und Benutzerberechtigungen für den Integration Service.
- Menü **Aktionen** Dienstverwaltung.

PowerCenter-Repository-Dienst

Verwaltet das PowerCenter-Repository. Er ruft Metadaten ab, fügt sie in die Datenbanktabellen des Repositories ein und aktualisiert sie. Wählen Sie einen PowerCenter-Repository-Dienst im Navigator aus, um auf Informationen über den Dienst zugreifen zu können.

Beim Auswählen eines PowerCenter-Repository-Diensts im Navigator werden in der Inhaltsübersicht folgende Informationen angezeigt:

- Ansicht **Eigenschaften**. Anzeigen des Status und des Betriebsmodus des Diensts. Verwalten allgemeiner und erweiterter Eigenschaften, Knotenzuweisungen und Datenbankeigenschaften.
- Ansicht **Prozesse**. Anzeigen des Status des Dienstprozesses auf jedem Knoten. Anzeigen und Bearbeiten der Dienstprozesseigenschaften für jeden zugewiesenen Knoten.
- **Ansicht Verbindungen und Sperren**. Anzeigen und Beenden der Repository-Verbindungen und Objektsperren.
- Ansicht **Plug-Ins**. Anzeigen und Verwalten der registrierten Plug-ins.
- Ansicht **Berechtigungen**. Anzeigen oder Bearbeiten von Gruppen- und Benutzerberechtigungen für den PowerCenter-Repository-Dienst.
- Menü **Aktionen**. Verwalten der Repository-Inhalte und Durchführen anderer administrativer Aufgaben.

PowerExchange-Listenerdienst

Ausführen des PowerExchange Listener.

Beim Auswählen eines Listener Service im Navigator werden in der Inhaltsangabe folgende Informationen angezeigt:

- Ansicht **Eigenschaften**. Anzeigen des Dienststatus und der URL der PowerExchange-Listenerinstanz. Anzeigen oder Bearbeiten der Eigenschaften für den Listener Service.
- Menü **Aktionen**. Enthält Aktionen, die Sie mit dem Listener Service durchführen können, zum Beispiel Anzeigen von Protokollen oder Aktivieren und Deaktivieren des Dienstes.

PowerExchange-Protokollierungsdienst

Ausführen des PowerExchange Logger für Linux, UNIX und Windows.

Beim Auswählen eines Logger Service im Navigator werden in der Inhaltsübersicht folgende Informationen angezeigt:

- Ansicht **Eigenschaften**. Anzeigen des Dienststatus und der URL der PowerExchange-Protokollierungsinstanz. Anzeigen oder Bearbeiten der Logger Service Eigenschaften.
- Menü **Aktionen**. Enthält Aktionen, die Sie mit dem Logger Service ausführen können, wie Anzeigen der Protokolle oder Aktivieren und Deaktivieren des Dienstes.

SAP BW-Dienst

Wartet auf RFC-Anfragen von SAP BW und initiiert Arbeitsabläufe zum Extrahieren von oder Laden in SAP BW. Durch Auswählen eines SAP BW-Diensts im Navigator erhalten Sie Zugriff auf Eigenschaften und andere Informationen über den Dienst.

Beim Auswählen eines SAP BW-Diensts im Navigator werden in der Inhaltsübersicht folgende Informationen angezeigt:

- Ansicht **Eigenschaften**. Anzeigen des Dienststatus. Verwalten allgemeiner Eigenschaften und Knotenzuweisungen.
- Ansicht **Zugeordneter Integration Service**. Anzeigen oder Bearbeiten des dem SAP BW-Dienst zugewiesenen Integration Service.
- Ansicht **Prozesse**. Anzeigen des Status des Dienstprozesses auf jedem Knoten. Anzeigen oder Bearbeiten des Verzeichnisses für die Parameterdatei BWParam.
- Ansicht **Berechtigungen**. Anzeigen oder Bearbeiten von Gruppen- und Benutzerberechtigungen für den SAP BW-Dienst.

- Menü **Aktionen** Dienstverwaltung.

Webdienst-Hub

Ein Web-Dienst-Gateway für externe Clients. Er verarbeitet SOAP-Anfragen von Web-Dienst-Clients, die über Web-Dienste auf die PowerCenter-Funktionalität zugreifen möchten. Web-Dienst-Clients greifen über den Webdienst-Hub auf den PowerCenter-Integrationsdienst und den PowerCenter-Repository-Dienst zu.

Beim Auswählen eines Webdienst-Hubs im Navigator werden in der Inhaltsübersicht folgende Informationen eingeblendet:

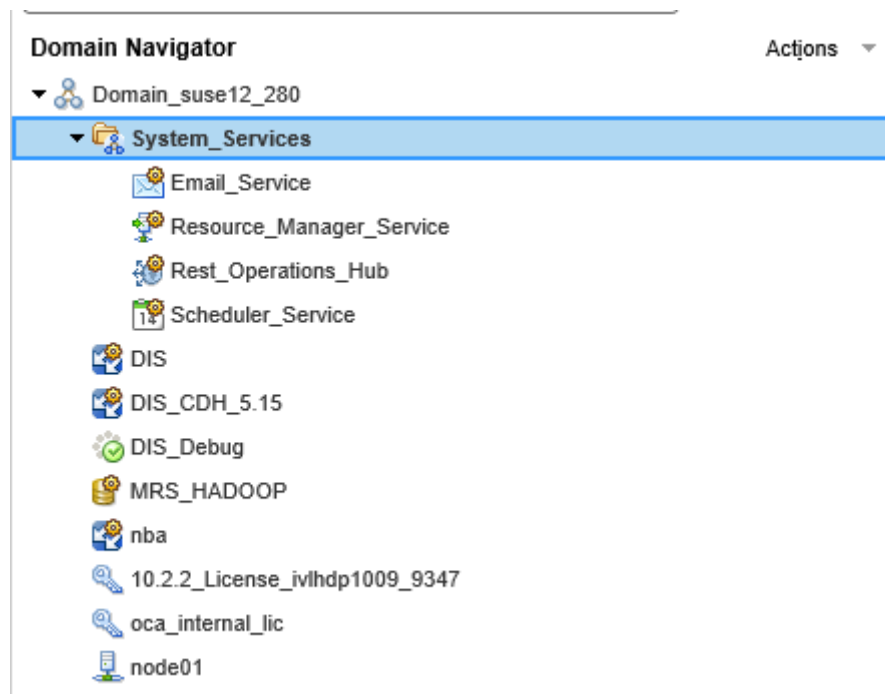
- Ansicht **Eigenschaften**. Anzeigen des Dienststatus. Anzeigen oder Bearbeiten der Eigenschaften des Webdienst-Hubs
- Ansicht **Zugeordnetes Repository**. Anzeigen der zum Webdienst-Hub gehörenden PowerCenter-Repository-Dienste.
- Ansicht **Berechtigungen**. Anzeigen oder Bearbeiten von Gruppen- und Benutzerberechtigungen für den Webdienst-Hub.
- Menü **Aktionen** Dienstverwaltung.

Systemdienste

Ein Systemdienst ist ein Anwendungsdienst, der in der Domäne eine einzelne Instanz aufweisen kann. Die Systemdienste werden beim Erstellen der Domäne angelegt. Sie können Systemdienste aktivieren, deaktivieren und konfigurieren.

Sie können Systemdienste auf der Registerkarte **Verwalten** in der Ansicht **Dienste und Knoten** verwalten.

Die folgende Abbildung zeigt den Ordner „Systemdienste“ im Domänennavigator:



Sie können die folgenden Systemdienste verwalten:

E-Mail-Dienst

Der E-Mail-Dienst sendet E-Mail-Benachrichtigungen für Unternehmensglossare, Scorecards und Arbeitsabläufe. Aktivieren Sie den E-Mail-Dienst, damit Benutzer E-Mail-Benachrichtigungen konfigurieren können.

Wenn Sie im Navigator im Ordner „Systemdienste“ auf „E-Mail-Dienst“ klicken, werden im Inhaltsbereich die folgenden Ansichten und Schaltflächen angezeigt:

- Ansicht **Eigenschaften**. Anzeigen des Dienststatus. Verwalten der Modellrepository-Optionen und der E-Mail-Server-Eigenschaften für den Dienst.
- Ansicht **Prozesse**. Anzeigen des Status des Dienstprozesses für jeden zugewiesenen Knoten.
- Ansicht **Berechtigungen**. Anzeigen und Bearbeiten der Gruppen- und Benutzerberechtigungen im Dienst.
- Menü **Aktionen** Dienstverwaltung.

Ressourcenmanager-Dienst

Der Ressourcenmanager-Dienst verwaltet Rechenressourcen in der Domäne und versendet Jobs, um optimale Leistung und Skalierbarkeit zu erreichen. Der Ressourcenmanager-Dienst sammelt Informationen über Knoten mit der Berechnungsrolle. Der Dienst gleicht die Jobanforderungen mit der Ressourcenverfügbarkeit ab und ermittelt so den besten Berechnungsknoten für die Ausführung des Jobs.

Der Ressourcenmanager-Dienst kommuniziert mit Berechnungsknoten in einem Datenintegrationsdienstgitter. Aktivieren Sie den Ressourcenmanager-Dienst, wenn Sie ein Datenintegrationsdienstgitter für die Ausführung von Jobs in separaten Remoteprozessen konfigurieren.

Wenn Sie im Navigator im Ordner „Systemdienste“ auf „Ressourcenmanager-Dienst“ klicken, werden im Inhaltsbereich die folgenden Ansichten und Schaltflächen angezeigt:

- Ansicht **Eigenschaften**. Anzeigen des Dienststatus. Verwalten der Protokollebene sowie der primären Knoten und Sicherungsknoten für den Dienst.
- Ansicht **Prozesse**. Anzeigen des Status des Dienstprozesses für jeden zugewiesenen Knoten.
- Ansicht **Berechtigungen**. Anzeigen und Bearbeiten der Gruppen- und Benutzerberechtigungen im Dienst.
- Menü **Aktionen**. Dienstverwaltung.

REST Operations Hub-Dienst

Der REST Operations Hub-Dienst ist ein Anwendungsdienst in der Informatica-Domäne, der externen Clients über REST-APIs Informatica-Produktfunktionalität zur Verfügung stellt.

Scheduler-Dienst

Der Scheduler-Dienst verwaltet Zeitpläne für Profile, Scorecards, bereitgestellte Mappings und bereitgestellte Arbeitsabläufe. Aktivieren Sie den Scheduler-Dienst zum Erstellen, Verwalten und Ausführen von Zeitplänen.

Wenn Sie im Navigator im Ordner „Systemdienste“ auf „Scheduler-Dienst“ klicken, werden im Inhaltsbereich die folgenden Ansichten und Schaltflächen angezeigt:

- Ansicht **Eigenschaften**. Anzeigen des Dienststatus. Verwalten der Protokollebene, der primären Knoten und Backup-Knoten sowie der Modellrepository-Dienstoptionen für den Dienst.
- Ansicht **Prozesse**. Anzeigen des Status des Dienstprozesses für jeden zugewiesenen Knoten und Konfigurieren von Prozesseigenschaften.

- Ansicht **Berechtigungen**. Anzeigen und Bearbeiten der Gruppen- und Benutzerberechtigungen im Dienst.
- Menü **Aktionen** Dienstverwaltung.

Knoten

Ein Knoten ist eine logische Darstellung eines physischen Computers in der Domäne. Auf der Registerkarte „Verwalten“ in der Ansicht „Dienste und Knoten“ weisen Sie den Knoten Ressourcen zu und konfigurieren Dienstprozesse, die auf den Knoten mit Dienstrolle ausgeführt werden.

Wenn Sie einen Knoten im Navigator auswählen, erscheinen im Inhaltsbereich folgende Informationen:

- **Eigenschaftensicht** Anzeige des Status des Knotens. Anzeigen oder Bearbeiten der Knoteneigenschaften, wie z. B. Repository-Backup-Verzeichnis oder Bereich von Portnummern für die Prozesse, die auf dem Knoten ausgeführt werden.
- Ansicht **Prozesse** Anzeigen des Status aller Prozesse, die zur Ausführung auf dem Knoten konfiguriert sind. Dienstprozesse werden auf Knoten mit der Dienstrolle ausgeführt.
- Ansicht **Ressourcen**. Anzeigen oder Bearbeiten der dem Knoten zugeordneten Ressourcen.
- **Berechtigungen**-Ansicht. Anzeigen oder Bearbeiten von Gruppen- und Benutzerberechtigungen für den Knoten.

Im Menü **Aktionen** im Navigator können Sie den Knoten löschen, ihn in einen Ordner verschieben, den Inhalt auf der Registerkarte **Verwalten** aktualisieren oder die Hilfe zur aktuellen Registerkarte öffnen.

Im Menü **Aktionen** auf der Registerkarte **Verwalten** können Sie die Knotenzuordnung löschen, das CPU-Profil-Benchmark neu berechnen oder den Knoten herunterfahren.

Gitter

Ein Gitter ist ein Alias für eine Gruppe von Knoten, auf denen PowerCenter-Integrationsdienst- oder Datenintegrationsdienst-Jobs ausgeführt werden.

Wenn Sie einen Job auf einem Gitter ausführen, verteilt der Integration Service die Verarbeitung über mehrere Knoten im Gitter. Wenn Sie zum Beispiel ein Profil auf einem Gitter ausführen, teilt der Datenintegrationsdienst die Arbeit in mehrere Jobs und weist jeden Job zu einem Knoten im Gitter zu. Sie weisen die Knoten einem Gitter in der Ansicht **Dienste und Knoten** auf der Registerkarte **Verwalten** zu.

Wenn Sie ein Gitter im Navigator auswählen, erscheinen im Inhaltsbereich folgende Informationen:

- Ansicht **Eigenschaften**. Hier können Sie die Knotenzuweisungen an ein Gitter anzeigen oder bearbeiten.
- Ansicht **Berechtigungen**. Hier können Sie die Gruppen- und Benutzerberechtigungen in einem Gitter anzeigen oder bearbeiten.

Im Menü **Aktionen** des Navigators können Sie das Gitter löschen, das Gitter in einen Ordner verschieben, die Inhalte auf der Registerkarte **Verwalten** aktualisieren oder Hilfe zur aktuellen Registerkarte anzeigen.

Lizenzen

Die Erstellung eines Lizenzobjekts auf der Registerkarte **Verwalten** erfordert eine von Informatica zur Verfügung gestellte Lizenzschlüsseldatei.

Nachdem Sie eine Lizenz erstellt haben, können Sie ihr Dienste zuordnen.

Beim Auswählen einer Lizenz im Navigator werden in der Inhaltsübersicht folgende Informationen eingeblendet:

- Ansicht **Eigenschaften**. Sie können Lizenzeigenschaften wie beispielsweise unterstützte Plattformen, Repositorys und lizenzierte Optionen anzeigen. Außerdem können Sie die Lizenzbeschreibung bearbeiten.
- Ansicht **Zugeordnete Dienste**. Anzeigen oder Bearbeiten der Dienste, die der Lizenz zugeordnet sind.
- **Ansicht Optionen**. Anzeigen der lizenzierten PowerCenter-Optionen.
- **Berechtigungen**-Ansicht. Anzeigen oder Bearbeiten von Benutzerberechtigungen für die Lizenz.

Im Menü **Aktionen** im Navigator können Sie die Lizenz löschen, in einen Ordner verschieben, den Inhalt auf der Registerkarte **Verwalten** aktualisieren oder auf die Hilfe für die aktuelle Registerkarte zugreifen.

Im Menü **Aktionen** auf der Registerkarte **Verwalten** können Sie einer Lizenz einen inkrementellen Schlüssel hinzufügen.

Registerkarte „Verwalten“ – Verbindungsansicht

Die Ansicht **Verbindungen** zeigt die Domäne und alle Verbindungen in der Domäne.

Die Ansicht **Verbindungen** hat folgende Komponenten:

Navigator

Zeigt die Domäne und die Verbindungen in der Domäne an.

Menü Aktionen im Navigator

Wenn Sie die Domäne im Navigator auswählen, können Sie eine Verbindung erstellen.

Wählen Sie eine Verbindung im Navigator, können Sie die Verbindung löschen.

Inhaltsübersicht

Zeigt Informationen über die Domäne oder die Verbindung an, die Sie im Navigator auswählen.

Wenn Sie die Domäne im Navigator auswählen, enthält die Inhaltsübersicht alle Verbindungen in der Domäne. In der Inhaltsübersicht können Sie Verbindungen filtern bzw. sortieren oder nach bestimmten Verbindungen suchen.

Wenn Sie eine Verbindung im Navigator auswählen, erscheinen im Inhaltsbereich folgende Informationen zu der Verbindung. Die Aufgaben, die Sie für die Verbindung abschließen können, hängt davon ab, welche der folgenden Ansichten Sie auswählen:

- Ansicht **Eigenschaften**. Anzeigen oder Bearbeiten von Eigenschaften.
- Ansicht **Pooling**. Anzeigen oder Bearbeiten von Pooling-Eigenschaften für die Verbindung.
- Ansicht **Berechtigungen**. Anzeigen oder Bearbeiten von Gruppen- oder Benutzerberechtigungen für die Verbindung.

Menü „Aktionen“ auf der Registerkarte „Verwalten“

Wenn Sie eine Verbindung im Navigator auswählen, können Sie die Verbindung testen.

Registerkarte „Verwalten“ - Ansicht „Pläne“

In der Ansicht **Pläne** können Sie Zeitpläne für bereitgestellte Mappings und Arbeitsabläufe anzeigen und verwalten.

Die Ansicht **Pläne** enthält folgende Komponenten:

Navigator

Zeigt die Domäne und die Zeitpläne in der Domäne an.

Ansicht „Alle Zeitpläne“

Wenn Sie im Navigator die Domäne auswählen, werden in der Ansicht **Alle Zeitpläne** der Name, der Status und die Beschreibung der Zeitpläne in der Domäne angezeigt.

Ansicht „Eigenschaften“

Wenn Sie im Navigator einen Zeitplan auswählen, werden in der Ansicht **Eigenschaften** Details zu dem Zeitplan angezeigt.

Ansicht „Geplante Aufträge“

Wenn Sie im Navigator die Domäne auswählen, werden in der Ansicht **Geplante Aufträge** Details zu den geplanten Jobs in der Domäne angezeigt.

Wenn Sie im Navigator einen Zeitplan auswählen, werden in der Ansicht **Geplante Aufträge** Details zu den Jobs angezeigt, die in diesem Zeitplan ausgeführt werden.

Menü „Aktionen“ auf der Registerkarte „Verwalten“

Welche Aktionen Sie im Menü „Aktionen“ durchführen können, hängt von der Ansicht ab, die Sie auswählen.

Über das Menü „Aktionen“ können Sie die folgenden Aktionen durchführen:

- Erstellen eines Zeitplans
- Bearbeiten eines Zeitplans
- Löschen eines Zeitplans
- Anhalten eines Zeitplans
- Fortsetzen eines Zeitplans
- Aktualisieren
- Entfernen eines Objekts aus dem Zeitplan
- Zurücksetzen von Filtern
- Zugreifen auf die Hilfe

Registerkarte „Überwachen“

Auf der Registerkarte **Überwachen** können Sie Datenintegrationsdienste und Objekte überwachen, die von den Datenintegrationsdiensten ausgeführt werden.

Nachdem Sie das Überwachungsmodellrepository in der Domäne konfiguriert haben, können Sie die Überwachungsstatistik im Administrator Tool anzeigen.

Sie können auf der Registerkarte **Überwachen** die folgenden Objekte überwachen:

- Ad-hoc-Jobs. Dies beinhaltet Profile, Unternehmensdatenprofile, Mappings, Scorecards, Referenztabelle und Vorschauen.
- Anwendungen. Dies beinhaltet bereitgestellte Mappings, logische Datenobjekte, SQL-Datendienste, Webdienste und Arbeitsabläufe.
- SQL-Datendienstverbindungen.
- Abfragen. Dies beinhaltet SQL-Datendienst- und Webdienstanfragen.

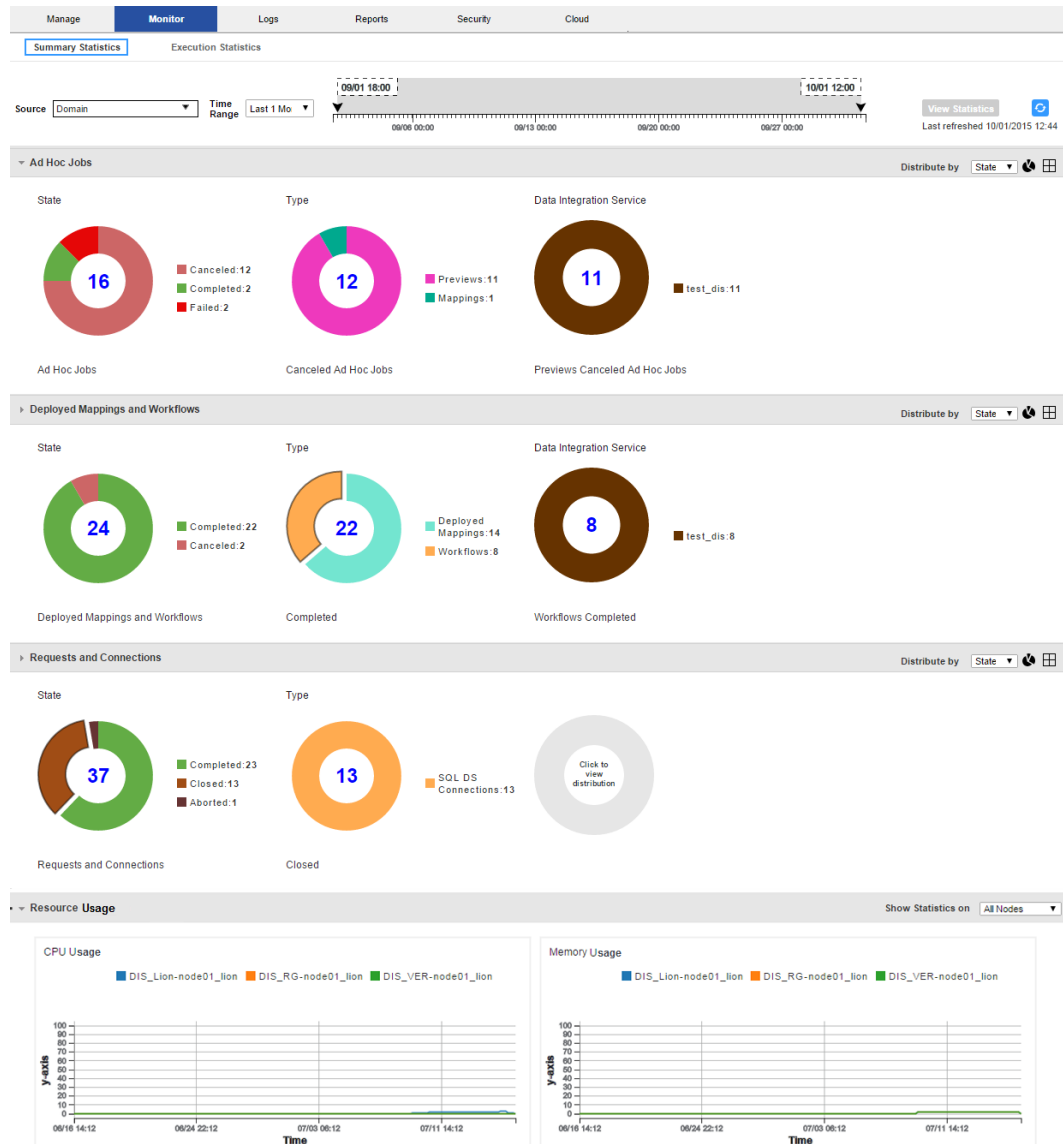
Sie können die folgenden Ansichten auswählen:

- Ansicht **Übersichtsstatistik**. Anzeigen von grafischen Informationen zum Objektstatus, zur Verteilung und zur Ressourcennutzung für alle Datenintegrationsdienste.
- Ansicht **Ausführungsstatistiken**. Anzeigen von Eigenschaften, Statistiken und Berichten für die Objekte, die vom Datenintegrationsdienst ausgeführt werden.

Registerkarte „Überwachen“ - Ansicht „Übersichtsstatistik“

In der Ansicht **Übersichtsstatistik** werden historische Statistiken zu Datenintegrationsdiensten und den von diesen ausgeführten Jobs angezeigt.

Die folgende Abbildung zeigt die Ansicht **Übersichtsstatistik**:



In der Ansicht **Übersichtsstatistik** können Sie grafische Informationen zum Objektstatus, zur Verteilung und zur Ressourcennutzung anzeigen.

Die Ansicht **Übersichtsstatistik** enthält die folgenden Komponenten:

Zeitleiste

Geben Sie eine Quelle und eine Zeitspanne an, für die Sie Statistiken anzeigen möchten.

Bereich „Ad-hoc-Jobs“

Zeigen Sie Ringdiagramme oder tabellarische Diagramme für Jobs für die ausgewählte Quelle und Zeitspanne an. Wählen Sie Abschnitte der Ringdiagramme zur Filterung nach Jobtyp, Status und Datenintegrationsdienst aus.

Bereich „Bereitgestellte Zuordnungen und Arbeitsabläufe“

Zeigen Sie Ringdiagramme oder tabellarische Diagramme für bereitgestellte Mappings und Arbeitsabläufe für die ausgewählte Quelle und Zeitspanne an. Wählen Sie Abschnitte der Ringdiagramme zur Filterung nach Typ, Status und Datenintegrationsdienst aus.

Bereich „Anfragen und Verbindungen“

Zeigen Sie Ringdiagramme oder tabellarische Diagramme für Datenintegrationsdienst-Jobs für die ausgewählte Quelle und Zeitspanne an. Wählen Sie Abschnitte der Ringdiagramme zur Filterung nach Objekttyp, Status und Datenintegrationsdienst aus.

Bereich „Ressourcennutzung“

Zeigen Sie die CPU-Nutzung und die Speichernutzung aller Datenintegrationsdienst-Prozesse an, die in der Domäne oder auf einem Knoten in der Domäne ausgeführt werden.

Registerkarte „Überwachen“ - Ansicht „Ausführungsstatistiken“

Auf der Registerkarte **Überwachen** in der Ansicht **Ausführungsstatistiken** können Sie Datenintegrationsdienste und Objekte anzeigen, die von den Datenintegrationsdiensten ausgeführt werden.

Die folgende Abbildung zeigt die Ansicht **Ausführungsstatistiken** auf der Registerkarte **Überwachen**:

Name	Type	State	Job ID	Started By	Start Time	Elapsed Time	End Time
Read_flat	Preview	Canceled	wapFh2dZee...	Administrator	09/30/2015 02:58:10	00:00:02	09/30/2015 02:58:12
Map_flat	Mapping	Canceled	tfoF32dZeeW...	Administrator	09/30/2015 02:57:50	00:00:09	09/30/2015 02:58:00
Map_flat	Mapping	Completed	NkBUEmdTE...	Administrator	09/30/2015 02:11:19	00:00:06	09/30/2015 02:11:28

General Properties	
Name	Map_flat
Type	Mapping
Started By	Administrator
User Security Domain	Native
Start Time	09/30/2015 02:57:50
Elapsed Time	00:00:09
End Time	09/30/2015 02:58:00

1. Navigator
2. Ordner
3. Menü „Aktionen“
4. Inhaltsbereich
5. Detailbereich
6. Ansichten im Detailbereich

Wenn Sie im Navigator ein Objekt auswählen, können Sie Details zu dem Objekt anzeigen und das Objekt überwachen.

Sie können die folgenden Objekttypen im Navigator der Ansicht **Ausführungsstatistiken** anzeigen:

Domäne

Anzeigen der Status und Eigenschaften der Datenintegrationsdienste in der Domäne.

Datenintegrationsdienst

Anzeigen von allgemeinen Eigenschaften zum Datenintegrationsdienst und Anzeigen von Statistiken zu Objekten, die vom Datenintegrationsdienst ausgeführt werden.

Ordner

Anzeigen einer Liste der Objekte im Ordner. Der Ordner ist eine logische Gruppierung von Objekten. Wenn Sie einen Ordner auswählen, wird eine Liste von Objekten im Inhaltsbereich angezeigt. Der Inhaltsbereich zeigt mehrere Ansichten, die verschiedene Informationen zu einem Objekt anzeigen. Sie können die im Inhaltsbereich angezeigten Spalten konfigurieren.

Die folgende Tabelle zeigt die Ordner, die im Navigator angezeigt werden:

Ordner	Speicherort
Ad-hoc-Jobs	Wird unter dem Datenintegrationsdienst angezeigt.
Bereitgestellte Zuordnungsjobs	Wird unter der entsprechenden Anwendung angezeigt.
Logische Datenobjekte	Wird unter der entsprechenden Anwendung angezeigt.
SQL-Datendienste	Wird unter der entsprechenden Anwendung angezeigt.
Webdienste	Wird unter der entsprechenden Anwendung angezeigt.
Arbeitsabläufe	Wird unter der entsprechenden Anwendung angezeigt.

Ansichten in der Ansicht „Ausführungsstatistiken“

Wenn Sie im Navigator oder in einer Objektverknüpfung im Inhaltsbereich der Ansicht **Ausführungsstatistiken** ein Integrationsobjekt auswählen, werden im Inhaltsbereich viele Ansichten mit verschiedenen Informationen angezeigt. Diese Ansichten enthalten Informationen zu dem ausgewählten Objekt, z. B. Eigenschaften, Laufzeit-Statistiken und Laufzeitberichte.

Je nach Objekttyp, den Sie im Navigator auswählen, werden im Inhaltsbereich die folgenden Ansichten angezeigt:

Ansicht „Eigenschaften“

Führt die allgemeinen Eigenschaften und Laufzeit-Statistiken zum ausgewählten Objekt auf. Allgemeine Eigenschaften können den Namen und die Beschreibung des Objekts enthalten. Die Statistiken variieren basierend auf dem ausgewählten Objekttyp.

Ansicht „Statistiken“

Zeigt historische Statistiken über Jobs in einer Anwendung oder Jobs an, die vom Datenintegrationsdienst ausgeführt wurden. Wenn Sie beispielsweise eine Anwendung auswählen, können Sie die Anzahl der bereitgestellten Mapping-Jobs anzeigen, die in den letzten vier Stunden fehlgeschlagen sind.

Ansicht Berichte

Zeigt Berichte zum ausgewählten Objekt an. Berichte enthalten die Schlüsselmetriken für das Objekt. Zum Beispiel: Sie können Berichte anzeigen, um die am längsten ausgeführten Jobs in einem Datenintegrationsdienst innerhalb einer bestimmten Zeitspanne ausfindig zu machen.

Ansicht „Übersichtsstatistik“

Zeigt Durchsatz- und Ressourcennutzungsstatistiken für Ad-hoc-Mapping-Jobs, bereitgestellte Mapping-Jobs oder Mappings in einem Arbeitsablauf an.

Ansicht „Detaillierte Statistiken“

Zeigt Diagramme zum Durchsatz und zur Ressourcennutzung für Ad-hoc-Mapping-Jobs, bereitgestellte Mapping-Jobs oder Mappings in einem Arbeitsablauf an.

Ansicht „Historische Statistik“

Zeigt Durchschnittsdaten aus mehreren Ausführungen eines bestimmten Jobs an. Sie können z. B. die minimale, maximale und durchschnittliche Dauer des Zuordnungs-Jobs anzeigen. Sie können die durchschnittliche CPU-Menge anzeigen, die der Job bei Ausführung verbraucht.

Verbindungsansicht

Zeigt Verbindungen an, die für das ausgewählte Objekt definiert wurden. Sie können Statistiken zu jeder Verbindung anzeigen, z. B. die Anzahl der geschlossenen, abgebrochenen und gesamten Verbindungen.

Ansicht Anfragen

Zeigt die Details zu Anfragen an. Es gibt zwei Typen von Anfragen: SQL-Abfragen und Webdienstanfragen. Die Benutzer können ein Client-Tool von einem Drittanbieter verwenden, um SQL-Abfragen gegen die virtuellen Tabellen in einem SQL-Datendienst auszuführen. Die Benutzer können einen Webdienstclient zum Ausführen von Webdienstanfragen an einen Webdienst verwenden. Jede Web-Dienst-Anfrage führt eine Web-Dienst-Operation aus.

Eine Anfrage ist entweder eine Webdienstanfrage oder eine SQL-Abfrage, die der Benutzer für eine virtuelle Tabelle im SQL-Datendienst ausführt.

Virtuelle Tabellenansicht

Zeigt die virtuellen Tabellen an, die in einem SQL-Datendienst definiert sind. Auch die Eigenschaften und Cache-Aktualisierungsdetails lassen sich für jede virtuelle Tabelle anzeigen.

Operationsansicht

Zeigt die Operationen, die für den Web-Dienst definiert wurden.

Statistiken in der Ansicht „Ausführungsstatistiken“

Wenn Sie im Navigator in der Ansicht **Ausführungsstatistiken** einen Datenintegrationsdienst oder eine Anwendung auswählen, werden im Abschnitt **Statistiken** der Ansicht **Eigenschaften** Statistiken für Jobs angezeigt, die im Datenintegrationsdienst ausgeführt werden.

In der folgenden Tabelle werden die Typen von Jobs und Statistiken beschrieben, die Sie anzeigen können:

Objekttyp	Statistiken
Ad-hoc-Jobs	Zeigt die folgenden Statistiken über Ad-hoc-Jobs an: <ul style="list-style-type: none"> - Gesamt. Gesamtzahl der Jobs. - Fehlgeschlagen. Anzahl der fehlgeschlagenen Jobs. - Abgebrochen. Anzahl der abgebrochenen Jobs. Der Datenintegrationsdienst wurde im Abbruchmodus bei laufendem Job wiederhergestellt bzw. deaktiviert. - Abgeschlossen. Anzahl der abgeschlossenen Jobs. - Storniert. Anzahl der stornierten Jobs.
Anwendungen	Zeigt die folgenden Statistiken über Anwendungen an: <ul style="list-style-type: none"> - Gesamt. Gesamtzahl der Anwendungen. - Wird ausgeführt. Anzahl der ausgeführten Anwendungen. - Fehlgeschlagen. Anzahl der fehlgeschlagenen Anwendungen. - Gestoppt. Anzahl der gestoppten Anwendungen. - Deaktiviert. Anzahl der deaktivierten Anwendungen.
Bereitgestellte Zuordnungs-Jobs	Zeigt die folgenden Statistiken über bereitgestellte Mapping-Jobs an: <ul style="list-style-type: none"> - Gesamt. Gesamtanzahl der bereitgestellten Mappings. - Fehlgeschlagen. Anzahl der fehlgeschlagenen Mapping-Jobs. - Abgebrochen. Anzahl der abgebrochenen Mapping-Jobs. - Abgeschlossen. Anzahl der abgeschlossenen Mapping-Jobs. - Storniert. Anzahl der stornierten Mapping-Jobs.
Verbindungen	Zeigt die folgenden Statistiken über SQL-Datendienstverbindungen zu virtuellen Datenbanken an: <ul style="list-style-type: none"> - Gesamt. Gesamtanzahl der Verbindungen. - Geschlossen. Anzahl der Datenbankverbindungen, für die zuvor SQL-Datendienstanfragen ausgeführt wurden. - Abgebrochen. Anzahl der Verbindungen, die entweder manuell oder bei der Wiederherstellung bzw. Deaktivierung des Datenintegrationsdiensts im Abbruchmodus abgebrochen wurden.
Abfragen	Zeigt die folgenden Statistiken über SQL-Datendienst- und Webdienstanfragen an: <ul style="list-style-type: none"> - Gesamt. Gesamtzahl der Anfragen. - Abgeschlossen. Anzahl der abgeschlossenen Anfragen. - Abgebrochen. Anfragen, die bei der Wiederherstellung bzw. Deaktivierung des Datenintegrationsdiensts im Abbruchmodus abgebrochen wurden. - Fehlgeschlagen. Anzahl der fehlgeschlagenen Anfragen.
Arbeitsabläufe	Zeigt die folgenden Statistiken über Arbeitsabläufe an: <ul style="list-style-type: none"> - Gesamt. Gesamtzahl der Arbeitsablaufinstanzen. - Abgeschlossen. Anzahl der abgeschlossenen Arbeitsablaufinstanzen. - Storniert. Anzahl der stornierten Arbeitsablaufinstanzen. - Abgebrochen. Anzahl der abgebrochenen Arbeitsablaufinstanzen. - Fehlgeschlagen. Anzahl der fehlgeschlagenen Arbeitsablaufinstanzen.

Berichte in der Ansicht „Ausführungsstatistiken“

Sie können Überwachungsberichte in der Ansicht **Berichte** unter **Ausführungsstatistiken** überwachen. Die Ansicht **Berichte** wird angezeigt, wenn Sie das entsprechende Objekt im Navigator auswählen. Sie können

Berichte anzeigen, um Objekte zu überwachen, die für einen Datenintegrationsdienst bereitgestellt wurden, z. B. Ad-hoc-Jobs, Webdienste, SQL-Datendienste und Arbeitsabläufe.

Welche Berichte in der Ansicht **Berichte** angezeigt werden, hängt von dem Objekt ab, das Sie auswählen. Zum Anzeigen von Berichten in der Ansicht **Berichte** müssen Sie diese auf der Registerkarte **Überwachen > Aktionen > Berichts- und Statistikeinstellungen** konfigurieren. Gemäß Voreinstellung werden in der Ansicht **Berichte** keine Berichte aufgeführt.

Sie können die folgenden Überwachungsberichte anzeigen:

Ad-hoc-Jobs mit längster Dauer

Zeigt Ad-hoc-Jobs an, die während des angegebenen Zeitraums am längsten liefen. Der Bericht zeigt Namen, ID, Typ, Status und Dauer des Jobs an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Datenintegrationsdienst überwachen.

Mapping-Jobs mit längster Dauer

Zeigt Mapping-Jobs an, die während des angegebenen Zeitraums am längsten liefen. Der Bericht zeigt Namen, ID, Status und Dauer des Jobs an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Datenintegrationsdienst überwachen.

Profil-Jobs mit längster Dauer

Zeigt Profil-Jobs an, die während des angegebenen Zeitraums am längsten liefen. Der Bericht zeigt Namen, ID, Status und Dauer des Jobs an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Datenintegrationsdienst überwachen.

Referenztabellen-Jobs mit längster Dauer

Zeigt Referenztabellen-Jobs an, die während des angegebenen Zeitraums am längsten liefen. Bei Referenztabellen-Jobs handelt es sich um Jobs, bei denen Sie Referenztabellendaten importieren oder exportieren. Der Bericht zeigt Namen, ID, Status und Dauer des Jobs an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Datenintegrationsdienst überwachen.

Scorecard-Jobs mit längster Dauer

Zeigt Scorecard-Jobs an, die während des angegebenen Zeitraums am längsten liefen. Der Bericht zeigt Namen, ID, Status und Dauer des Jobs an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Datenintegrationsdienst überwachen.

SQL-Datendienstverbindungen mit längster Dauer

Zeigt SQL-Datendienstverbindungen an, die während des angegebenen Zeitraums am längsten liefen. Der Bericht zeigt Verbindungs-ID, SQL-Datendienst, Verbindungsstatus und Dauer an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Datenintegrationsdienst, einen SQL-Datendienst oder eine Anwendung überwachen.

SQL-Datendienstanfragen mit längster Dauer

Zeigt SQL-Datendienstanfragen an, die während des angegebenen Zeitraums am längsten liefen. Der Bericht zeigt Nummer der Anfrage, SQL-Datendienst, Anfragestatus und Dauer an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Datenintegrationsdienst, einen SQL-Datendienst oder eine Anwendung überwachen.

Web-Dienst-Anfragen mit längster Dauer

Zeigt Web-Dienst-Anfragen an, die während des angegebenen Zeitraums am längsten liefen. Der Bericht zeigt Nummer der Anfrage, Web-Dienst-Operation, Anfragestatus und Dauer an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Datenintegrationsdienst, einen Webdienst oder eine Anwendung überwachen.

Arbeitsabläufe mit längster Dauer

Zeigt alle Arbeitsabläufe an, die im angegebenen Zeitraum am längsten ausgeführt werden. Der Bericht zeigt den Namen, den Status, die Instanz-ID und die Dauer des Arbeitsablaufs an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Datenintegrationsdienst oder eine Anwendung überwachen.

Arbeitsabläufe mit längster Dauer, ausgenommen Human-Tasks

Zeigt Arbeitsabläufe an, die keine Human-Task enthalten, die im angegebenen Zeitraum am längsten ausgeführt werden. Der Bericht zeigt den Namen, den Status, die Instanz-ID und die Dauer des Arbeitsablaufs an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Datenintegrationsdienst oder eine Anwendung überwachen.

Bericht für minimale, maximale und durchschnittliche Dauer

Zeigt die minimale, maximale und durchschnittliche Dauer für SQL-Datendienst- und Webdienstanfragen während eines bestimmten Zeitraums an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Datenintegrationsdienst, einen SQL-Datendienst, einen Webdienst oder eine Anwendung überwachen.

Aktivste IP für SQL-Datendienstanfragen

Zeigt die Gesamtzahl der SQL-Datendienst- und Web-Dienst-Anfragen von jeder IP-Adresse während des angegebenen Zeitraums an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Datenintegrationsdienst, einen SQL-Datendienst oder eine Anwendung überwachen.

Aktivste SQL-Datendienstverbindungen

Zeigt SQL-Datendienstverbindungen an, die während des angegebenen Zeitraums die meisten Verbindungsanfragen erhalten haben. Der Bericht zeigt Verbindungs-ID, SQL-Datendienst und Gesamtanzahl der Verbindungsanfragen an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Datenintegrationsdienst, eine Anwendung oder einen SQL-Datendienst überwachen.

Aktivste Benutzer für Ad-hoc-Jobs

Zeigt die Benutzer an, die während des angegebenen Zeitraums die meisten Ad-hoc-Jobs ausgeführt haben. Der Bericht zeigt den Benutzernamen und die Gesamtzahl der vom Benutzer ausgeführten Jobs an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Datenintegrationsdienst überwachen.

Aktivste Web-Dienst-Client-IP

Zeigt die IP-Adressen an, die während des angegebenen Zeitraums die meisten Web-Dienst-Anfragen erhalten haben. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Datenintegrationsdienst, eine Anwendung, einen Webdienst oder einen Webdienstvorgang überwachen.

Häufigste Fehler bei Ad-hoc-Jobs

Zeigt die häufigsten Fehler bei Ad-hoc-Jobs während des angegebenen Zeitraums unabhängig vom jeweiligen Jobtyp an. Der Bericht zeigt Jobtyp, Fehlernummer, Status und Anzahl der Fehler an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Datenintegrationsdienst überwachen.

Häufigste Fehler für SQL-Datendienstanfragen

Zeigt die häufigsten Fehler bei SQL-Datendienstanfragen während des angegebenen Zeitraums an. Der Bericht zeigt die Fehlernummer und die Anzahl der Fehler an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Datenintegrationsdienst, einen SQL-Datendienst oder eine Anwendung überwachen.

Häufigste Fehler für Web-Dienst-Anfragen

Zeigt die häufigsten Fehler bei Web-Dienst-Anfragen während des angegebenen Zeitraums an. Der Bericht zeigt die Fehlernummer und die Anzahl der Fehler an. Sie können diesen Bericht in der Ansicht **Berichte** anzeigen, wenn Sie auf der Registerkarte **Überwachen** einen Datenintegrationsdienst, einen Webdienst oder eine Anwendung überwachen.

Ansicht „Übersichtsstatistik“

Sie können Durchsatz- und Ressourcennutzungsstatistiken für Mapping-Jobs in der Ansicht **Ausführungsstatistiken** anzeigen.

Wenn Sie im Inhaltsbereich einen Ad-hoc-Mapping-Job, einen bereitgestellten Mapping-Job oder ein Mapping in einem Arbeitsablauf auswählen, wird im Detailbereich die Ansicht **Ausführungsstatistiken** angezeigt. In der Ansicht **Übersichtsstatistik** werden Laufzeitstatistiken zum Durchsatz und zur Ressourcennutzung für den Job angezeigt. Die Laufzeit beginnt, wenn der Datenintegrationsdienst mit dem Lesen ab der ersten Zeile beginnt.

Sie können die folgenden Durchsatzstatistiken für den Job anzeigen:

- Quelle. Der Name der Mapping-Quelldatei.
- Zielname. Der Name der Zieldatei.
- Zeilen. Anzahl der für Quelle und Ziel gelesenen Zeilen.
- Durchschnittliche Zeilen/Sek. Durchschnittliche Anzahl der pro Sekunde für Quelle und Ziel gelesenen Zeilen.
- Byte. Anzahl der für Quelle und Ziel gelesenen Byte.
- Durchschnittliche Byte/Sek. Durchschnittliche Anzahl der pro Sekunde für Quelle und Ziel gelesenen Byte.
- Zugriff auf erste Zeile. Datum und Uhrzeit, als der Datenintegrationsdienst mit dem Lesen der ersten Zeile in der Quelldatei begann.
- Fallen gelassene Zeilen. Anzahl der Quellzeilen, die der Datenintegrationsdienst nicht gelesen hat.
- Abgelehnte Zeilen. Anzahl der Zielzeilen, die der Datenintegrationsdienst nicht in das Ziel geschrieben hat.

Sie können die folgenden Ressourcennutzungsstatistiken für den Job anzeigen:

- Ausgeführter Knoten. Knoten, auf dem der Datenintegrationsdienst ausgeführt wird, der den Job ausgeführt hat.
- Durchschnittliche CPU-Nutzung. Die durchschnittliche Menge an CPU-Ressourcen, die der Datenintegrationsdienst zur Ausführung des Jobs genutzt hat.
- Durchschnittliche Speichernutzung. Die durchschnittliche Speichermenge, die der Datenintegrationsdienst zur Ausführung des Jobs genutzt hat.

Ansicht „Detaillierte Statistiken“

Sie können Diagramme der Durchsatz- und Ressourceninformationen für Mapping-Jobs anzeigen, die länger als eine Minute ausgeführt werden.

Wenn Sie im Inhaltsbereich der Ansicht **Ausführungsstatistiken** einen Ad-hoc-Mapping-Job, einen bereitgestellten Mapping-Job oder ein Mapping in einem Arbeitsablauf auswählen, wird im Detailbereich die Ansicht **Detaillierte Statistiken** angezeigt. In der Ansicht **Detaillierte Statistiken** werden Laufzeitstatistiken zum Durchsatz und zur Ressourcennutzung für den Job angezeigt. Die Laufzeit beginnt, wenn der Datenintegrationsdienst mit dem Lesen ab der ersten Zeile beginnt.

In der Ansicht **Detaillierte Statistiken** werden die folgenden Diagramme angezeigt:

Diagramm „Durchsatz“

Bildet die Anzahl der gelesenen und geschriebenen Zeilen im Verhältnis zur Laufzeit des Jobs ab.

Diagramm „CPU-Nutzung“

Bildet den Prozentsatz der CPU des Datenintegrationsdiensts ab, der für die Ausführung des Jobs zugewiesen wurde, im Verhältnis zur Laufzeit des Jobs ab.

Diagramm „Speichernutzung“

Bildet die Speichermenge in Megabyte ab, die der Datenintegrationsdienst für die Ausführung des Jobs zugewiesen hat, im Verhältnis zur Laufzeit des Jobs ab.

Registerkarte "Protokolle"

Die Registerkarte **Protokolle** zeigt Protokolle an.

Auf der Registerkarte **Protokolle** können Sie die folgenden Arten von Protokollen anzeigen:

- Domänenprotokoll. Domänenprotokollereignisse sind Protokollereignisse, die anhand der vom Service Manager ausgeführten Domänenfunktionen generiert werden.
- Dienstprotokoll. Dienstprotokollereignisse sind Ereignisse, die von jedem Anwendungsdienst generiert werden.
- Benutzeraktivitätsprotokoll. Benutzeraktivitätsprotokollereignisse zum Überwachen der Benutzeraktivitäten in der Domäne.

Auf der Registerkarte **Protokolle** werden für jede Art von Protokoll die folgenden Komponenten angezeigt.

- Filter Zum Konfigurieren der Filteroptionen für die Protokolle.
- Log Viewer. Zeigt Protokollereignisse entsprechend den Filterkriterien.
- Filter zurücksetzen Zum Zurücksetzen der Filterkriterien.
- Zeilen kopieren. Zum Kopieren des Protokolltexts der ausgewählten Zeilen.
- Menü **Aktionen** Enthält Optionen zum Speichern, Löschen und Verwalten von Protokollen. Es enthält auch Filteroptionen.

Registerkarte Berichte

Die Registerkarte **Berichte** zeigt die Domänenberichte an.

Auf der Registerkarte **Berichte** können Sie folgende Domänenberichte ausführen:

- Lizenzverwaltungsbericht Führen Sie einen Bericht aus, um die Anzahl der Softwareoptionen zu überwachen, die für die Lizenz erworben wurden, sowie die mit der Lizenz verbundene Anzahl an Benutzerbeschränkungen. Führen Sie einen Bericht aus, um die Verwendung logischer CPUs und der PowerCenter Repository Services zu überwachen. Für die Ausführung des Berichts ist eine Lizenz erforderlich.
- Web-Dienste-Bericht. Führen Sie einen Bericht aus, um die Performance der Web-Dienste zu analysieren, die auf einem Web-Dienste-Hub ausgeführt werden. Ein Bericht wird während eines bestimmten Zeitintervalls ausgeführt.

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 Sicherheitsdomänenordnern 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 Kontosperrung“ der Seite „Kontoverwaltung“ ist angegeben, ob die Kontosperrung 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.

Dienststatus

Sie können den Status eines Anwendungsdiensts über das im Administrator Tool angezeigte Symbol identifizieren.

In der folgenden Tabelle werden die Symbole beschrieben, die Dienststatus angeben:

Status	Symbol
Verfügbar	
Deaktiviert	
Nicht verfügbar	




















Prozessstatus

Sie können den Status eines Datenintegrationsdienst-Prozesses oder PowerCenter-Integrationsdienstprozesses über das im Administrator Tool angezeigte Symbol ermitteln.

Die Statussymbole geben auch den Typ des Knotens an, auf dem der Prozess ausgeführt wird. Falls der Primärknoten hochverfügbar ist, befindet sich über dem Prozessstatussymbol ein gelbes Diamantsymbol. Wird der Prozess in einem Gitter ausgeführt, befindet sich über dem Prozessstatussymbol ein Gittersymbol.

In der folgenden Tabelle werden die Symbole beschrieben, die den Prozessstatus angeben:

Status	Symbol
Vorzeitig beendet	
Vorzeitig beendet (mit hoher Verfügbarkeit)	





Status	Symbol
Vorzeitig beendet (Gitter)	
Deaktiviert	
Deaktiviert (mit hoher Verfügbarkeit)	
Deaktiviert (Gitter)	
Fehlgeschlagen	
Fehlgeschlagen (mit hoher Verfügbarkeit)	
Fehlgeschlagen (Gitter)	
Wird ausgeführt	
Wird ausgeführt (mit hoher Verfügbarkeit)	
Wird ausgeführt (Gitter)	
„Im Wartezustand“ oder „Verzögert“	
„Im Wartezustand“ oder „Verzögert“ (mit hoher Verfügbarkeit)	
„Im Wartezustand“ oder „Verzögert“ (Gitter)	
Wird gestartet	
Wird gestartet (mit hoher Verfügbarkeit)	
Wird gestartet (Gitter)	
Gestoppt	
Gestoppt (mit hoher Verfügbarkeit)	
Gestoppt (Gitter)	

Status	Symbol
Stoppen	
Stoppen (mit hoher Verfügbarkeit)	
Stoppen (Gitter)	

Jobstatus

Sie können den Status eines Jobs über das im Administrator Tool angezeigte Symbol ermitteln.

In der folgenden Tabelle werden die Symbole für jeden Jobstatus beschrieben:

Status	Symbol
Vorzeitig beendet	
Storniert	
Abgeschlossen	
Fehlgeschlagen	
„In Warteschlange eingereiht“ oder „Ausstehend“	
Wird ausgeführt	
Wird gestartet	
Gestoppt	
Stoppen	
Beendet	
Unbekannt	

Barrierefreiheit von Informatica Administrator - Übersicht

Sie können eine Sprachausgabe und Tastenkombinationen verwenden, um in der Administrator Tool-Schnittstelle zu navigieren und damit zu arbeiten.

Zum Ein- bzw. Ausschalten des JAWS Virtual PC-Cursors verwenden Sie die Tastenkombination **Einf+Z**.

Hinweis: Damit Sie die JAWS-Sprachausgabe mit dem Administrator Tool verwenden können, benötigen Sie Internet Explorer 11.

Tastenkombinationen

Sie können Tastenkombinationen verwenden, um mit der Administrator Tool-Schnittstelle zu navigieren und darin zu arbeiten.

Sie können die Werte im Administrator Tool hinzufügen, bearbeiten und ändern. Der Tastaturfokus im Administrator Tool wird durch einen blauen Rahmen um die Schnittstellenbeschriftung angegeben. Wenn das Objekt im Fokus steht, wird es ebenfalls mit einer gepunkteten Linie umrandet. Wenn ein Beschriftungselement mit der Tastatur fokussiert wird oder wenn die Maus darüber bewegt wird, werden Tooltips angezeigt. Die Navigationsreihenfolge der Objekte im Editor verläuft von oben nach unten und von links nach rechts.

Sie können die folgenden Aufgaben mit Tastenkombinationen durchführen:

Zwischen Elementen navigieren oder ein Element auswählen

Drücken Sie die **TAB-TASTE**.

Das vorherige Objekt auswählen

Drücken Sie **UMSCHALT+TAB**.

Zwischen den Darstellungsregisterkarten navigieren

Drücken Sie die **NACH-LINKS-** bzw. **NACH-RECHTS-TASTE**.

Ein Kontrollkästchen oder eine Optionsschaltfläche aktivieren oder deaktivieren

Drücken Sie die **LEERTASTE**.

Dateien hochladen über die Schaltfläche „Datei hochladen“

Drücken Sie die **LEERTASTE**.

Navigieren Sie durch Datensätze in einem Dialogfeld.

Drücken Sie die **NACH-OBEN-** bzw. **NACH-UNTEN-TASTE**.

Ein Dropdown-Menüelement mit Untermenüs auswählen und öffnen

Drücken Sie die **LEERTASTE**. Mit der **ESC-TASTE** gelangen Sie zurück zum Hauptmenü.

Den Wert von Gitterinhalten wie z. B. den Feldern „Zugriff“ oder „Widerrufen“ in den Dialogfeldern „Berechtigung zuweisen“ und „Direkte Berechtigungen bearbeiten“ bearbeiten

Drücken Sie die **LEERTASTE**.

Hinweis: Geben Sie entsprechende Werte für alle Formularelemente ein, die mit einem Sternchen (*) gekennzeichnet sind.

Den Fokus aus dem Dropdown-Menü „Aktualisierungshäufigkeit“ zum Kontrollkästchen „Zeitspanne“ im Listengitter „Statistik und Berichte“ im Dialogfeld „Berichts- und Statistikeinstellungen“ der Registerkarte „Überwachen“ oder des Überwachungstools verschieben.

Drücken Sie die **ESC-TASTE**.

Über die Tastatur können Sie nicht auf die Fensterteiler im Administrator Tool zugreifen und die Fenstergröße anpassen. Auf der Registerkarte „Audit-Berichte“ unter „Sicherheit“ können Sie mehrere Elemente mit der **STRG-TASTE** auswählen.

KAPITEL 4

Verwenden der Domänenansicht

Dieses Kapitel umfasst die folgenden Themen:

- [Über die Ansicht „Domäne“, 69](#)
- [Abhängigkeitsgrafik, 70](#)
- [Befehlshistorie, 72](#)
- [Ansicht „Historie“, 73](#)

Über die Ansicht „Domäne“

In der Ansicht „Domäne“ wird eine Übersicht zum Status der Domäne und den in ihr enthaltenen Objekten angezeigt. Sie können sich in der Ansicht „Domäne“ aktuelle und historische Informationen zu der Domäne ansehen.

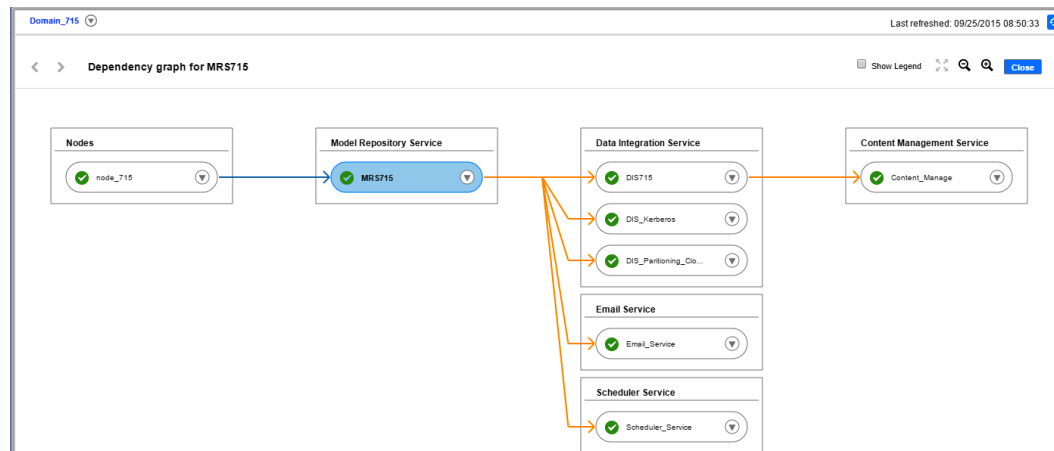
In der Ansicht „Domäne“ können Sie die folgenden Aufgaben durchführen:

- Anzeigen des aktuellen Status, der Ressourcennutzung und von Details für die Domäne und die Objekte in der Domäne.
- Anzeigen von Abhängigkeiten zwischen Objekten in der Domäne.
- Durchführen von Domänenaktionen, z. B. Herunterfahren der Domäne, Aktivieren und Deaktivieren von Diensten sowie Herunterfahren von Knoten.
- Anzeigen der letzten Dienstbefehle, die Benutzer im Administrator Tool ausgeführt haben.
- Anzeigen von historischen Informationen zum Status, zur Ressourcennutzung und zu Ereignissen in der Domäne.

Abhängigkeitsgrafik

In der **Abhängigkeitsgrafik** werden Abhängigkeiten zwischen Diensten, Knoten und Gittern in der Informatica-Domäne angezeigt.

Die folgende Abbildung zeigt die **Abhängigkeitsgrafik** für einen Modellrepository-Dienst:



In der **Abhängigkeitsgrafik** können Sie die folgenden Aufgaben durchführen:

- Anzeigen von Abhängigkeiten zwischen Knoten, Diensten und Gittern.
- Herunterfahren eines Knotens.
- Aktivieren, Deaktivieren oder Wiederherstellen eines Diensts.
- Deaktivieren bzw. Wiederherstellen von Diensten, die von anderen Diensten abhängen.

Wenn Sie Abhängigkeiten für ein Objekt anzeigen, werden in der **Abhängigkeitsgrafik** die vorangehenden und nachfolgenden Abhängigkeiten angezeigt. Vorangehende Abhängigkeiten sind Objekte, von denen das ausgewählte Objekt abhängt. Bei nachfolgenden Abhängigkeiten handelt es sich um Objekte, die vom ausgewählten Objekt abhängen.

Wenn Sie Dienste in der **Abhängigkeitsgrafik** aktivieren, deaktivieren oder wiederherstellen, werden die entsprechenden Aktionen im Bereich **Befehlshistorie** angezeigt.

Anzeigen von Abhängigkeiten für Anwendungsdienste, Knoten und Gitter

Sie können Abhängigkeiten zwischen Anwendungsdiensten, Knoten und Gittern in der Informatica-Domäne anzeigen.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie im Inhaltsbereich auf das Menü **Aktionen** für ein Domänenobjekt und wählen Sie dann **Abhängigkeiten anzeigen** aus.

Die **Abhängigkeitsgrafik** wird geöffnet und zeigt das Objekt und seine direkten Abhängigkeiten an. In der **Abhängigkeitsgrafik** werden die durch blaue und orange Linien verbundenen Domänenobjekte wie folgt angezeigt:

- Blaue Linien geben Dienst-zu-Knoten- und Dienst-zu-Gitter-Abhängigkeiten an.

- Gestrichelte blaue Linien geben Backup-Knoten-zu-Dienst-Abhängigkeiten an.
- Orange Linien geben Dienst-zu-Dienst-Abhängigkeiten an, beispielsweise eine Datenintegrationsdienst-zu-Content-Management-Dienst-Abhängigkeit oder eine Modellrepository-Dienst-zu-Datenintegrationsdienst-Abhängigkeit.

In der folgenden Tabelle wird beschrieben, welche Informationen in der **Abhängigkeitsgrafik** basierend auf dem jeweiligen Objekt dargestellt werden:

Domänenobjekt	Vorangehende Abhängigkeiten	Nachfolgende Abhängigkeiten
Knoten	N/V	Dienste, die auf dem Knoten ausgeführt werden.
Knoten, der in einem Gitter ausgeführt wird.	N/V	Der Knoten weist die folgenden nachfolgenden Abhängigkeiten auf: <ul style="list-style-type: none"> - Gitter, in dem der Knoten ausgeführt wird. - Dienstprozess, der im Gitter ausgeführt wird. - Dienstprozesse, die auf dem Knoten, aber nicht im Gitter ausgeführt werden.
Dienst	Knoten, auf dem der Dienstprozess ausgeführt wird.	Dienste, die von dem Dienst abhängen.
Dienst, der in einem Gitter ausgeführt wird	Der Dienst weist die folgenden vorangehenden Abhängigkeiten auf: <ul style="list-style-type: none"> - Knoten, auf denen der Dienstprozess ausgeführt wird. - Das Gitter, in dem die Dienstprozesse ausgeführt werden. 	Dienste, die von dem Dienst abhängen.
Dienst, der im HA-Modus ausgeführt wird	Primäre Knoten und Backup-Knoten, auf denen die Dienstprozesse ausgeführt werden können.	Dienste, die von dem Dienst abhängen.
Gitter	Knoten, die dem Gitter zugewiesen sind.	Dienste, die im Gitter ausgeführt werden.

3. In der **Abhängigkeitsgrafik** können Sie optional die folgenden Aufgaben ausführen:
- Auswählen von **Legende anzeigen**, um Informationen zu den in der Grafik verwendeten Symbolen und Linien anzuzeigen.
 - Klicken und Ziehen, um andere Teile der Grafik anzuzeigen.
 - Vergrößern oder Verkleinern der Grafik.
 - Zum Verlassen der **Abhängigkeitsgrafik** klicken Sie auf **Schließen**.

Wiederherstellen bzw. Deaktivieren von nachgelagerten Diensten

Sie können nachgelagerte Dienste in der **Abhängigkeitsgrafik** wiederherstellen bzw. deaktivieren.

Nachgelagerte Dienste sind Dienste, die von anderen Diensten abhängen. Beispiel: Ein Datenintegrationsdienst ist von einem Modellrepository-Dienst abhängig. Zum Wiederherstellen bzw.

Deaktivieren von nachgelagerten Diensten verwenden Sie das Menü „Aktionen“ für den Dienst, von dem sie abhängen. Wenn Sie nachgelagerte Dienste deaktivieren, werden die Dienstprozesse abgebrochen.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie auf das Menü **Aktionen** für ein Domänenobjekt und wählen Sie dann **Abhängigkeiten anzeigen** aus.
Die **Abhängigkeitsgrafik** wird geöffnet und zeigt das Objekt und seine direkten Abhängigkeiten an.
3. Klicken Sie auf **Aktionen > Nachfolgende Abhängigkeiten wiederherstellen** bzw. auf **Aktionen > Nachfolgende Abhängigkeiten deaktivieren**.
Das Fenster „Nachfolgende Abhängigkeiten wiederherstellen“ bzw. „Nachfolgende Abhängigkeiten deaktivieren“ wird angezeigt.
4. Wählen Sie optional aus, ob die Aktion **Geplant** oder **Ungeplant** ist.
5. Fügen Sie optional Kommentare über die Aktion hinzu.
6. Wählen Sie die Dienste aus, die Sie wiederherstellen bzw. deaktivieren möchten.
7. Klicken Sie auf **Dienste wiederherstellen** bzw. **Dienste deaktivieren**.

Befehlshistorie

In der Ansicht **Domäne** werden im Bereich **Befehlshistorie** die letzten Dienst-Lebenszyklusbefehle angezeigt, die Benutzer im Administrator Tool ausgeführt haben. Zu den Dienst-Lebenszyklusbefehlen zählen Befehle zum Aktivieren, Deaktivieren und Wiederherstellen.

Zum Anzeigen der Befehlshistorie klicken Sie auf **Domänenaktionen > Befehlshistorie anzeigen**.

Sie können die folgenden Informationen über die Befehle im Bereich **Befehlshistorie** anzeigen:

- Dienstname. Name des Diensts, für den der Befehl ausgeführt wurde.
- Diensttyp.
- Befehl.
- Status. Kann „Fehlgeschlagen“, „Erfolgreich“ oder „In Warteschlange eingereiht“ sein.
- Status aktualisiert
- Kommentare. Kommentare, die Benutzer beim Wiederherstellen oder Aktivieren des Diensts eingegeben haben.
- Nachricht. Mit dem Befehl verknüpfte Protokollmeldungen.

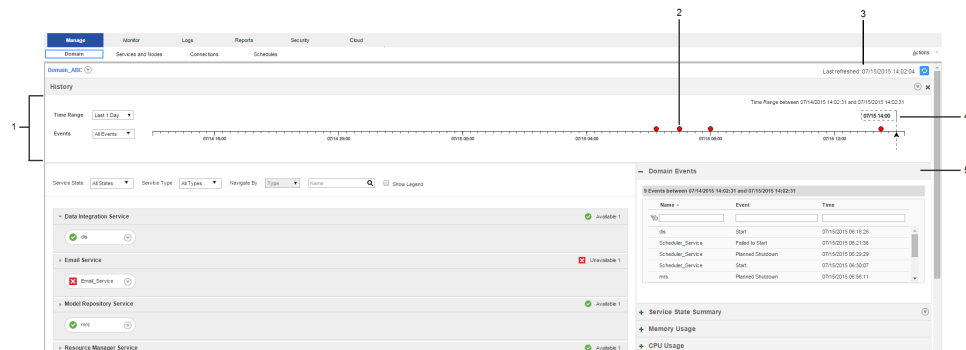
Optional können Sie Spalten in der Befehlshistorie ein- bzw. ausblenden. Zum Ändern der Spalten klicken Sie mit der rechten Maustaste auf die Kopfzeile der betreffenden Spalten. Wählen Sie dann Spalten aus bzw. löschen Sie sie.

Hinweis: Die Befehlshistorie wird gelöscht, wenn Sie den Master-Gateway-Knoten herunterfahren oder neu starten.

Ansicht „Historie“

In der Ansicht **Historie** werden historische Daten für die Domäne, einen Dienst oder einen Knoten angezeigt. Sie können historische Daten für den Inhaltsbereich, die Dienststatus-Zusammenfassung, die Ressourcennutzungsanzeigen und den Detailbereich anzeigen. Darüber hinaus können Sie Informationen zu Ereignissen in der Domäne anzeigen.

Die folgende Abbildung zeigt die Ansicht **Historie**:



1. Zeitleiste
2. Ereigniskreis
3. Zuletzt aktualisiert
4. Zeitleisten-Schieberegl
5. Bereich „Ereignisse“

Die Ansicht **Historie** enthält folgende Komponenten:

Zeitleiste

Wählen Sie in der Zeitleiste aus, welcher Zeitraum und welche Ereignisse angezeigt werden sollen. Wenn um einen Zeitpunkt herum Ereignisse auftreten, wird dieser mit einem roten Ereignispunkt gekennzeichnet. Klicken Sie auf einen Kreis, werden im Bereich „Ereignisse“ die Ereignisse angezeigt, die um diesen Zeitpunkt herum aufgetreten sind. In der Zeitleiste werden standardmäßig Abstürze und ungeplantes Herunterfahren während des letzten Tags angezeigt.

Bereich „Ereignisse“

Zeigt Ereignisse ein, die während eines bestimmten Zeitraums aufgetreten sind. Wenn Sie die Ansicht **Historie** öffnen, werden in diesem Bereich Abstürze und ungeplantes Herunterfahren während des letzten Tags angezeigt.

Inhaltsbereich

Zeigt aktuelle und historische Domäneninhalte und -status an. Wenn Sie die Ansicht **Historie** öffnen, werden im Inhaltsbereich Domänenobjekte und -status zum Zeitpunkt der letzten Aktualisierung angezeigt. Wenn Sie den Schieberegler der Zeitleiste zu einem bestimmten Zeitpunkt ziehen, werden im Inhaltsbereich Domänenobjekte und -status zu diesem Zeitpunkt angezeigt.

Dienststatus - Zusammenfassung

Zeigt aktuelle und historische Dienststatus-Zusammenfassungen an. Wenn Sie die Ansicht **Historie** über das Menü „Aktionen“ der Domäne öffnen, wird der Bereich „Dienststatus - Zusammenfassung“ mit der Anzahl und dem Status der Dienste zum Zeitpunkt der letzten Aktualisierung angezeigt. Wenn Sie den Schieberegler der Zeitleiste zu einem bestimmten Zeitpunkt ziehen, wird im Bereich „Dienststatus - Zusammenfassung“ die Anzahl der zu diesem Zeitpunkt verfügbaren bzw. nicht verfügbaren Dienste angezeigt.

Detailbereich

Zeigt aktuelle und historische Status für einen Dienst oder Knoten an. Wenn Sie die Ansicht **Historie** öffnen, wird im Detailbereich der Status des Diensts oder Knotens zum Zeitpunkt der letzten Aktualisierung angezeigt. Wenn Sie den Schieberegler der Zeitleiste zu einem bestimmten Zeitpunkt ziehen, wird im Detailbereich der Objektstatus zu diesem Zeitpunkt angezeigt.

Ressourcennutzungsanzeigen

Zeigt aktuelle und historische Ressourcennutzungsinformationen an. Wenn Sie die Ansicht **Historie** öffnen, werden in den Nutzungsanzeigen die Nutzungsstatistiken so angezeigt, wie sie zum Zeitpunkt der letzten Aktualisierung angezeigt wurden. Wenn Sie den Schieberegler der Zeitleiste zu einem bestimmten Zeitpunkt ziehen, werden in den Anzeigen Statistiken für diesen Zeitpunkt angezeigt.

Die Daten, die Sie in der Ansicht „Historie“ anzeigen, werden im Überwachungsmodellrepository gespeichert. Vor der Anzeige historischer Daten müssen Sie das Überwachungsmodellrepository auf der Registerkarte **Verwalten > Dienste und Knoten > Überwachungskonfiguration** konfigurieren. Sie können die pro Minute ermittelten Daten für bis zu zwei Wochen in der Vergangenheit anzeigen. Nach zwei Wochen handelt es sich bei den angezeigten Statistiken um stündliche Durchschnittswerte. Sie können die pro Stunde ermittelten Durchschnittsdaten für bis zu ein Jahr in der Vergangenheit anzeigen.

Hinweis: Der Überwachungsmodellrepository-Dienst, den Sie für die Speicherung der historischen Daten konfigurieren, kann keine Daten zu Ereignissen erfassen, die auftreten, während der Dienst nicht verfügbar oder deaktiviert ist. Beispielsweise werden Startereignisse für den Überwachungsmodellrepository-Dienst und Absturzereignisse für den Knoten, auf dem der Überwachungsmodellrepository-Dienstprozess ausgeführt wird, nicht in der Ansicht „Historie“ angezeigt.

Anzeigen der Historie

Sie können eine historische Statistik für die Domäne, einen Dienst oder einen Knoten anzeigen.

In welchem Umfang Sie die Historie anzeigen können, hängt von den Überwachungsmodellrepository-Optionen ab, die Sie auf der Registerkarte „Überwachungskonfiguration“ konfigurieren. Sie müssen auf der Registerkarte „Überwachungskonfiguration“ ein Überwachungsmodellrepository konfigurieren, bevor Sie die historische Statistik anzeigen können.

1. Klicken Sie für den Zugriff auf die Ansicht **Historie** auf das Menü **Aktionen** für die Domäne, einen Dienst oder einen Knoten und wählen Sie dann **Verlauf anzeigen** aus.

Die Ansicht **Historie** wird geöffnet. Die automatische Aktualisierung wird beim Zeitstempel „Zuletzt aktualisiert“ angehalten. Die Zeitleiste und der Bereich **Ereignisse** werden angezeigt. Darin werden Abstürze und ungeplantes Herunterfahren während des letzten Tags angezeigt.

2. Zum Ändern des Zeitraums wählen Sie in der Liste **Zeitspanne** eine Zeitspanne aus.

Wenn Sie den Zeitraum ändern, wird die Zeitleiste aktualisiert und zeigt die ausgewählte Zeitspanne an.

3. Zur Auswahl einer benutzerdefinierten Zeitspanne wählen Sie in der Liste **Zeitspanne** die Option **Benutzerdefiniert** aus.

Sie können eine benutzerdefinierte Zeitspanne von einer Stunde bis zu einem Monat auswählen.

4. Wenn Sie die Ereignisse ändern möchten, die angezeigt werden, wählen Sie in der Liste **Ereignisse** die entsprechenden Ereignisse aus.

Sie können Informationen zu folgenden Ereignissen anzeigen:

- Absturz
- Fehler beim Starten
- Ungeplantes Herunterfahren

- Geplantes Herunterfahren
- Start

Wenn Sie verschiedene Ereignisse auswählen, wird die Zeitleiste aktualisiert und zeigt die Änderung an.

5. Wenn Sie die historische Statistik zu der Domäne anzeigen möchten, ziehen Sie den Schieberegler der Zeitleiste zum gewünschten Zeitpunkt.

Die Ansicht **Historie** wird aktualisiert und zeigt den Domänenstatus zu diesem Zeitpunkt an.

6. Zum Verlassen der Ansicht **Historie** klicken Sie auf **Schließen**.

Hinweis: Aktuelle Dienste werden als „Nicht verfügbar“ angezeigt, wenn die Zeitspanne zu einem Zeitpunkt vor ihrer Erstellung beginnt.

Anzeigen von Ereignissen

Sie können Ereignisse für die Domäne, einen Knoten oder einen Dienst anzeigen.

1. Klicken Sie zum Anzeigen von Ereignissen auf das Menü **Aktionen** für die Domäne, einen Knoten oder einen Dienst und wählen Sie dann **Verlauf anzeigen** aus.

Die Ansicht **Historie** wird geöffnet, in der der Bereich „Ereignisse“ angezeigt wird. Im Bereich „Ereignisse“ werden standardmäßig Abstürze und ungeplantes Herunterfahren während des letzten Tags angezeigt.

1. Sie können die folgenden Informationen zu Ereignissen anzeigen:

- Objektname
- Objekttyp
- Ereignistyp
- Zeitpunkt, zu dem das Ereignis aufgetreten ist
- Name des zugeordneten Knotens
- Kommentare zu wiederhergestellten oder deaktivierten Diensten
- Kommentare zu heruntergefahrenen Knoten

2. Im Bereich „Ereignisse“ können Sie optional die folgenden Aktionen ausführen:

Option	Beschreibung
Ereignisse suchen	Geben Sie die Suchkriterien in das Suchfeld ein und drücken Sie dann die EINGABETASTE. Um die Suche zu löschen, klicken Sie auf das Symbol „Filter zurücksetzen“.
Spalte sortieren	Wenn Sie eine Spalte in aufsteigender Reihenfolge sortieren möchten, klicken Sie auf die Kopfzeile der Spalte. Um die Spalte in absteigender Reihenfolge zu sortieren, klicken Sie erneut auf die Kopfzeile der Spalte.
Spalten hinzufügen bzw. entfernen	Wenn Sie die im Bereich „Ereignisse“ angezeigten Spalten ändern möchten, klicken Sie mit der rechten Maustaste auf die Kopfzeile einer Spalte und wählen die Spalte aus bzw. heben die Spaltenauswahl auf.
Filter zurücksetzen	Wenn Sie auf einen Kreis in der Zeitleiste klicken, können Sie die Auswahl aufheben, indem Sie auf „Filter zurücksetzen“ klicken.

KAPITEL 5

Domänenverwaltung

Dieses Kapitel umfasst die folgenden Themen:

- [Domänenverwaltung - Übersicht, 76](#)
- [Alarmverwaltung, 77](#)
- [Ordnerverwaltung, 79](#)
- [Domänensicherheitsmanagement, 81](#)
- [Sicherheitsverwaltung für Benutzer, 81](#)
- [Anwendungsdienstverwaltung, 82](#)
- [Gateway-Konfiguration, 84](#)
- [Domänenkonfigurationsverwaltung, 85](#)
- [Umbenennen der Domäne, 90](#)
- [Herunterfahren einer Domäne, 91](#)
- [Domäneneigenschaften, 91](#)

Domänenverwaltung - Übersicht

Eine Informatica-Domäne besteht aus einer Reihe von Knoten und Diensten zur Definition der Informatica-Umgebung. Um die Domäne zu verwalten, müssen Sie die Knoten und Dienste in der Domäne verwalten.

Mit dem Administrator-Tool können Sie folgenden Aufgaben durchführen:

- Alarme verwalten. Konfigurieren, Aktivieren und Deaktivieren von Domänen- und Dienstalarmen für Benutzer.
- Ordner erstellen. Erstellen von Ordnern zum Organisieren von Domänenobjekten und für die Sicherheitsverwaltung durch Einstellen von Ordnerberechtigungen.
- Domänensicherheits-Verwaltung. Konfigurieren sicherer Kommunikation zwischen Domänenkomponenten.
- Benutzersicherheits-Verwaltung. Zuweisen von Berechtigungen zu Benutzern und Gruppen.
- Verwalten von Anwendungsdiensten. Aktivieren, Deaktivieren, Recyclen und Entfernen von Anwendungsdiensten. Aktivieren und Deaktivieren von Dienstprozessen.
- Verwalten von Knoten. Konfigurieren der Knoteneigenschaften, wie Sicherungsverzeichnis und Ressourcen, sowie Herunterfahren der Knoten.
- Konfigurieren von Gateway-Knoten. Konfigurieren von Knoten, die als Gateway fungieren sollen.

- Herunterfahren der Domäne. Herunterfahren der Domäne zwecks Ausführung administrativer Aufgaben in der Domäne.
- Verwalten der Domänenkonfiguration. Sichern Sie die Domänenkonfiguration regelmäßig. Es kann erforderlich sein, die Domänenkonfiguration aus der Sicherung wieder herzustellen, um die Konfiguration zu einem anderen Datenbank-Benutzerkonto zu migrieren. Vielleicht müssen Sie auch die Datenbank-Informationen für die Domänenkonfiguration zurücksetzen, falls sie sich ändern.
- Abschließen von Domänenaufgaben. Sie können den Status aller Anwendungsdienste und Knoten überwachen, gegenseitige Abhängigkeiten der Anwendungsdienste und Knoten anzeigen und die Domäne herunterfahren.
- Konfigurieren von Domäneneigenschaften. Zum Beispiel können Sie die Datenbankeigenschaften, die SMTP-Eigenschaften für Alarme und die Domänenbelastbarkeitseigenschaften ändern.

Um Knoten und Dienste über eine einzige Schnittstelle zu verwalten, müssen sich alle Knoten und Dienste in derselben Domäne befinden. Der Zugriff auf mehrere Informatica-Domänen in ein- und demselben Fenster des Administrator-Tools ist nicht möglich. Das Einrichten von Metadaten für die gemeinsame Nutzung durch mehrere Domänen ist möglich, indem Sie ein lokales Repository in der lokalen Informatica-Domäne mit einem globalen Repository in einer anderen Informatica-Domäne registrieren oder deregistrieren.

Alarmverwaltung

Alarme stellen dem Benutzer Domänen- und Dienstalarme bereit. Domänenalarme enthalten Informationen zu fehlerhaften Knoten und Master-Gateway-Auswahl. Dienstalarme enthalten Informationen zu fehlerhaften Dienstprozessen.

Um Alarme zu verwenden, führen Sie folgende Aufgaben durch:

- Konfigurieren Sie die SMTP-Einstellungen für den ausgehenden Mailserver.
- Abonnieren Sie Alarme.

Nachdem Sie die SMTP-Einstellungen konfiguriert haben, können die Benutzer die Domänen- und Dienstalarme abonnieren.

Konfigurieren der SMTP-Einstellungen

Konfigurieren Sie die SMTP-Einstellungen für den ausgehenden Mailserver, um Alarme zu aktivieren.

Die SMTP-Einstellungen konfigurieren Sie in der Domänenansicht **Eigenschaften**.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie auf die Ansicht **Dienste und Knoten**.
3. Wählen Sie die Domäne im Navigator aus.
4. Klicken Sie im Inhaltsbereich auf die Ansicht **Eigenschaften**.
5. Klicken Sie im Abschnitt „SMTP-Konfiguration“ auf **Bearbeiten**.

6. Bearbeiten Sie die SMTP-Einstellungen.

Eigenschaft	Beschreibung
Hostname	Hostname für ausgehenden SMTP-Mailserver. Geben Sie zum Beispiel den Microsoft Exchange-Server für Microsoft Outlook ein.
Port	Vom ausgehenden Mailserver verwendeter Port. Die gültigen Werte liegen zwischen 1 und 65535. Standardwert ist 25.
Benutzername	Benutzername für die Authentifizierung beim Senden, wenn dies vom ausgehenden Mailserver gefordert wird.
Passwort	Benutzerpasswort für die Authentifizierung beim Senden, wenn dies vom ausgehenden Mailserver gefordert wird.
E-Mail-Adresse des Absenders	E-Mail-Adresse, die der Dienstmanager im Feld „Von“ beim Senden von Benachrichtigungs-E-Mails verwendet. Wenn Sie dieses Feld leer lassen, verwendet der Dienstmanager Administrator@<Hostname> als Absender.

7. Klicken Sie auf **OK**.

Alarmer abbonieren

Nachdem Sie die SMTP-Konfiguration abgeschlossen haben, können Sie Alarmer abbonieren.

1. Überprüfen Sie, ob der Domänenadministrator eine gültige E-Mail-Adresse für Ihr Benutzerkonto auf der Seite **Sicherheit** eingegeben hat.

Wenn die E-Mail-Adresse oder die SMTP-Konfiguration ungültig ist, kann der Service Manager keine Warnmeldung liefern.

2. Klicken Sie im Kopfbereich des Administrator-Tools auf **Einstellungen > verwalten**.

Die Seite **Einstellungen** erscheint.

3. Klicken Sie im Abschnitt "Benutzereinstellungen" auf **Bearbeiten**.

Das Dialogfeld **Einstellungen bearbeiten** erscheint.

4. Wählen Sie **Alarmer abbonieren** aus.

5. Klicken Sie auf **OK**.

6. Klicken Sie auf **OK**.

Der Service Manager schickt E-Mails mit Warnmeldungen entsprechend Ihren Domänen-Berechtigungen.

Die folgende Tabelle listet die Alarmtypen und Ereignisse für Benachrichtigungs-E-Mails auf:

Alarmtyp	Ereignis
Domäne	Knotenfehler Master Gateway Election
Dienst	Dienstprozess Failover

Alarmer anzeigen

Wenn Sie Alarmer abonnieren, erhalten Sie zu bestimmten Ereignissen Domänen- und Dienstbenachrichtigungen per E-Mail. Tritt in der Domäne oder dem Dienst ein Ereignis auf, das die Benachrichtigung auslöst, können Sie den Alarmstatus wie folgt nachverfolgen:

- Der Service Manager schickt an alle Abonnenten, die für diese Domäne oder diesen Dienst die entsprechenden Berechtigungen haben, eine E-Mail mit der Alarmbenachrichtigung.
- Der Log-Manager protokolliert die erfolgreiche oder fehlgeschlagene Zustellung der Alarmbenachrichtigung im Domänen- oder Dienstprotokoll.

Zum Beispiel: Der Service Manager schickt die folgende Benachrichtigung an alle Abonnenten, die für den fehlerhaften Dienst die entsprechenden Berechtigungen haben:

```
From: Administrator@<database host>
To: Jon Smith
Subject: Alert message of type [Service] for object [HR_811].
The service process on node [node01] for service [HR_811] terminated unexpectedly.
```

Ferner schreibt der Protokoll-Manager die folgende Meldung in das Dienstprotokoll:

```
ALERT_10009 Alert message [service process failover] of type [service] for object
[HR_811] was successfully sent.
```

Sie können die Protokolle der Domäne oder des Dienstes nach unzustellbaren E-Mails für Alarmbenachrichtigungen durchsehen. Im Domänenprotokoll filtern Sie nach der Kategorie Alarmer. Im Dienstprotokoll suchen Sie nach dem Meldungscode ALERT. Wenn der Service Manager keine E-Mail zur Alarmbenachrichtigung versenden kann, erscheint folgende Meldung im Domänen- oder Dienstprotokoll:

```
ALERT_10004: Unable to send alert of type [alert type] for object [object name], alert
message [alert message], with error [error].
```

Ordnerverwaltung

Verwenden Sie Ordner in der Domäne, um Objekte zu organisieren und die Sicherheit zu verwalten.

Ordner können Knoten, Dienste, Gitter, Lizenzen und andere Ordner enthalten. Möglicherweise brauchen Sie Ordner ebenfalls zum Gruppieren der Dienste nach Typ. So können Sie zum Beispiel einen Ordner anlegen, den Sie IntegrationServices nennen, und alle Integration Services dort hineinschieben. Oder Sie erstellen Ordner zum Gruppieren aller Dienste für einen Funktionsbereich, wie Vertrieb oder Finanzen.

Wenn Sie eine Benutzerberechtigung für den Ordner festlegen, erbt der Benutzer die Berechtigung für sämtliche Objekte in diesem Ordner.

Mit Ordnern können Sie folgende Tasks durchführen:

- Anzeigen von Diensten und Knoten. Anzeigen aller Dienste in dem Ordner und der Knoten, auf denen sie ausgeführt werden. Anklicken eines Konten- oder Dienstnamens für den Zugriff auf die Eigenschaften dieses Knotens oder Dienstes.
- Ordner erstellen. Ordner zum Gruppieren von Objekten in der Domäne erstellen.
- Verschieben von Objekten in Ordner. Wenn Sie ein Objekt in einen Ordner verschieben, erben die Benutzer des Ordners die Berechtigung für das Objekt im Ordner. Beim Verschieben eines Ordners in einen anderen Ordner wird der andere Ordner zum übergeordneten Ordner des verschobenen Ordners.
- Entfernen von Ordnern. Wenn Sie einen Ordner entfernen, können Sie die Objekte in dem Ordner löschen oder in den übergeordneten Ordner verschieben.

Hinweis: Der Ordner System_Services wird bei Erstellung der Domäne für Sie erstellt und enthält alle Systemdienste. Ein Systemdienst ist ein Anwendungsdienst, der in der Domäne eine einzelne Instanz haben

kann. Die Eigenschaften oder Inhalte des Ordners System_Services können nicht gelöscht, verschoben oder bearbeitet werden.

Erstellen eines Ordners

Sie können einen Ordner in der Domäne oder in einem anderen Ordner erstellen.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten** > Ansicht **Dienste und Knoten**.
2. Wählen Sie im Domänen-Navigator die Domäne oder den Ordner aus, in der bzw. dem Sie einen Ordner erstellen möchten.
3. Im Menü Navigator-Aktionen klicken Sie auf Neu > Ordner.
4. Bearbeiten Sie die folgenden Eigenschaften:

Eigenschaft „Knoten“	Beschreibung
Name	Name des Ordners. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Er darf nicht länger als 80 Zeichen sein oder mit @ beginnen. Außerdem darf er weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () []
Beschreibung	Beschreibung des Ordners. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Pfad	Speicherort im Navigator.

5. Klicken Sie auf OK.

Objekte in einen Ordner verschieben

Wenn Sie ein Objekt in einen Ordner verschieben, erben die Ordnerbenutzer die Berechtigung für das Objekt. Wenn Sie einen Ordner in einen anderen Ordner verschieben, wird der verschobene Ordner zu einem untergeordneten Objekt des Ordners, in dem er sich befindet.

Hinweis: Die Domäne dient als Ordner, wenn Sie Objekte in Ordner und aus Ordnern verschieben.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten** > Ansicht **Dienste und Knoten**.
2. Wählen Sie im Domänen-Navigator ein Objekt aus.
3. Im Menü Aktionen des Navigation wählen Sie "In Ordner verschieben".
4. Im Dialogfeld Ordner auswählen, markieren Sie einen Ordner und klicken auf OK.

Entfernen eines Ordners

Wenn Sie einen Ordner entfernen, können Sie die Objekte im Ordner löschen oder in den übergeordneten Ordner verschieben.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten** > Ansicht **Dienste und Knoten**.
2. Wählen Sie im Domänen-Navigator einen Ordner aus.
3. Im Menü Aktionen des Navigators wählen Sie "Löschen".
4. Bestätigen Sie, dass Sie den Ordner löschen möchten.

Sie können die Inhalte nur löschen, wenn Sie die entsprechenden Berechtigungen für alle Objekte in dem Ordner besitzen.

5. Wählen Sie aus, ob Sie warten möchten, bis alle Prozesse abgeschlossen sind, oder ob alle Prozesse abgebrochen werden sollen.
6. Klicken Sie auf OK.

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.

Anwendungsdienstverwaltung

Folgende Verwaltungstasks lassen sich für Anwendungsdienste ausführen:

- Dienste und Dienstprozesse aktivieren und deaktivieren.
- Die Domäne für den Neustart von Dienstprozessen konfigurieren.
- Anwendungsdienste entfernen.
- Probleme mit einem Anwendungsdienst beheben.

Hinweis: Sie können alle allgemeinen Verwaltungsaufgaben für Systemdienste ausführen, bis auf das Entfernen des Systemdiensts.

Aktivieren und Deaktivieren von Diensten und Dienstprozessen

Anwendungsdienste und Dienstprozesse aktivieren und deaktivieren können Sie im Administrator-Tool. Ist ein Dienst aktiviert, muss mindesten ein Dienstprozess aktiviert sein und ausgeführt werden, damit der Dienst verfügbar ist. Per Standard sind alle Dienstprozesse aktiviert.

Das Verhalten eines Diensts beim Starten von Dienstprozessen ist von seiner Konfiguration abhängig:

- Ist der Dienst für hohe Verfügbarkeit konfiguriert, dann startet er den Dienstprozess auf dem Primärknoten. Die Dienstprozesse auf den Backup-Knoten befinden sich im Status „Im Wartezustand“.
- Ist der Dienst für die Ausführung auf einem Gitter konfiguriert, dann startet er Dienstprozesse auf allen Knoten mit der Dienstrolle.

Einen deaktivierten Dienstprozess startet ein Dienst unter keinen Umständen.

Der Status eines Diensts ist vom Status seiner Prozesse abhängig. Ein Dienst kann folgenden Status haben:

- Verfügbar. Sie haben den Dienst aktiviert und mindestens ein Dienstprozess wird ausgeführt. Der Dienst steht für die Bearbeitung von Anfragen zur Verfügung.
- Nicht verfügbar. Sie haben den Dienst aktiviert und keiner seiner Prozesse wird ausgeführt. Dies kann daran liegen, dass die Dienstprozesse deaktiviert sind oder nicht gestartet werden konnten. Der Dienst steht nicht zur Bearbeitung von Anfragen zur Verfügung.
- Deaktiviert. Sie haben den Dienst deaktiviert.

Sie können einen Dienst deaktivieren, um einen Verwaltungsaufgaben durchzuführen, wie Ändern des Datenverschiebungsmodus für einen PowerCenter Integration Service. Vielleicht müssen Sie den Dienstprozess auf einem Knoten deaktivieren, wenn Sie den Knoten zu Wartungszwecken herunterfahren müssen. Wenn Sie einen Dienst deaktivieren, werden alle zugeordneten Dienstprozesse angehalten, bleiben aber aktiviert.

Die folgende Tabelle beschreibt, welche Status ein Dienst und seine Prozesse haben können:

Dienstprozess-Konfiguration	Dienstprozess-Status	Beschreibung
Aktiviert	Wird ausgeführt	Der Dienstprozess läuft auf dem Knoten.
Aktiviert	Im Wartezustand	Der Dienstprozess ist aktiviert, wird jedoch nicht ausgeführt, da ein anderer Dienstprozess als primärer Dienstprozess ausgeführt wird. Er befindet sich im Standby, um bei Failover des Dienstes ausgeführt zu werden.
Deaktiviert	Deaktiviert	Der Dienst ist aktiviert, aber der Dienstprozess wird auf dem Knoten nicht ausgeführt.
Aktiviert	Gestoppt	Der Dienst ist nicht verfügbar.
Aktiviert	Fehlgeschlagen	Dienst und Dienstprozess sind aktiviert, aber der Dienstprozess konnte nicht starten.

Dienstprozesse anzeigen

Sie können den Status eines Dienstprozesses anzeigen, indem Sie in die Prozessansicht eines Dienstes wechseln. Sie können den Status aller Dienstprozesse in der Übersichtsansicht der Domäne anzeigen. Um den Status aller Dienstprozesse anzuzeigen verfahren Sie wie folgt:

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten** > Ansicht **Dienste und Knoten**.
2. Wählen Sie im Domänen-Navigator einen Dienst aus.
3. Klicken Sie im Inhaltsbereich auf die Ansicht "Prozesse".

In der Prozessansicht wird der Status der Prozesse dargestellt.

Konfigurieren des Neustarts für Dienstprozesse

Wird ein Anwendungsdienstprozess bei laufendem Knoten nicht verfügbar, versucht die Domäne, den Prozess auf demselben Knoten basierend auf den in den Domäneneigenschaften konfigurierten Neustartoptionen neu zu starten.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten** > Ansicht **Dienste und Knoten**.
2. Wählen Sie im Domänen-Navigator die Domäne aus.
3. Konfigurieren Sie in der Ansicht "Eigenschaften" die folgenden Neustarteigenschaften:

Domäneneigenschaft	Beschreibung
Maximale Versuche für Neustart	Gibt an, wie oft die Domäne im angegebenen Zeitraum versucht, einen Anwendungsdienstprozess zu starten, der fehlschlägt. Der Wert muss größer oder gleich 1 sein. Standardwert ist 3.
Innerhalb des Neustartzeitraums (Sek.)	Maximaler Zeitraum, in dem die Domäne versucht, einen Anwendungsdienstprozess neu zu starten, der fehlschlägt. Wenn ein Dienst nicht nach der angegebenen Anzahl von Versuchen in diesem Zeitraum startet, startet er überhaupt nicht. Standardwert ist 900.

Anwendungsdienste entfernen

Sie können einen Anwendungsdienst über das Administrator Tool löschen. Bevor Sie einen Anwendungsdienst entfernen, müssen Sie ihn deaktivieren.

Hinweis: Sie können einen Systemdienst nicht entfernen.

Deaktivieren Sie den Dienst, bevor Sie ihn löschen, um sicherzustellen, dass der Dienst keine Prozesse ausführt. Wenn Sie den Dienst nicht deaktivieren, können beim Löschen des Dienstes wählen zu warten, bis alle Prozesse abgeschlossen sind, oder alle Prozesse abubrechen.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten** > Ansicht **Dienste und Knoten**.
2. Wählen Sie im Domänen-Navigator den Anwendungsdienst aus.
3. Wählen Sie auf der Registerkarte **Verwalten** im Menü „Aktionen“ **Löschen** aus.
4. Klicken Sie in der daraufhin angezeigten Warnmeldung auf **Ja**, um andere Dienste zu stoppen, die von dem Anwendungsdienst abhängig sind.
5. Wenn das Dialogfeld **Dienst deaktivieren** angezeigt wird, warten Sie entweder, bis alle Prozesse abgeschlossen sind, oder brechen Sie alle Prozesse ab und klicken Sie dann auf **OK**.

Problembehebung für Anwendungsdienste

Ich habe den Eindruck, dass ein Dienst falsche Werte für die Umgebungsvariablen benutzt. Wie kann ich herausfinden, welche Umgebungsvariablenwerte von einem Dienst verwendet werden?

Setzen Sie den Fehlerschweregrad für den Knoten auf Debug. Wenn der Dienst auf dem Knoten startet, zeigt der Domänen-Log die Umgebungsvariablen an, die der Dienst verwendet.

Gateway-Konfiguration

Für eine Domäne muss mindestens ein Knoten als Gateway-Knoten konfiguriert werden. Sie können mehrere Gateway-Knoten als Backup konfigurieren.

Ein Gateway-Knoten in der Domäne dient als Master-Gateway-Knoten für die Domäne. Der Dienstmanager auf dem Master-Gateway-Knoten nimmt Dienstanfragen entgegen und verwaltet die Domäne und die Dienste in der Domäne. Wenn die Domäne nur über einen Gateway-Knoten verfügt und dieser ausfällt, kann die Domäne keine Dienstanfragen mehr annehmen. Wenn die Domäne über mehrere Gateway-Knoten verfügt und der Master-Gateway-Knoten nicht verfügbar ist, wählen die Dienstmanager auf den anderen Gateway-Knoten einen neuen Master-Gateway-Knoten aus. Der neue Master-Gateway-Knoten nimmt Dienstanfragen entgegen. Zu einem gegebenen Zeitpunkt kann nur ein Gateway-Knoten als Master-Gateway-Knoten festgelegt sein.

Sie können an der Gateway-Konfiguration die folgenden Änderungen für die Domäne vornehmen:

Einen Worker-Knoten in einen Gateway-Knoten konvertieren.

Sie können einen Worker-Knoten in einen Gateway-Knoten konvertieren, wenn der Worker-Knoten ausgeführt wird und die Dienstrolle aktiviert ist. Wenn Sie einen Worker-Knoten in einen Gateway-Knoten konvertieren, müssen Sie das Protokollverzeichnis für den Knoten festlegen. Bei mehreren Gateway-Knoten müssen Sie alle Gateway-Knoten so konfigurieren, dass die Protokolldateien in dasselbe Verzeichnis auf einer gemeinsamen Festplatte geschrieben werden.

Nach dem Konvertieren eines Worker-Knotens in einen Gateway-Knoten schreibt der Dienstmanager des Master-Gateway-Knotens die Verbindung der Domänen-Konfigurationsdatenbank in die Datei `nodemeta.xml` des neuen Gateway-Knotens.

Einen Gateway-Knoten in einen Worker-Knoten konvertieren.

Sie können einen Gateway-Knoten in einen Worker-Knoten konvertieren, wenn ein anderer Knoten in der Domäne als Gateway-Knoten konfiguriert ist.

Wenn Sie einen Master-Gateway-Knoten in einen Worker-Knoten konvertieren, müssen Sie den Knoten neu starten, damit die Dienstmanager einen neuen Master-Gateway-Knoten wählen. Ohne Neustart des Knotens bleibt die Funktion des Master-Gateway-Knotens bestehen, bis Sie den Knoten neu starten oder der Knoten nicht mehr verfügbar ist.

Konfigurieren von Gateway- und Worker-Knoten

Sie können einen vorhandenen Worker-Knoten in einen Gateway-Knoten umwandeln. Alternativ können Sie einen vorhandenen Gateway-Knoten in einen Worker-Knoten umwandeln.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten** > Ansicht **Dienste und Knoten**.
2. Wählen Sie die Domäne im Domänennavigator aus.
3. Wählen Sie in der Inhaltsübersicht die Ansicht **Eigenschaften** aus.
4. Klicken Sie in der Ansicht **Eigenschaften** im Abschnitt **Gateway-Konfigurationseigenschaften** auf **Bearbeiten**.
5. Um einen Worker-Knoten in einen Gateway-Knoten umzuwandeln, führen Sie die folgenden Schritte durch:
 - a. Wählen Sie das Kontrollkästchen neben dem Knoten aus.
 - b. Wenn die Domäne eine sichere Domänen-Konfigurationsdatenbank verwendet, müssen Sie die Truststore-Datei und das Passwort für die Datenbank angeben.
 - c. Konfigurieren Sie den Verzeichnispfad für die Protokolldateien für jeden Knoten, den Sie in einen Gateway-Knoten umwandeln möchten.

Bei mehreren Gateway-Knoten müssen Sie alle Gateway-Knoten so konfigurieren, dass die Protokolldateien in dasselbe Verzeichnis auf einer gemeinsamen Festplatte geschrieben werden.

Hinweis: Sie müssen den Befehl „`infacmd isp SwitchToWorkerNode`“ verwenden, um einen Worker-Knoten in einen Gateway-Knoten in einer Domäne umzuwandeln, die für die Verwendung der SAML-Authentifizierung konfiguriert ist. Anweisungen zur Verwendung des Befehls „`infacmd isp SwitchToWorkerNode`“ finden Sie in der *Informatica-Befehlsreferenz*.

6. Um einen Gateway-Knoten in einen Worker-Knoten umzuwandeln, deaktivieren Sie das Kontrollkästchen neben dem Knoten.
7. Klicken Sie auf **OK**.

Domänenkonfigurationsverwaltung

Der Service Manager auf dem Master-Gateway-Knoten verwaltet die Domänenkonfiguration. Die Domänenkonfiguration besteht aus einer Reihe von Metadatatabellen, die in einer für alle Gateway-Knoten in der Domäne zugänglichen relationalen Datenbank gespeichert sind. Immer wenn Sie eine Änderung an der Domäne vornehmen, schreibt der Service Manager die Änderung in die Domänenkonfiguration. Beispiel: Beim Hinzufügen eines Knotens zur Domäne fügt der Service Manager die Knoteninformationen zur

Domänenkonfiguration hinzu. Die Gateway-Knoten greifen mittels JDBC-Verbindung auf die Domänenkonfigurations-Datenbank zu.

Sie können folgenden Domänenkonfigurations-Verwaltungstasks ausführen:

- Domänenkonfiguration sichern Sichern Sie die Domänenkonfiguration regelmäßig. Ist die Domänenkonfiguration in der Datenbank verfälscht, müssen Sie die Domänenkonfiguration möglicherweise aus einer Sicherung wiederherstellen.
- Stellen Sie die Domänenkonfiguration wieder her. Vielleicht müssen Sie die Domänenkonfiguration auch wiederherstellen, wenn Sie die Domänenkonfiguration zu einem anderen Datenbank-Benutzerkonto migrieren. Oder Sie müssen die Sicherungs-Domänenkonfiguration in einem Datenbankbenutzerkonto wiederherstellen.
- Migrieren Sie die Domänenkonfiguration. Unter Umständen müssen Sie die Domänenkonfiguration zu einem anderen Datenbank-Benutzerkonto migrieren.
- Konfigurieren Sie die Verbindung zur Domänenkonfigurations-Datenbank. Jeder Gateway-Knoten muss Zugriff auf die Domänenkonfigurations-Datenbank haben. Die Datenbankverbindung wird beim Erstellen der Domäne konfiguriert. Wenn Sie die Datenbank-Verbindungsinformationen ändern oder die Domänenkonfiguration in eine neue Datenbank migrieren, müssen Sie die Datenbank-Verbindungsinformationen für jeden Gateway-Knoten aktualisieren.
- Konfigurieren Sie benutzerdefinierte Eigenschaften. Konfigurieren Sie Domäneneigenschaften, die für Ihre Umgebung eindeutig sind oder in bestimmten Fällen angewendet werden. Benutzerdefinierte Eigenschaften dürfen Sie nur verwenden, wenn Sie vom globalen Kundensupport von Informatica entsprechende Anweisungen erhalten.

Hinweis: Die Domänenkonfigurations-Datenbank und das Model Repository dürfen nicht dasselbe Datenbankbenutzerschema verwenden.

Sichern der Domänenkonfiguration

Sichern Sie die Domänenkonfiguration regelmäßig. Sie können die Domänenkonfiguration von einer Sicherungsdatei wiederherstellen, wenn die Domänenkonfiguration in der Datenbank korrupt wird.

Führen Sie den Befehl *infasetup BackupDomain* aus, um die Domänenkonfiguration in einer Binärdatei zu sichern.

Hinweis: Wenn der *infasetup*-Befehl „BackupDomain“ mit einem Java-Speicherfehler fehlschlägt, stellen Sie für „infasetup“ mehr Systemspeicher zur Verfügung. Um den Systemspeicher zu vergrößern, legen Sie den -Xmx-Wert in der Umgebungsvariablen `INFA_JAVA_CMD_OPTS` fest.

Beim Ausführen dieses Befehls sichert *infasetup* die Datenbanktabellen für die Domänenkonfiguration. Zum Wiederherstellen der Domäne in einer anderen Datenbank müssen Sie die Inhalte der Tabelle `ISP_RUN_LOG` manuell sichern, um die vorherigen Arbeitsablauf- und Sitzungsprotokolle zu erhalten.

Verwenden Sie zusätzlich das Dienstprogramm zur Datenbanksicherung, um zusätzliche Repository-Tabellen manuell zu sichern, die vom *infasetup*-Befehl nicht gesichert werden.

Wiederherstellen der Domänen-Konfiguration

Sie können eine Domänenkonfiguration aus einer Repository-Backup-Datei wiederherstellen. Unter Umständen müssen Sie die Domänenkonfiguration wiederherstellen, wenn die Domänenkonfiguration in der Datenbank inkonsistent wird oder Sie die Domänenkonfiguration in eine andere Datenbank migrieren möchten.

Informatica stellt die Domänenkonfiguration aus der aktuellen Version wieder her. Wenn Sie über eine Backup-Datei aus einer früheren Produktversion verfügen, müssen Sie die frühere Produktversion verwenden, um die Domänenkonfiguration wiederherzustellen.

Sie können die Domänenkonfiguration in dasselbe oder ein anderes Datenbankbenutzerkonto migrieren. Bei der Wiederherstellung der Domänenkonfiguration in ein Datenbankbenutzerkonto mit einer vorhandenen Domänenkonfiguration müssen Sie den Befehl so konfigurieren, dass die bestehende Domänenkonfiguration überschrieben wird. Wenn Sie den Befehl nicht für das Überschreiben der bestehenden Domänenkonfiguration konfigurieren, schlägt der Befehl fehl.

Jeder Knoten in einer Domäne verfügt über einen Hostnamen und eine Portnummer. Wenn Sie die Domänenkonfiguration wiederherstellen, können Sie die Verknüpfung mit Hostnamen und Portnummern für alle Knoten in der Domäne aufheben. Dies ist sinnvoll, wenn Sie die Knoten auf unterschiedlichen Rechnern laufen lassen möchten. Nachdem Sie die Domänenkonfiguration wiederhergestellt haben, können Sie neue Hostnamen und Portnummern mit den Knoten verknüpfen. Führen Sie den Befehl *infasetup* `DefineGatewayNode` oder `DefineWorkerNode` aus, um einem Knoten einen neuen Hostnamen und eine neue Portnummer zuzuweisen.

Wenn Sie die Domänenkonfiguration in eine andere Datenbank wiederherstellen, müssen Sie die Datenbankverbindungen für alle Gateway-Knoten zurücksetzen.

Wichtig: Sie verlieren alle Daten in den Übersichtstabellen, wenn Sie die Domänenkonfiguration wiederherstellen.

Führen Sie folgende Tasks durch, um die Domäne wiederherzustellen:

1. Deaktivieren Sie den Dienst. Fahren Sie die Anwendungsdienste im vollständigen Modus herunter, um sicherzustellen, dass Sie keine laufenden Dienstprozesse abbrechen. Sie müssen die Anwendungsdienste deaktivieren, um sicherzustellen, dass beim Herunterfahren der Domäne kein Dienstprozess ausgeführt wird.
2. Abschalten der Domäne. Sie müssen die Domäne abschalten, um sicherzustellen, dass während der Wiederherstellung der Domäne keine Änderungen an der Domäne vorgenommen werden.
3. Führen Sie den Befehl *infasetup* `RestoreDomain` aus, um die Domänenkonfiguration in eine Datenbank wiederherzustellen. Der Befehl `RestoreDomain` stellt die Domänenkonfiguration aus der Backup-Datei im angegebenen Datenbankbenutzerkonto wieder her.
4. Weisen Sie nach der Wiederherstellung der Domänenkonfiguration den Knoten in der Domäne neue Hostnamen und Portnummern zu, wenn Sie die Verknüpfung mit den vorherigen Hostnamen und Portnummern aufgehoben haben. Führen Sie den Befehl *infasetup* `DefineGatewayNode` oder `DefineWorkerNode` aus, um einem Knoten einen neuen Hostnamen und eine neue Portnummer zuzuweisen.
5. Setzen Sie die Datenbankverbindungen für alle Gateway-Knoten zurück, wenn Sie die Domänenkonfiguration in eine andere Datenbank wiederherstellen. Alle Gateway-Knoten müssen eine Verbindung zur Domänenkonfigurationsdatenbank haben.

Migrieren der Domänen-Konfiguration

Sie können die Domänenkonfiguration in ein anderes Datenbankbenutzerkonto migrieren. Unter Umständen müssen Sie die Domänenkonfiguration migrieren, wenn Sie das vorhandene Datenbankbenutzerkonto nicht mehr unterstützen. Zum Beispiel: Wenn in Ihrem Unternehmen alle Abteilungen auf einen neuen Datenbanktyp migrieren müssen, müssen Sie auch die Domänenkonfiguration migrieren.

1. Abschalten aller Anwendungsdienste in der Domäne.
2. Abschalten der Domäne.
3. Backup der Domänenkonfiguration erstellen.
4. Erstellen Sie das Datenbankbenutzerkonto dort, wo die Domänenkonfiguration wiederhergestellt werden soll.
5. Stellen Sie das Backup der Domänenkonfiguration im Datenbankbenutzerkonto wieder her.

6. Aktualisieren Sie die Datenbankverbindung für jeden Gateway-Knoten.
7. Starten Sie alle Knoten in der Domäne.
8. Aktivieren Sie alle Anwendungsdienste in der Domäne.

Wichtig: Zusammenfassungstabellen gehen verloren, wenn Sie die Domänenkonfiguration wiederherstellen.

Schritt 1. Alle Anwendungsdienste deaktivieren

Sie müssen alle Anwendungsdienste deaktivieren, um alle Dienstprozesse zu deaktivieren. Wenn Sie einen Anwendungsdienst nicht deaktivieren und ein Benutzer einen Dienstprozess startet, während Sie die Domäne sichern und wiederherstellen, können die Änderungen des Dienstprozesses verloren gehen, und die Daten können beschädigt werden.

Deaktivieren Sie Anwendungsdienste im vollständigen Modus, um sicherzustellen, dass Sie keine laufenden Dienstprozesse abbrechen.

Deaktivieren Sie die Anwendungsdienste in der nachstehenden Reihenfolge:

1. Webdienst-Hub
2. SAP BW-Dienst
3. Metadata Manager-Dienst
4. PowerCenter-Integrationsdienst
5. PowerCenter-Repository-Dienst
6. Suchdienst
7. Analyst-Dienst
8. Content-Managementdienst
9. Datenintegrationsdienst
10. Modellrepository-Dienst

Schritt 2. Domäne herunterfahren

Sie müssen die Domäne herunterfahren, um sicherzustellen, dass die Benutzer die Domäne nicht verändern, während Sie die Domänenkonfiguration migrieren. Zum Beispiel: Wenn die Domäne ausgeführt wird, während Sie die Domänenkonfiguration sichern, können Benutzer einen neuen Dienst und neue Objekte erstellen. Hinzu kommt: Wenn Sie die Domäne nicht herunterfahren und die Domänenkonfiguration in einer anderen Datenbank wiederherstellen, ist die Domäne nicht mehr betriebsfähig. Die Verbindungen zwischen den Gateway-Knoten und der Domänenkonfigurationsdatenbank werden ungültig. Die Gateway-Knoten werden heruntergefahren, denn sie können keine Verbindung zur Domänenkonfigurationsdatenbank herstellen. Eine Domäne ist nicht betriebsfähig, wenn sie nicht über einen ausgeführten Gateway-Knoten verfügt.

Schritt 3. Domänenkonfiguration sichern

Führen Sie den Befehl `infasetup BackupDomain` aus, um die Domänenkonfiguration in einer Binärdatei zu sichern.

Schritt 4. Benutzerkonto für Datenbank erstellen

Erstellen Sie ein Datenbankbenutzerkonto, wenn Sie die Domänenkonfiguration in einem neuen Datenbankbenutzerkonto wiederherstellen möchten.

Schritt 5. Domänenkonfiguration wiederherstellen

Führen Sie den Befehl *infasetup RestoreDomain* aus, um die Domänenkonfiguration in einer Datenbank wiederherzustellen. Der Befehl *RestoreDomain* stellt die Domänenkonfiguration aus der Sicherungsdatei im angegebenen Benutzerkonto der Datenbank wieder her.

Schritt 6. Datenbankverbindung prüfen

Wenn Sie die Domänenkonfiguration in einem anderen Datenbankbenutzerkonto wiederherstellen, müssen Sie die Datenbankverbindungsinformationen für jeden Gateway-Knoten in der Domäne aktualisieren. Gateway-Knoten müssen eine Verbindung zur Domänenkonfigurationsdatenbank haben, um die Domänenkonfiguration laden und aktualisieren zu können.

Schritt 7. Knoten in der Domäne starten

Starten Sie alle Knoten in der Domäne. Sie müssen die Knoten starten, um die Dienste für die Ausführung zu aktivieren.

1. Fahren Sie den Gateway-Knoten herunter, den Sie aktualisieren möchten.
2. Führen Sie den Befehl *infasetup UpdateGatewayNode* aus, um den Gateway-Knoten zu aktualisieren.
3. Starten Sie den Gateway-Knoten.
4. Wiederholen Sie diesen Vorgang für jeden Gateway-Knoten.

Schritt 8. Alle Anwendungsdienste aktivieren

Aktivieren Sie alle Anwendungsdienste, die Sie zuvor heruntergefahren haben. Die Anwendungsdienste müssen aktiv sein, um die Dienstprozesse auszuführen.

Aktualisieren der Domänenkonfigurationsdatenbankverbindung

Alle Gateway-Knoten müssen eine Verbindung zur Domänenkonfigurationsdatenbank haben, um die Domänenkonfiguration abzurufen und zu aktualisieren. Wenn Sie einen Gateway-Knoten erstellen oder einen Knoten als Gateway konfigurieren, geben Sie die Datenbankverbindung einschließlich des Benutzernamens und Passworts der Datenbank ein. Wenn Sie die Domäne auf eine andere Datenbank migrieren oder den Datenbankbenutzernamen oder das Passwort ändern, müssen Sie die Datenbankverbindung für jede Gateway-Knoten aktualisieren. Zum Beispiel könnte Ihr Unternehmen im Rahmen einer Sicherheitspolitik verlangen, dass Sie das Passwort für die Domänen-Konfigurationsdatenbank alle drei Monate ändern.

Um den Knoten mit der neuen Datenbankverbindung zu aktualisieren, führen Sie folgende Schritte durch:

1. Abschalten des Gateway-Knotens.
2. Ausführen des Befehls *infasetup UpdateGatewayNode*.

Wenn Sie den Benutzernamen und das Passwort ändern, müssen Sie den Knoten aktualisieren.

Um den Knoten nach der Änderung des Benutzers oder Passworts zu aktualisieren, führen Sie folgende Schritte durch:

1. Abschalten des Gateway-Knotens.
2. Ausführen des Befehls *infasetup UpdateGatewayNode*.

Wenn Sie den Hostnamen oder die Portnummer ändern, müssen Sie den Knoten neu definieren.

Um den Knoten nach der Änderung des Hostnamens oder der Portnummer neu zu definieren, führen Sie folgende Schritte durch:

1. Abschalten des Gateway-Knotens.
2. Entfernen der Knotenzuweisung im Administrator Tool.
3. Ausführen des Befehls *infasetup* DefineGatewayNode.

Umbenennen der Domäne

Sie können den Domänennamen ändern und Knoten aktualisieren, um auf den aktualisierten Domänennamen zu verweisen.

Wenn die Informatica-Domäne Kerberos-Authentifizierung verwendet, weisen alle Dienst- und Knoten-SPNs denselben Kerberos-Bereichsnamen auf. Nach dem Ändern des Informatica-Domänennamens müssen Sie SPNs und Keytab-Dateien mit dem neuen Informatica-Domänennamen erzeugen.

Führen Sie zum Umbenennen der Domäne die folgenden Aufgaben aus:

1. Wenn die Domäne ein globales PowerCenter-Repository enthält, müssen Sie die Registrierung aller lokalen Repositories mit dem globalen Repository aufheben.
2. Fahren Sie die Domäne herunter. Fahren Sie die Domäne über das Administrator Tool herunter und stellen Sie sicher, dass alle Knoten heruntergefahren werden.
3. Sichern Sie die Domäne mit dem Befehl „*infasetup BackupDomain*“.
4. Sichern Sie die Sitekey- und Keytab-Dateien. Standardmäßig befinden sich die Dateien in folgendem Speicherort:

```
<Informatica installation directory>/isp/config/keys
```

5. Aktualisieren Sie die Domäne und die Knoten.

Um den Domänennamen zu aktualisieren, führen Sie den Befehl „*infasetup updateDomainName*“ von einem beliebigen Gateway-Knoten aus.

Führen Sie die Befehle „*updateGatewayNode*“ und „*updateWorkerNode*“ mit dem aktualisierten Domänennamen für alle Gateway- und Worker-Knoten aus.

6. Registrieren Sie in PowerCenter unter Verwendung des Befehls „*pmrep Register*“ das lokale Repository mit einem verbundenen globalen Repository und dem aktualisierten Domänennamen.
7. Sie können SPN und Keytab-Dateien mit dem aktualisierten Domänennamen für die Kerberos-Authentifizierung erstellen. Kopieren Sie die Keytab-Dateien in das Schlüsselverzeichnis. Sie können die ältere Standortschlüsseldatei weiter verwenden. Wenn Sie einen fehlenden oder fehlerhaften Standortschlüssel erneut generieren müssen, müssen Sie den älteren Domänennamen angeben.
8. Optional können Sie den Lizenzverwaltungsbericht im Administrator Tool ausführen, um den aktualisierten Domänennamen zu überprüfen.
9. Sie müssen die Informatica-Clients für die Verwendung des aktualisierten Domänennamens konfigurieren.

Herunterfahren einer Domäne

Um administrative Aufgaben in einer Domäne ausführen zu können, müssen Sie die Domäne eventuell herunterfahren. Beispielsweise müssen Sie zum Sichern und Wiederherstellen einer Domänenkonfiguration zunächst die Domäne herunterfahren.

Beim Herunterfahren einer Domäne stoppt der Dienstmanager auf dem Master-Gateway-Knoten alle Anwendungsdienste und Informatica-Dienste in der Domäne. Alle Dienstprozesse, die auf Knoten in der Domäne ausgeführt werden, werden abgebrochen. Um einen möglichen Daten- oder Metadatenverlust zu vermeiden, und damit die laufenden Prozesse abgeschlossen werden können, können Sie jeden einzelnen Knoten über das Administrator Tool oder das Betriebssystem herunterfahren.

Stellen Sie vor dem Herunterfahren einer Domäne sicher, dass alle Prozesse, einschließlich Arbeitsabläufe, abgeschlossen sind und keine Benutzer bei Repositories in der Domäne angemeldet sind.

1. Klicken Sie auf die Registerkarte **Verwalten**.
2. Klicken Sie auf die Ansicht **Dienste und Knoten**.
3. Wählen Sie die Domäne im Navigator aus.
4. Klicken Sie auf die Registerkarte **Verwalten > Aktionen > Domäne herunterfahren**.

Im Dialogfeld **Domäne herunterfahren** werden die Prozesse aufgelistet, die in der Domäne ausgeführt werden.

5. Klicken Sie auf **Herunterfahren**.

Im Dialogfeld **Domäne herunterfahren** wird eine Warnmeldung angezeigt.

6. Klicken Sie auf **Herunterfahren**.

Der Dienstmanager auf dem Master-Gateway-Knoten fährt alle Anwendungsdienste und Informatica-Dienste auf jedem Knoten in der Domäne herunter.

7. Zum Neustart der Domäne starten Sie die Informatica-Dienste auf den Gateway- und Worker-Knoten in der Domäne neu.

Domäneneigenschaften

Auf der Registerkarte **Verwalten** können Sie Domäneneigenschaften einschließlich Datenbankeigenschaften, Gateway-Konfiguration und Dienstebenen konfigurieren.

Klicken Sie auf die Registerkarte **Verwalten**, um Eigenschaften anzuzeigen und zu bearbeiten. Wählen Sie im Navigator eine Domäne aus. Dann klicken Sie auf **Eigenschaften**, um die Inhaltsangabe einzublenden. In der Inhaltsübersicht stehen die Domäneneigenschaften.

Sie können die Eigenschaften konfigurieren, wenn Sie die Domäne ändern möchten. Sie können die Datenbankeigenschaften in der Admin Console nicht ändern. Sie müssen diese Eigenschaften mit dem Befehl „UpdateGatewayNode“ ändern. Sie können SMTP-Eigenschaften für Warnungen und die Eigenschaften der Domänenfallsicherheit ändern.

Sie können die folgenden Domäneneigenschaften konfigurieren:

- Allgemeine Eigenschaften. Bearbeiten der allgemeinen Eigenschaften wie Dienstbelastbarkeit und Dispatch-Modus.
- Datenbankeigenschaften. Anzeigen der Datenbankeigenschaften wie Datenbankname und Datenbank-Host.

- Gateway-Konfigurationseigenschaften. Konfigurieren eines Knotens als Gateway und Angeben des Speicherorts zum Schreiben von Protokollereignissen.
- Dienstebenenverwaltung. Dienstebenen erstellen und konfigurieren.
- SMTP-Konfiguration. Bearbeiten der SMTP-Einstellungen für den Ausgangs-Mailserver zum Aktivieren der Warnmeldungen.
- Benutzerdefinierte Eigenschaften. Bearbeiten der für die Informatica-Umgebung einmaligen oder nur in Sonderfällen zutreffenden benutzerdefinierten Eigenschaften. Beim Erstellen einer Domäne hat diese keine benutzerdefinierten Eigenschaften. Benutzerdefinierte Eigenschaften dürfen Sie nur nach Anweisung des globalen Kundensupports von Informatica verwenden.

Allgemeine Eigenschaften

Im Bereich "Allgemeine Eigenschaften" können Sie allgemeine Eigenschaften für die Domäne konfigurieren.

Klicken Sie zum Bearbeiten der allgemeinen Eigenschaften auf **Bearbeiten**.

Die folgende Tabelle beschreibt die Eigenschaften, die im Bereich Allgemeine Eigenschaften bearbeitet werden können:

Eigenschaft	Beschreibung
Name	Schreibgeschützt. Der Name der Domäne.
Resistenz-Timeout	Anzahl von Sekunden, in denen ein Anwendungsdienst versucht, eine Verbindung oder eine erneute Verbindung zum PowerCenter-Repository-Dienst oder zum PowerCenter-Integrationsdienst herzustellen. Die gültigen Werte liegen im Bereich zwischen 0 und 1000000. Voreingestellt ist 30 Sekunden.
Grenzwert für Resistenz-Timeout	Maximale Anzahl von Sekunden, in denen die Anwendungs-Clients oder Anwendungsdienste versuchen können, eine Verbindung oder eine erneute Verbindung zum PowerCenter-Repository-Dienst oder zum PowerCenter-Integrationsdienst herzustellen. Standardwert ist 180 Sekunden.
Neustartzeitraum	Maximale Zeit in Sekunden, in denen die Domäne versucht, einen Anwendungsdienstprozess neu zu starten. Die gültigen Werte liegen im Bereich zwischen 0 und 1000000.
Maximale Anzahl Neustartversuche innerhalb des Neustartzeitraums	Gibt an, wie oft die Domäne versucht, einen Anwendungsdienstprozess neu zu starten. Gültige Werte sind 0 bis 1000. Wenn Sie den Wert auf 0 festlegen, versucht die Domäne nicht, den Dienstprozess neu zu starten.
Sendemodus	Der Modus, den der Load Balancer verwendet, um PowerCenter-Integrationsdienst-Aufgaben auf Knoten in einem Gitter zu verteilen. Wählen Sie einen der folgenden Sendemodi aus: <ul style="list-style-type: none"> - MetricBased - RoundRobin - Adaptiv

Eigenschaft	Beschreibung
Sichere Kommunikation aktivieren	<p>Konfiguriert Dienste zur Verwendung des TLS-Protokolls, um Daten sicher innerhalb der Domäne zu übertragen. Durch das Aktivieren sicherer Kommunikation für die Domäne verwenden Dienste sichere Verbindungen zur Kommunikation mit anderen Informatica-Anwendungsdiensten und -Clients.</p> <p>Stellen Sie sicher, dass alle Domänenknoten verfügbar sind, bevor Sie die sichere Kommunikation für die Domäne aktivieren. Wenn ein Knoten nicht verfügbar ist, können Änderungen der sicheren Kommunikation nicht auf den Dienstmanager des Knotens angewendet werden. Um die Änderungen zu übernehmen, müssen Sie die Domäne neu starten. Setzen Sie diese Eigenschaft auf True oder False.</p>
Dienstresistenz-Timeout	Die maximale Anzahl von Sekunden, die Anwendungs-Clients und Anwendungsdienste versuchen können, eine Verbindung zum Datenintegrationsdienst oder dem Modellrepository-Dienst aufzubauen. Der Standardwert ist 180 Sekunden.

Datenbankeigenschaften

Im Bereich „Datenbankeigenschaften“ können Sie die Datenbankeigenschaften für die Domäne anzeigen, z.B. den Namen und Host der Datenbank. Sie können diese Eigenschaften nicht in der Admin-Konsole bearbeiten. Sie müssen diese Eigenschaften mit dem Befehl „UpdateGatewayNode“ aktualisieren.

In der folgenden Tabelle werden die Datenbankeigenschaften beschrieben:

Eigenschaft	Beschreibung
Datenbanktyp	Datenbanktyp, der die Metadaten der Domänenkonfiguration speichert
Datenbankhost	Der Name des Computers, der die Datenbank hostet.
Datenbankport	Die von der Datenbank verwendete Portnummer.
Datenbankname	Der Name der Datenbank.
Datenbankbenutzer	Benutzerkonto für die Datenbank, die die Informationen der Domänenkonfiguration enthält.
Datenbank-TLS aktiviert	Gibt an, ob es sich bei der Datenbank für das Domänenkonfigurations-Repository um eine sichere Datenbank handelt. TRUE, wenn die Domänenkonfigurations-Repository-Datenbank sicher ist. Sie können ein sicheres Domänenkonfigurations-Repository verwenden, wenn die sichere Kommunikation für die Informatica-Domäne aktiviert ist.

Hinweis: Der Dienstmanager verwendet die DataDirect-Treiber, die in der Installation von Informatica enthalten sind. Informatica bietet keine Unterstützung für die Verwendung von anderen Datenbanktreibern.

Gateway-Konfigurationseigenschaften

Im Bereich für die Gateway-Konfigurationseigenschaften können Sie einen Knoten als Gateway für eine Domäne konfigurieren und das Verzeichnis angeben, in das der Dienstmanager dieses Knotens die Protokollereignisdateien schreibt.

Beim Bearbeiten von Gateway-Konfigurationseigenschaften werden keine früheren Protokolle eingeblendet. Außerdem gelten die geänderten Eigenschaften nur für Neustart- und Failover-Szenarien.

Klicken Sie zum Bearbeiten der Gateway-Konfigurationseigenschaften auf **Bearbeiten**.

Um Gateway-Konfigurationseigenschaften zu sortieren, klicken Sie auf die Spaltenüberschrift, nach der Sie sortieren möchten.

Die folgende Tabelle beschreibt die Eigenschaften, die Sie im Bereich für die Gateway-Konfigurationseigenschaften bearbeiten können:

Eigenschaft	Beschreibung
Knotenname	Schreibgeschützt. Der Name des Knotens
Status	Der Status des Knotens
Gateway	Wählen Sie diese Option, um den Knoten als Gateway zu konfigurieren. Wenn die Domäne eine sichere Domänen-Konfigurationsdatenbank verwendet, müssen Sie die Truststore-Datei und das Passwort für die Datenbank angeben. Um den Knoten als Worker-Knoten zu konfigurieren, löschen Sie diese Option.
Protokollverzeichnispfad	Der Verzeichnispfad für die Protokollereignisdateien. Kann der Protokollmanager nicht in den Verzeichnispfad schreiben, schreibt er Protokollereignisse in die Datei node.log auf dem Master-Gateway-Knoten.

Sicheres Domänenkonfigurations-Repository

Wenn Sie einen Knoten als Gateway-Knoten konfigurieren und die Domäne eine sichere Domänen-Konfigurationsdatenbank verwendet, müssen Sie die Truststore-Datei und das Passwort für die sichere Datenbank angeben.

Wenn Sie mehrere Gateway-Knoten für die Domäne konfigurieren, legen Sie die Datenbank-Truststore-Datei und das Passwort für alle Gateway-Knoten fest.

In der folgenden Tabelle werden die Datenbankeigenschaften beschrieben:

Eigenschaft	Beschreibung
Datenbank-Truststore-Passwort	Passwort für die Truststore-Datei
Datenbank-Truststore-Speicherort	Pfad und Dateiname der Truststore-Datei für die sichere Datenbank.

Hinweis: Damit Sie eine sichere Domänenkonfigurations-Repository-Datenbank verwenden können, muss die Option „Sichere Kommunikation“ für die Domäne aktiviert sein.

Dienstebenenverwaltung

Im Bereich Dienstebenenverwaltung können Sie Dienstebenen anzeigen, hinzufügen und bearbeiten.

Dienstebenen legen die Priorität unter den Tasks fest, die darauf warten, versendet zu werden. Wenn der Load Balancer mehr Aufgaben zu versenden hat als der der PowerCenter Integration Service gleichzeitig ausführen kann, stellt der Load Balancer diese Aufgaben in die Dispatch-Warteschlange. Wenn mehrere Tasks in der Dispatch-Warteschlange stehen, bestimmt der Load Balancer anhand der Dienstebenen die Reihenfolge, in der die Tasks aus der Warteschlange verteilt werden.

Da es sich bei den Dienstebenen um Domäneneigenschaften handelt, können Sie für all Repositories in einer Domäne die gleichen Dienstebenen verwenden. Sie erstellen und bearbeiten Dienstebenen in den Domäneneigenschaften der Domäne oder mithilfe von infacmd.

Sie können die Standard-Dienstebene bearbeiten, aber nicht löschen. Diese Standard-Dienstebene hat eine Dispatch-Priorität von 5 und eine maximale Dispatch-Wartezeit von 1800 Sekunden.

Um eine Dienstebene hinzuzufügen, klicken Sie auf **Hinzufügen**.

Um eine Dienstebene zu bearbeiten, klicken Sie auf den Link für die Dienstebene.

Um eine Dienstebene zu löschen, wählen Sie die Dienstebene aus und klicken auf die Schaltfläche Löschen.

Die folgende Tabelle beschreibt die Eigenschaften, die Sie im Bereich Dienstebenenverwaltung bearbeiten können:

Eigenschaft	Beschreibung
Name	Der Name der Dienstebene. Beim Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden, und er muss in der Domäne eindeutig sein. Er darf nicht länger als 128 Zeichen sein oder mit @ beginnen. Er darf auch keine Leerzeichen oder die folgenden Sonderzeichen enthalten: ` ~ % ^ * + = { } \ ; : / ? . < > ! ()] [Nachdem Sie eine Dienstebene hinzugefügt haben, können Sie ihren Namen nicht mehr ändern.
Dispatch-Priorität	Eine Zahl, die die Dispatch-Priorität für die Dienstebene festlegt. Der Load Balancer versendet zuerst Tasks mit einer hohen Priorität, dann Tasks mit niedriger Priorität. Die Dispatch-Priorität 1 ist die höchste Priorität. Gültige Werte sind 1 bis 10. Der Standard ist 5.
Maximale Dispatch-Wartezeit (Sekunden)	Die Zeit in Sekunden, die der Load Balancer wartet, bevor er die Dispatch-Priorität für eine Task auf die höchsten Priorität ändert. Diese Eigenschaft sorgt dafür, dass keine Task für immer in der Dispatch-Warteschlange wartet. Gültige Werte sind 1 bis 86400. Standard ist 1800.

SMTP-Konfiguration

Mithilfe der SMTP-Konfigurationseigenschaften können Sie SMTP-Einstellungen für die Domäne konfigurieren. Der ausgehende Mailserver verwendet die SMTP-Einstellungen zum Versenden von Alarmen und Scorecard-Benachrichtigungen.

Die nachstehende Tabelle beschreibt die Eigenschaften, die sich im Bereich Datenbankeigenschaften bearbeiten lassen:

Eigenschaft	Beschreibung
Hostname	Hostname für ausgehenden SMTP-Mailserver. Geben Sie zum Beispiel den Microsoft Exchange-Server für Microsoft Outlook ein.
Port	Vom ausgehenden Mailserver verwendeter Port. Die gültigen Werte liegen zwischen 1 und 65535. Standardwert ist 25.
Benutzername	Benutzername für die Authentifizierung beim Senden, wenn dies vom ausgehenden Mailserver gefordert wird.

Eigenschaft	Beschreibung
Passwort	Benutzerpasswort für die Authentifizierung beim Senden, wenn dies vom ausgehenden Mailserver gefordert wird.
E-Mail-Adresse des Absenders	E-Mail-Adresse, die der Dienstmanager im Feld „Von“ beim Senden von Benachrichtigungs-E-Mails verwendet. Wenn Sie dieses Feld leer lassen, verwendet der Dienstmanager Administrator@<Hostname> als Absender.

Benutzerdefinierte Eigenschaften für die Domäne

Konfigurieren Sie benutzerdefinierte Eigenschaften, die für bestimmte Umgebungen eindeutig sind.

In speziellen Fällen ist die Anwendung von benutzerdefinierten Eigenschaften erforderlich. Wenn Sie eine benutzerdefinierte Eigenschaft definieren, geben Sie den Eigenschaftennamen und einen Anfangswert ein. Definieren Sie die benutzerdefinierten Eigenschaften nur auf Anforderung des globalen Kundensupports von Informatica.

Konfigurieren einer Katalogdienst-URL für E-Mail-Benachrichtigungen

Konfigurieren Sie eine benutzerdefinierte Katalogdienst-URL, um über E-Mail-Benachrichtigungen auf den Katalogdienst zuzugreifen.

1. Wählen Sie im Navigator eine Domäne aus.
2. Dann klicken Sie in der Inhaltsübersicht auf „Eigenschaften“.
In der Inhaltsübersicht stehen die Domäneneigenschaften.
3. Klicken Sie auf **Benutzerdefinierte Eigenschaften bearbeiten > Neu**.
Das Fenster „Neue benutzerdefinierte Eigenschaft“ wird angezeigt.
4. Geben Sie im Feld „Name“ den Wert `LdmCustomOptions.change.notification.ldm.catalog.custom.url` ein. Geben Sie im Feld „Wert“ eine URL ein, die Ihren Anforderungen entspricht. Zum Beispiel `http://hostname.informatica.com:9085/`.
5. Klicken Sie auf **OK**. Starten Sie den Katalogdienst neu.

KAPITEL 6

Knoten

Dieses Kapitel umfasst die folgenden Themen:

- [Knoten – Übersicht, 97](#)
- [Knotentypen, 98](#)
- [Knotenrollen, 99](#)
- [Definieren und Hinzufügen von Knoten, 101](#)
- [Konfigurieren der Knoteneigenschaften, 103](#)
- [Herunterfahren und Neustarten des Knotens, 106](#)
- [Entfernen der Knotenzuordnung, 107](#)
- [Entfernen eines Knotens, 107](#)

Knoten – Übersicht

Ein Knoten entspricht der logischen Darstellung eines einzelnen Computers in der Domäne. Wenn Sie eine Domäne mit mehreren Knoten konfigurieren, können Sie die Dienstverarbeitung auf verschiedene Computer verteilen. Der Dienstmanager läuft auf allen Knoten in der Domäne, um die Domäne und Anwendungsdienste zu unterstützen. Wenn der Dienstmanager nicht läuft, ist der Knoten nicht verfügbar.

Eine Installation auf mehreren Computern besteht aus einem Master-Gateway-Knoten, der die Domäne hostet, sowie zusätzlichen Gateway- und Worker-Knoten, auf denen Informatica-Anwendungsdienste ausgeführt werden. Der Knotentyp legt fest, ob der Knoten als Gateway-Knoten oder als Worker-Knoten dient, und bestimmt die Domänenfunktionen, die der Knoten ausführt. Legen Sie den Knotentyp bei der Installation der Informatica-Dienste fest und fügen Sie den Knoten zur Domäne hinzu. Sie können den Knotentyp nach der Installation mithilfe des Administrator tool ändern.

Standardmäßig kann jeder Knoten einer Domäne Anwendungsdienste und Berechnungsprozesse ausführen. Durch die Knotenrolle wird bestimmt, ob ein Knoten Anwendungsdienste, Berechnungsprozesse oder beides ausführen kann. Ist für den Knoten die Dienstrolle aktiviert, können Sie die auf dem Knoten ausgeführten Anwendungsdienstprozesse anzeigen. Bevor Sie einen Knoten entfernen oder herunterfahren, stellen Sie sicher, dass alle laufenden Prozesse gestoppt wurden. Möglicherweise müssen Sie den Knoten herunterfahren, um Wartungsarbeiten auf dem Computer auszuführen oder um sicherzustellen, dass Änderungen an der Domänenkonfiguration wirksam werden.

Auf der Registerkarte „Verwalten“ im Administrator Tool können Sie Knoten verwalten und unter anderem Knoteneigenschaften konfigurieren, eine Knotenrolle aktualisieren und Knoten aus einer Domäne entfernen. Die Eigenschaften, die Sie konfigurieren können, sind abhängig von der Knotenrolle.

Wenn Ihre Lizenz Gitter umfasst, können Sie den Datenintegrationsdienst oder PowerCenter-Integrationsdienst zur Ausführung in einem Gitter konfigurieren. Ein Gitter ist ein Alias, das einer Gruppe von

Knoten zugewiesen ist. Wenn Sie Jobs in einem Gitter aus Knoten ausführen, verbessern Sie die Skalierbarkeit und Leistung durch die Verteilung von Jobs auf Prozesse, die auf mehreren Knoten im Gitter ausgeführt werden. Wenn der PowerCenter-Integrationsdienst auf einem Gitter läuft, können Sie ihn konfigurieren, um die verfügbaren Ressourcen auf jedem Knoten zu überprüfen. Weisen Sie Verbindungsressourcen zu und definieren Sie benutzerdefinierte sowie Datei-/Verzeichnisressourcen auf einem Knoten, der einem PowerCenter-Integrationsdienst-Gitter zugewiesen wurde.

Knotentypen

Der Knotentyp legt fest, ob der Knoten als Gateway-Knoten oder als Worker-Knoten dient, und bestimmt die Domänenfunktionen, die der Knoten ausführt.

Legen Sie den Knotentyp bei der Installation der Informatica-Dienste fest und fügen Sie den Knoten zur Domäne hinzu. Sie können den Knotentyp nach der Installation mithilfe des Administrator tool ändern. Der Knotentyp kann in den Gateway-Konfigurationseigenschaften für die Domäne geändert werden.

VERWANDTE THEMEN:

- [“Gateway-Konfiguration” auf Seite 84](#)

Gateway-Knoten

Ein Gateway-Knoten ist ein Knoten, den Sie konfigurieren, damit er als Gateway für die Domäne eingesetzt werden kann. Ein Gateway-Knoten kann Anwendungsdienste und Berechnungen ausführen und als Master-Gateway-Knoten dienen. Zu einem gegebenen Zeitpunkt fungiert nur ein Gateway-Knoten als Master-Gateway. Der Master-Gateway-Knoten ist der Eingangspunkt zur Domäne.

Alle Domänenfunktionen auf dem Master-Gateway-Knoten werden vom Dienstmanager des Master-Gateway-Knotens ausgeführt. Die auf den anderen Gateway-Knoten laufenden Dienstmanager führen eingeschränkte Domänenvorgänge auf diesen Knoten aus.

Sie können mehr als einen Knoten als Gateway konfigurieren. Ist der Master-Gateway-Knoten nicht verfügbar, wählen die Dienstmanager auf anderen Gateway-Knoten einen anderen Master-Gateway-Knoten aus. Wenn Sie nur einen Knoten als Gateway konfigurieren und der Knoten unverfügbar wird, kann die Domäne keine Dienstanfragen annehmen.

Worker-Knoten

Ein Arbeitsknoten ist ein beliebiger Knoten, den Sie nicht als Gateway für die Domäne konfigurieren. Ein Worker-Knoten kann Anwendungsdienste ausführen und Berechnungen durchführen, er kann jedoch nicht als Gateway dienen. Der Dienstmanager führt auf einem Worker-Knoten nur eingeschränkte Domänenfunktionen aus.

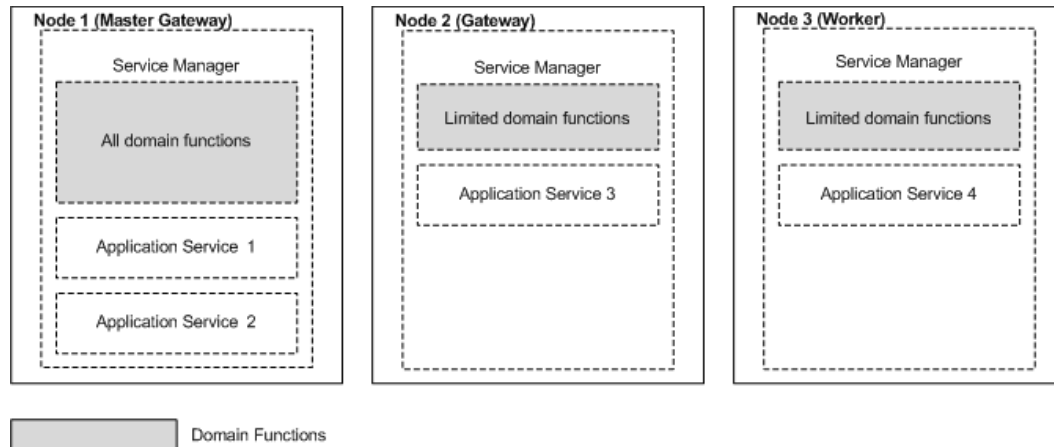
Beispiel: Domäne mit mehreren Knoten

Diese Beispieldomäne enthält drei Knoten. Für jeden Knoten sind die Dienst- und Berechnungsrolle aktiviert.

Alle Knoten führen den Dienstmanager aus. Knoten 1 ist der Master-Gateway-Knoten und führt zwei Anwendungsdienste aus. Knoten 2 ist ein Backup-Gateway-Knoten und führt einen Anwendungsdienst aus. Knoten 3 ist ein Worker-Knoten und führt einen Anwendungsdienst aus. Wenn Knoten 1 nicht mehr verfügbar ist, wird Knoten 2 als neuer Master-Gateway-Knoten ausgewählt. Der Dienstmanager auf Knoten 2 führt dann

alle Domänenfunktionen aus. Wenn Knoten 1 neu gestartet wird, wird er zu einem Backup-Gateway-Knoten und der Dienstmanager führt eingeschränkte Domänenfunktionen aus.

Die folgende Abbildung zeigt eine Domäne mit zwei Gateway-Knoten und einem Worker-Knoten:



Knotenrollen

Die Knotenrolle gibt den Zweck des Knotens an. Ein Knoten mit der Dienstrolle kann Anwendungsdienste ausführen. Ein Knoten mit der Berechnungsrolle kann Berechnungen durchführen, die von Remote-Anwendungsdiensten angefragt werden. Ein Knoten mit beiden Rollen kann Anwendungsdienste ausführen und lokal Berechnungen für diese Dienste durchführen.

Standardmäßig sind für alle Gateway- und Worker-Knoten sowohl die Dienst- als auch die Berechnungsrolle aktiviert. Für jeden Knoten muss mindestens eine Rolle aktiviert sein.

Sie können ein Datenintegrationsdienst-Gitter so konfigurieren, dass einige Knoten Anwendungsdienst-Prozesse ausführen und andere Knoten Berechnungen durchführen. Wenn Sie auf einem Knoten in einem Datenintegrationsdienst-Gitter nur die Berechnungsrolle aktivieren, muss der Knoten den Dienstprozess nicht ausführen. Der Computer verwendet sämtliche verfügbare Verarbeitungskapazität zum Ausführen von Mappings. Sie können zusätzliche Knoten, für die nur die Berechnungsrolle aktiviert ist, zum Gitter hinzufügen, um die Skalierbarkeit der Datenintegrationsdienst-Mappings zu erhöhen.

Weitere Informationen zum Einrichten eines Datenintegrationsdienst-Gitters finden Sie im *Handbuch für Informatica-Anwendungsdienste*.

Dienstrolle

Ein Knoten mit der Dienstrolle kann Anwendungsdienste ausführen.

Wenn Sie die Dienstrolle auf einem Knoten aktivieren, unterstützt der Dienstmanager die Anwendungsdienste, die für die Ausführung auf diesem Knoten konfiguriert wurden.

In den folgenden Situationen ist die Dienstrolle für einen Knoten erforderlich:

- Der Knoten ist ein Gateway-Knoten.
- Der Knoten ist als Primär- oder Backup-Knoten für einen Anwendungsdienst konfiguriert.
- Der Knoten ist einem PowerCenter-Integrationsdienst-Gitter oder einem Datenintegrationsdienst-Gitter zugewiesen und ein Dienstprozess wird auf dem Knoten ausgeführt.

Berechnungsrolle

Ein Knoten mit der Berechnungsrolle kann Berechnungen durchführen, die von Remote-Anwendungsdiensten angefragt werden.

Wenn einem Knoten die Berechnungsrolle zugewiesen wurde, verwaltet der Dienstmanager die Container auf dem Knoten. Ein Container ist eine Zuweisung von Speicher- und CPU-Ressourcen. Ein Anwendungsdienst verwendet die Container, um Berechnungen auf dem Knoten remote durchzuführen. Beispiel: Ein Datenintegrationsdienst-Gitter beinhaltet Knoten 1 mit der Dienstrolle und Knoten 2 mit der Berechnungsrolle. Der Datenintegrationsdienst-Prozess läuft auf Knoten 1 und führt ein Mapping in einem Container auf Knoten 2 aus.

Ein Knoten erfordert die Berechnungsrolle, wenn der Datenintegrationsdienst Jobs auf diesem Knoten ausführt. Wenn der Datenintegrationsdienst auf einem einzelnen Knoten ausgeführt wird, muss der Knoten die Dienstrolle und die Berechnungsrolle aufweisen. Wenn der Datenintegrationsdienst auf einem Gitter ausgeführt wird, muss mindestens einer der Knoten im Gitter die Berechnungsrolle aufweisen.

Die Berechnungsrolle ist für einen Knoten nicht erforderlich, wenn der Datenintegrationsdienst keine Jobs auf diesem Knoten ausführt. In diesem Fall können Sie die Berechnungsrolle auf dem Knoten deaktivieren. Da die Containerverwaltungsfunktion des Dienstmanagers ein leichter Prozess ist, hat das Deaktivieren oder Aktivieren der Berechnungsrolle keine Auswirkungen auf die Leistung.

Wenn Sie die Berechnungsrolle auf einem Knoten deaktivieren, müssen Sie angeben, ob laufende Berechnungen beendet, abgeschlossen oder abgebrochen werden sollen.

Aktualisieren der Knotenrolle

Standardmäßig verfügt jeder Knoten sowohl über die Dienstrolle als auch die Berechnungsrolle. Wenn ein Knoten einem Datenintegrationsdienst-Gitter zugewiesen ist, das für die Ausführung von Jobs in separaten Remoteprozessen konfiguriert wurde, können Sie die Knotenrolle bei Bedarf aktualisieren.

Aktivieren Sie nur die Dienstrolle, wenn der Knoten den Datenintegrationsdienst-Prozess ausführen soll. Aktivieren Sie nur die Berechnungsrolle, wenn der Knoten Datenintegrationsdienst-Mappings ausführen soll.

Hinweis: Um die Dienstrolle auf einem Knoten zu deaktivieren zu können, müssen Sie zunächst alle auf dem Knoten ausgeführten Anwendungsdienstprozesse herunterfahren und den Knoten als primären oder Backup-Knoten für jeden Anwendungsdienst entfernen. Sie können die Dienstrolle auf einem Gateway-Knoten nicht deaktivieren.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten** > Ansicht **Dienste und Knoten**.
2. Wählen Sie im Domänen-Navigator einen Knoten aus, der einem Datenintegrationsdienst-Gitter zugewiesen ist.
3. Klicken Sie in der Ansicht „Eigenschaften“ für die allgemeinen Eigenschaften auf **Bearbeiten**.
Das Dialogfeld **Allgemeine Eigenschaften bearbeiten** wird angezeigt.
4. Wählen Sie die Dienst- oder Berechnungsrolle aus oder löschen Sie sie, um die Knotenrolle zu aktualisieren.
5. Klicken Sie auf **OK**.
6. Falls Sie die Berechnungsrolle aktiviert hatten, wird das Dialogfeld **Berechnungsrolle deaktivieren** angezeigt. Führen Sie die folgenden Schritte durch:
 - a. Wählen Sie zum Deaktivieren der Berechnungsrolle einen der folgenden Modi aus:
 - Abschließen. Ermöglicht die Fertigstellung von Jobs, bevor die Rolle deaktiviert wird.

- Stoppen. Stoppt alle Jobs und deaktiviert danach die Rolle.
 - Abbrechen. Es wird versucht, alle Jobs vor deren Abbruch und Deaktivieren der Rolle anzuhalten.
- b. Klicken Sie auf **OK**.
7. Wenn Sie die Rolle auf einem Knoten aktualisiert haben, der einem Datenintegrationsdienst oder einem Datenintegrationsdienst-Gitter zugewiesen ist, stellen Sie den Datenintegrationsdienst wieder her.

Anzeigen von Prozessen auf einem Knoten mit Dienstrolle

Sie können den Status aller Anwendungsdienstprozesse anzeigen, die auf einem Knoten mit Dienstrolle ausgeführt werden. Vor dem Herunterfahren oder Entfernen eines Knotens können Sie den Status jedes Anwendungsdienstprozesses anzeigen, um die zu deaktivierenden Dienstprozesse festzulegen.

Wenn ein Knoten nicht über die Dienstrolle verfügt, werden auf diesem Knoten keine Anwendungsdienstprozesse ausgeführt.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten** > Ansicht **Dienste und Knoten**.
2. Wählen Sie im Domänen-Navigator einen Knoten mit Dienstrolle aus.
3. Klicken Sie im Inhaltsbereich auf die Ansicht **Prozesse**.

Der Status jedes Anwendungsdienstprozesses, der zur Ausführung auf dem Knoten konfiguriert wurde, wird angezeigt.

Definieren und Hinzufügen von Knoten

Um einen Knoten zu erstellen, definieren Sie den Knoten als Gateway- oder Worker-Knoten und fügen Sie ihn anschließend zur Domäne hinzu.

Definieren Sie einen Knoten mit einem der folgenden Programme:

Informatica-Installationsprogramm

Führen Sie das Installationsprogramm auf jedem Computer aus, den Sie als Knoten definieren möchten.

infasetup-Befehlszeilenprogramm

Führen Sie den Befehl „infasetup DefineGatewayNode“ oder „infasetup DefineWorkerNode“ auf jedem Computer aus, den Sie als Knoten definieren möchten. Sie können infasetup zum Definieren eines Knotens verwenden, wenn Sie einen Knoten von einer Domäne auf eine andere verschieben möchten.

Wenn das Informatica-Installationsprogramm oder infasetup einen Knoten definiert, erstellt das Programm die Datei `nodemeta.xml`. Diese Datei dient dem Knoten als Knotenkonfigurationsdatei. Ein Gateway-Knoten verwendet die Informationen in der Datei `nodemeta.xml`, um eine Verbindung mit der Datenbank für die Domänenkonfiguration herzustellen. Ein Worker-Knoten nutzt die Informationen in `nodemeta.xml`, um eine Verbindung mit der Domäne herzustellen. Die Datei wird auf jedem Knoten in dem folgenden Verzeichnis gespeichert:

```
<Informatica-Installationsverzeichnis>/isp/config
```

Bei der Knotendefinition mit dem Informatica-Installationsprogramm sind die Dienstrolle und die Berechnungsrolle aktiviert, wenn der Knoten zur Domäne hinzugefügt wird. Sobald Sie sich im Administrator tool anmelden, wird der Knoten im Navigator angezeigt.

Wenn Sie einen Knoten mit infasetup definieren, müssen Sie den Knoten manuell zur Domäne hinzufügen. Sie können einen Knoten über das Administrator Tool oder mit dem Befehl „infacmd isp AddDomainNode“ zur

Domäne hinzufügen. Beim Hinzufügen des Knotens legen Sie fest, welche Rollen auf dem Knoten aktiviert werden sollen.

Sie können das Administrator tool verwenden, um einen Knoten vor dem Definieren zur Domäne hinzuzufügen. In diesem Fall zeigt das Administrator tool eine Meldung an mit der Information, dass Sie das Informatica-Installationsprogramm ausführen müssen, um dem Knoten einen physischen Hostnamen und eine Portnummer zuzuweisen. Der für den Knoten eingegebene Name muss mit dem Namen übereinstimmen, den Sie bei der Definition des Knotens verwenden.

Hinzufügen von Knoten zur Domäne

Sie können das Administrator tool verwenden, um einen Knoten zur Domäne hinzuzufügen.

Verwenden Sie das Administrator tool zum Hinzufügen eines Knotens zur Domäne in den folgenden Situationen:

- Nach dem Ausführen der Befehle „infasetup DefineGatewayNode“ oder „infasetup DefineWorkerNode“.
- Wenn Sie den Knoten vor Ausführen des Informatica-Installationsprogramms oder des infasetup-Befehlszeilenprogramms hinzufügen möchten, um den Knoten zu definieren.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten** > Ansicht **Dienste und Knoten**.
2. Wählen Sie im Domänen-Navigator den Ordner aus, dem Sie den Knoten hinzufügen möchten. Wenn der Knoten nicht in einem Ordner erscheinen soll, wählen Sie die Domäne aus.
3. Klicken Sie im Navigator-Menü „Aktionen“ auf **Neu > Knoten**.

Das Dialogfeld **Knoten erstellen** wird angezeigt.

4. Geben Sie den Knotennamen ein.

Der Name muss mit dem Knotennamen übereinstimmen, den Sie bei der Definition des Knotens verwenden.

5. Wenn Sie den Ordner für den Knoten ändern möchten, klicken Sie auf **Durchsuchen** und wählen Sie einen neuen Ordner oder die Domäne.

6. Optional können Sie die Knotenrolle aktualisieren.

Standardmäßig verfügt jeder Knoten sowohl über die Dienstrolle als auch die Berechnungsrolle. Wenn ein Knoten einem Datenintegrationsdienst-Gitter zugewiesen ist, können Sie die Knotenrolle aktualisieren, um den Knoten zum Ausführen von Mappings oder des Datenintegrationsdienst-Prozesses zu bestimmen.

7. Klicken Sie auf **OK**.

Wenn Sie einen Knoten hinzufügen, bevor Sie den Knoten mit dem Informatica-Installationsprogramm oder mit „infasetup“ definiert haben, zeigt das Administrator tool eine Meldung an mit der Information, dass Sie das Installationsprogramm ausführen müssen, um dem Knoten einen physischen Hostnamen und eine Portnummer zuzuweisen.

VERWANDTE THEMEN:

- ["Knotenrollen" auf Seite 99](#)

Konfigurieren der Knoteneigenschaften

Knoteneigenschaften werden in der Ansicht „Eigenschaften“ des Knotens konfiguriert. Sie können Eigenschaften wie die Knotenrollen, die Fehlerschweregradstufe und die niedrigste und höchste Portnummer konfigurieren.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten** > Ansicht **Dienste und Knoten**.
2. Wählen Sie im Domänen-Navigator einen Knoten aus.
3. Klicken Sie auf die Ansicht **Eigenschaften**.

In der Ansicht „Eigenschaften“ stehen die Knoteneigenschaften in separaten Abschnitten.

4. Klicken Sie in der Ansicht **Eigenschaften** für den Abschnitt mit der Eigenschaft, die Sie festlegen möchten, auf **Bearbeiten**.
5. Bearbeiten Sie die folgenden Eigenschaften:

Eigenschaft „Knoten“	Beschreibung
Name	Name des Knotens. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Er darf weder mehr als 128 Zeichen enthalten noch mit @ beginnen. Außerdem darf er weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! ()] [
Beschreibung	Beschreibung des Knotens Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Hostname	Hostname des vom Knoten dargestellten Computers.
Port	Die vom Knoten verwendete Portnummer.
Gateway-Knoten	Gibt an, ob der Knoten als Gateway eingesetzt werden kann. Wenn diese Eigenschaft deaktiviert ist, handelt es sich um einen Worker-Knoten.
Dienstrolle	Gibt an, ob dem Knoten die Dienstrolle zugewiesen wurde. Wenn die Eigenschaft aktiviert ist, können Anwendungsdienste auf dem Knoten ausgeführt werden. Wenn sie deaktiviert ist, können keine Anwendungsdienste auf dem Knoten ausgeführt werden. Deaktivieren Sie diese Eigenschaft nur, wenn der Knoten einem Datenintegrationsdienst-Gitter zugewiesen ist und Mappings auf dem Knoten ausgeführt werden sollen. Standardwert ist „Aktiviert“.

Eigenschaft „Knoten“	Beschreibung
Berechnungsrolle	<p>Gibt an, ob dem Knoten die Berechnungsrolle zugewiesen wurde. Wenn die Eigenschaft aktiviert ist, kann der Knoten Berechnungen durchführen. Wenn sie deaktiviert ist, kann der Knoten keine Berechnungen durchführen.</p> <p>Für einen Knoten ist die Berechnungsrolle erforderlich, wenn der Datenintegrationsdienst Jobs auf diesem Knoten ausführt. Wenn der Datenintegrationsdienst auf dem Knoten keine Jobs ausführt, können Sie die Berechnungsrolle deaktivieren. Das Deaktivieren oder Aktivieren der Berechnungsrolle hat keine Auswirkungen auf die Leistung.</p> <p>Standardwert ist „Aktiviert“.</p>
Backup-Verzeichnis	<p>Verzeichnis zum Speichern der Repository-Backup-Dateien. Der Zugriff auf das Verzeichnis muss über den Knoten möglich sein.</p>
Fehlerschweregradstufe	<p>Ebene der Fehlerprotokollierung für den Knoten. Diese Meldungen werden in den Protokollmanager-Anwendungsdienst und die Dienstmanager-Protokolldateien geschrieben. Legen Sie eine der folgenden Meldungsebenen fest:</p> <ul style="list-style-type: none"> - ERROR Schreibt ERROR-Codemeldungen in das Protokoll. - WARNING Schreibt WARNING- und ERROR-Codemeldungen in das Protokoll. - INFO Schreibt INFO-, WARNING- und ERROR-Codemeldungen in das Protokoll. - TRACING Schreibt TRACE-, INFO-, WARNING- und ERROR-Codemeldungen in das Protokoll. - DEBUG Schreibt DEBUG-, TRACE-, INFO-, WARNING- und ERROR-Codemeldungen in das Protokoll. <p>Standardwert ist WARNING.</p>
Niedrigste Portnummer	<p>Niedrigste von den Dienstprozessen auf dem Knoten verwendete Portnummer. Starten Sie Informatica-Dienste neu, um die Änderungen zu übernehmen. Der Standardwert ist der bei der Definition des Knotens eingegebene Wert.</p>
Höchste Portnummer	<p>Höchste von den Dienstprozessen auf dem Knoten verwendete Portnummer. Starten Sie Informatica-Dienste neu, um die Änderungen zu übernehmen. Der Standardwert ist der bei der Definition des Knotens eingegebene Wert.</p>
CPU-Profil-Benchmark	<p>Stuft die CPU-Leistung des Knotens im Vergleich zu einem Baseline-System ein. Wird von der Load Balancer-Komponente des PowerCenter-Integrationsdienstes verwendet.</p> <p>Beispiel: Wenn die CPU 1,5 Mal schneller als der Baseline-Computer ausgeführt wird, beträgt der Wert dieser Eigenschaft 1,5. Sie können den Benchmark berechnen, indem Sie auf Aktionen > CPU-Profil-Benchmark neu berechnen klicken. Die Berechnung dauert ca. fünf Minuten und lastet eine CPU des Computers zu 100% aus. Sie können den Wert jedoch auch manuell aktualisieren.</p> <p>Der Standardwert ist 1,0. Der Minimalwert beträgt 0,001. Der Maximalwert beträgt 1.000.000.</p> <p>Wird im adaptiven Sendemodus verwendet. Im Sendemodus auf Zufallsbasis (Round-Robin) oder im messgrößenbasierten Sendemodus wird die Eigenschaft ignoriert.</p>

Eigenschaft „Knoten“	Beschreibung
Maximale Anzahl der Prozesse	<p>Maximale Anzahl der ausgeführten Sitzungs- oder Befehlsaufgaben, die für jeden auf dem Knoten ausgeführten PowerCenter-Integrationsdienstprozess zulässig sind. Wird von der Load Balancer-Komponente des PowerCenter-Integrationsdiensts verwendet.</p> <p>Wenn Sie den Wert beispielsweise auf 5 setzen, können bis zu 5 Befehlsaufgaben und 5 Sitzungsaufgaben ausgeführt werden.</p> <p>Damit der Load Balancer diesen Schwellenwert ignoriert, müssen Sie ihn auf einen hohen Wert, wie etwa 200, einstellen. Damit der Load Balancer keine Aufgaben an diesen Knoten sendet, stellen Sie diesen Schwellenwert auf 0 ein.</p> <p>Standardwert ist 10. Minimalwert ist 0. Der Maximalwert beträgt 1.000.000.000.</p> <p>Wird in allen Sendemodi verwendet.</p>
Maximale Länge der CPU-Ausführungswarteschlange	<p>Maximale Anzahl an ausführbaren Threads, die auf CPU-Ressourcen auf dem Knoten warten. Wird von der Load Balancer-Komponente des PowerCenter-Integrationsdiensts verwendet.</p> <p>Setzen Sie diesen Schwellenwert auf einen niedrigen Wert, wenn Sie Ressourcen für andere Anwendungen aufbewahren möchten. Setzen Sie diesen Schwellenwert auf einen hohen Wert (z. B. 200), wenn er vom Load Balancer ignoriert werden soll.</p> <p>Standardwert ist 10. Minimalwert ist 0. Der Maximalwert beträgt 1.000.000.000.</p> <p>Wird im metrisch basierten und adaptiven Sendemodus eingesetzt. Im Runklaufmodus wird der Wert ignoriert.</p>
Maximaler Speicher %	<p>Maximaler Prozentsatz des virtuellen Speichers, der auf dem Knoten relativ zur Gesamtgröße des virtuellen Speichers zugeordnet ist. Wird von der Load Balancer-Komponente des PowerCenter-Integrationsdiensts verwendet.</p> <p>Setzen Sie diesen Schwellenwert auf einen Wert größer 100%, wenn Sie zulassen möchten, dass beim Senden von Aufgaben mehr virtuelle Speicherkapazität als physische Speicherkapazität zugewiesen werden kann. Setzen Sie diesen Schwellenwert auf einen hohen Wert (z. B. 1.000), wenn er vom Load Balancer ignoriert werden soll.</p> <p>Standardwert ist 150. Minimalwert ist 0. Der Maximalwert beträgt 1.000.000.000.</p> <p>Wird im metrisch basierten und adaptiven Sendemodus eingesetzt. Im Runklaufmodus wird der Wert ignoriert.</p>
Verzeichnis für die Protokollsammlung	<p>Das Verzeichnis, in dem die Protokolle für den Anwendungsdienst gespeichert werden, wenn der Protokoll-Aggregator ausgeführt wird. Der Zugriff auf das Verzeichnis muss von allen Knoten in der Domäne aus möglich sein. Wenn andere Knoten nicht auf das Verzeichnis für die Protokollsammlung zugreifen können, werden die zusammengefassten Protokolle nicht im Listengitter der zusammengefassten Protokolle angezeigt. Die Benutzer, die Knotenprozesse ausführen, müssen über Lese-/Schreibberechtigungen für das Verzeichnis verfügen.</p> <p>Konfigurieren Sie das Verzeichnis für die Protokollsammlung für den Master-Gateway-Knoten in der Domäne.</p>
Hauptspeicherverzeichnis	<p>Das Verzeichnis, in dem die Hauptspeicherdateien für die Domänenprozesse gespeichert werden, wenn der Protokoll-Aggregator ausgeführt wird.</p> <p>Konfigurieren Sie das Hauptspeicherverzeichnis für alle Knoten in der Domäne.</p>

6. Klicken Sie auf **OK**.

Herunterfahren und Neustarten des Knotens

Für einige administrative Aufgaben ist es möglicherweise erforderlich, dass Sie einen Knoten herunterfahren. Zum Beispiel müssen Sie möglicherweise eine Wartung oder ein Benchmarking auf einem Computer durchführen. Möglicherweise müssen Sie auch einen Knoten herunterfahren und neu starten, damit einige Änderungen an der Konfiguration wirksam werden können. Zum Beispiel, wenn Sie das freigegebene Verzeichnis für den Protokollmanager oder die Domäne ändern, müssen Sie den Knoten herunterfahren und neu starten, um die Konfigurationsdateien zu aktualisieren.

Sie können einen Knoten aus dem Administrator-Tool oder aus dem Betriebssystem heraus herunterfahren. Wenn Sie einen Knoten herunterfahren, werden die Informatica-Dienste gestoppt und alle auf dem Knoten ausgeführten Anwendungsdienstprozesse und Berechnungen abgebrochen.

Um einen Knoten neu zu starten, starten Sie die Informatica-Dienste auf dem Knoten.

Warnhinweis: Um beim Herunterfahren von Knoten den Verlust von Daten oder Metadaten zu vermeiden, deaktivieren Sie alle aktuell ausgeführten Prozesse im vollständigen Modus.

Herunterfahren eines Knotens über das Administrator tool

Wenn Sie einen Knoten über das Administrator tool herunterfahren, können Sie alle auf dem Knoten ausgeführten Anwendungsdienstprozesse anzeigen.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten** > Ansicht **Dienste und Knoten**.
2. Wählen Sie im Domänen-Navigator einen Knoten aus.
3. Wählen Sie im Navigator-Menü **Aktionen** die Option **Knoten herunterfahren** aus.

Wenn der Knoten über die Dienstrolle verfügt, zeigt das Administrator tool die Liste der auf dem Knoten ausgeführten Anwendungsdienstprozesse an.

4. Wählen Sie optional aus, ob das Herunterfahren geplant oder ungeplant sein soll.
5. Fügen Sie optional Kommentare über das Herunterfahren hinzu.
6. Klicken Sie auf **OK**, um alle Dienstprozesse zu stoppen und den Knoten herunterzufahren, oder klicken Sie auf **Abbrechen**, um den Vorgang abubrechen.

Starten oder Anhalten eines Knotens unter Windows

Verwenden Sie unter Windows die Systemsteuerung, um den Informatica-Dienst zu starten und zu stoppen.

1. Öffnen Sie die Windows-Systemsteuerung.
2. Wählen Sie **Verwaltung**.
3. Klicken Sie mit der rechten Maustaste auf **Dienste** und wählen Sie **Als Administrator ausführen** aus.
4. Klicken Sie mit der rechten Maustaste auf den Informatica-Dienst.
5. Wenn der Dienst ausgeführt wird, klicken Sie auf **Beenden**.

Wenn der Dienst angehalten ist, klicken Sie auf **Starten**.

Einen Knoten unter UNIX starten und anhalten

Unter UNIX wird der Informatica-Dämon durch Ausführen von `infaservice.sh` gestartet und beendet. `infaservice.sh` ist standardmäßig im folgenden Verzeichnis installiert:

```
<InformaticaInstallationDir>/tomcat/bin
```

1. Gehen Sie zu dem Verzeichnis, in dem sich `infaservice.sh` befindet.

2. Geben Sie nach der Befehlseingabeaufforderung den folgenden Befehl ein, um den Dämon zu starten:

```
infaservice.sh startup
```

Geben Sie den folgenden Befehl ein, um den Daemon zu beenden:

```
infaservice.sh shutdown
```

Hinweis: Starten Sie Informatica-Knoten immer mit einem Nicht-Root-Benutzer. Wenn Sie den Speicherort von infaservice.sh mithilfe eines Softlinks festlegen, stellen Sie die Umgebungsvariable INFA_HOME auf den Speicherort des Informatica-Installationsverzeichnis ein.

Entfernen der Knotenzuordnung

Sie können den Hostnamen und die Portnummer entfernen, die einem Knoten zugeordnet ist. Wenn Sie die Knotenzuordnungen entfernt haben, bleibt der Knoten in der Domäne, ist aber nicht mehr mit einer Hostmaschine verbunden.

Um dem Knoten einen anderen Hostcomputer zuzuordnen, müssen Sie auf dem neuen Hostcomputer das Installationsprogramm oder den Befehl „infasetup DefineGatewayNode“ bzw. „infasetup DefineWorkerNode“ ausführen. Anschließend starten Sie den Knoten auf der neuen Hostmaschine erneut.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten** > Ansicht **Dienste und Knoten**.
2. Wählen Sie im Navigator einen Knoten aus.
3. Wählen Sie in der Ansicht **Dienste und Knoten** im Menü **Aktionen** die Option **Knotenzuordnung entfernen** aus.

Entfernen eines Knotens

Wenn Sie einen Knoten aus einer Domäne entfernen, ist er im Navigator nicht mehr sichtbar. Wenn der Knoten ausgeführt wird, während Sie ihn entfernen, wird er heruntergefahren und bricht alle Anwendungsdienstprozesse ab.

Hinweis: Um beim Entfernen von Knoten den Verlust von Daten oder Metadaten zu vermeiden, deaktivieren Sie alle aktuell ausgeführten Prozesse im vollständigen Modus.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten** > Ansicht **Dienste und Knoten**.
2. Wählen Sie im Domänen-Navigator einen Knoten aus.
3. Wählen Sie im Navigator-Menü **Aktionen** die Option **Löschen** aus.
4. Klicken Sie in der angezeigten Warnmeldung auf **OK**.

KAPITEL 7

Hohe Verfügbarkeit

Dieses Kapitel umfasst die folgenden Themen:

- [Hohe Verfügbarkeit - Übersicht, 108](#)
- [Belastbarkeit, 109](#)
- [Neustart und Failover, 112](#)
- [Wiederherstellung, 114](#)
- [Konfiguration für einen hochverfügbare Domäne, 115](#)
- [Oracle RAC-Datenbank-Failover, 119](#)
- [Netzwerk, hohe Verfügbarkeit, 120](#)

Hohe Verfügbarkeit - Übersicht

Hohe Verfügbarkeit bedeutet unterbrechungslose Verfügbarkeit der Computersystemressourcen. In einer Informatica-Domäne eliminiert Hochverfügbarkeit einen einzelnen Fehlerpunkt und gewährleistet im Fehlerfall die Minimierung der Dienstunterbrechungen. Wenn Sie hohe Verfügbarkeit für eine Domäne konfigurieren, kann die Domäne auch bei vorübergehendem Netzwerk-, Hardware- oder Dienstaussfall weiter ausgeführt werden.

Durch folgende Hochverfügbarkeitskomponenten werden Dienste in einer Informatica-Domäne hoch verfügbar:

- **Belastbarkeit.** Eine Informatica-Domäne kann temporäre Verbindungsfehler so lange tolerieren, bis entweder das Belastbarkeits-Timeout abläuft oder der Fehler behoben wurde.
- **Neustart und Failover.** Ein Prozess kann auf demselben Knoten oder auf einen Backup-Knoten erneut starten, nachdem der Prozess nicht mehr verfügbar ist.
- **Wiederherstellung.** Operationen können nach einer Dienstunterbrechung abgeschlossen werden. Nach Neustart oder Failover eines Dienstprozesses werden Dienststatus und Operationen wieder hergestellt.

Wenn Sie eine hoch verfügbare Informatica-Umgebung planen, konfigurieren Sie hohe Verfügbarkeit für die internen Informatica-Komponenten und für externe Informatica-Systeme. Interne Komponenten umfassen die Domäne, Anwendungsdienste, Anwendungs-Clients und Befehlszeilenprogramme. Externe Systeme sind Netzwerk, Hardware, Datenbankverwaltungssysteme, FTP-Server, Meldungswarteschlangen und gemeinsame Speicher.

Funktionen für die Hochverfügbarkeit für die Informatica-Umgebung stehen Ihnen basierend auf Ihrer Lizenz zur Verfügung.

Beispiel

Wenn Sie ein Mapping im PowerCenter Designer-Arbeitsbereich öffnen, ist der PowerCenter-Repository-Dienst nicht mehr verfügbar und die Anfrage schlägt fehl. Die Domäne enthält mehrere Knoten für Failover und der PowerCenter Designer ist gegenüber temporären Ausfällen belastbar.

Der PowerCenter Designer versucht, innerhalb des Belastbarkeits-Timeouts eine Verbindung zum PowerCenter-Repository-Dienst herzustellen. Der PowerCenter-Repository-Dienst führt ein Failover zu einem anderen Knoten durch, weil er nicht auf demselben Knoten starten kann.

Der PowerCenter-Repository-Dienst startet innerhalb des Belastbarkeits-Timeout-Zeitraums und der PowerCenter Designer stellt die Verbindung wieder her.

Nachdem der PowerCenter Designer die Verbindung wiederhergestellt hat, erholt sich der PowerCenter-Repository-Dienst von der fehlgeschlagenen Operation und holt das Mapping in den PowerCenter Designer Workspace.

Belastbarkeit

Die Domäne toleriert temporäre Verbindungsfehler zwischen Anwendungs-Clients, Anwendungsdiensten und Knoten.

Ein temporärer Verbindungsfehler kann auftreten, weil ein Anwendungsdienstprozess fehlschlägt oder ein Netzwerkfehler auftritt. Wenn ein temporärer Verbindungsfehler auftritt, versucht der Dienstmanager, die Verbindungen zwischen den Anwendungs-Clients, Anwendungsdiensten und Knoten wiederherzustellen.

Belastbarkeit der Anwendungs-Clients

Die Anwendungs-Clients versuchen, eine erneute Verbindung zu Anwendungsdiensten herzustellen, wenn ein temporärer Verbindungsfehler auftritt.

Basierend auf Ihrer Lizenz sind die folgenden Anwendungs-Clients belastbar in Bezug auf die Dienste, mit denen sie verbunden sind.

Developer Tool-Client

Der Developer Tool-Client versucht, eine erneute Verbindung zum Datenintegrationsdienst oder Datenintegrationsdienstraster herzustellen, wenn ein temporärer Netzwerkfehler auftritt.

Wenn ein Job ausgeführt wird und das Developer Tool innerhalb des Wiederverbindungs-Timeout-Zeitraums keine erneute Verbindung mit dem Datenintegrationsdienst oder dem Datenintegrationsdienstraster herstellen kann, sendet das Developer Tool den Job weder erneut an einen Datenintegrationsdienst noch an ein Datenintegrationsdienstraster auf einem anderen Knoten. Der Developer Tool-Client kann den Job nicht ausführen.

PowerCenter Client

Der PowerCenter Client versucht, eine erneute Verbindung zum PowerCenter-Repository-Dienst und zum PowerCenter-Integrationsdienst herzustellen, wenn ein temporärer Netzwerkfehler auftritt.

Wenn Sie eine PowerCenter Client-Aktion durchführen, die eine Verbindung zum Repository benötigt, während der PowerCenter Client versucht, die Verbindung wiederherzustellen, fordert Sie der PowerCenter Client auf, den Vorgang noch einmal zu versuchen, nachdem der PowerCenter Client die Verbindung wieder hergestellt hat. Wenn der PowerCenter Client nicht in der Lage ist, die Verbindung während des Belastbarkeits-Timeout-Zeitraums wieder herzustellen, fordert der PowerCenter Client Sie auf, sich manuell mit dem Repository zu verbinden.

Befehlszeilenprogramme

Befehlszeilenprogramme versuchen, eine erneute Verbindung zur Domäne oder zu einem Anwendungsdienst herzustellen, wenn beim Ausführen eines Befehlszeilenprogramms ein temporärer Netzwerkfehler auftritt.

Wenn das Befehlszeilenprogramm auf einem Datenintegrationsdienst oder einem Datenintegrationsdiensttraster ausgeführt wird und das Befehlszeilenprogramm innerhalb des Wiederverbindungs-Timeout-Zeitraums keine erneute Verbindung mit dem Datenintegrationsdienst oder dem Datenintegrationsdiensttraster herstellen kann, sendet das Befehlszeilenprogramm den Job weder erneut an einen Datenintegrationsdienst noch an ein Datenintegrationsdiensttraster auf einem anderen Knoten. Das Befehlszeilenprogramm kann den Befehl nicht ausführen.

Beispiel: Belastbarkeit von PowerCenter Clients in Bezug auf Anwendungsdienste

Beim Überwachen eines Arbeitsablaufs durch einen Entwickler tritt zwischen dem PowerCenter-Arbeitsablauf-Monitor und dem PowerCenter-Repository-Dienst ein Netzwerkverbindungsverlust von 120 Sekunden auf. Der PowerCenter Client und der Arbeitsablauf-Monitor haben ein Belastbarkeits-Timeout von 60 Sekunden und der PowerCenter-Repository-Dienst hat ein Belastbarkeits-Timeout von 180 Sekunden.

Der Entwickler bemerkt den Verbindungsverlust von 120 Sekunden nicht. Auf der Registerkarte **Benachrichtigungen** im PowerCenter-Arbeitsablauf-Monitor wird jedoch die folgende Meldung angezeigt:

```
Repository Service notifications are enabled.  
DATE TIME-[REP_55101] Connection to the Repository Service [Repository_Service_Name] is  
broken.  
DATE TIME-[REP_55114] Reconnecting to the Repository Service [Repository_Service_Name].  
The resilience time is 180 seconds.  
DATE TIME-Reconnected to Repository Service [Repository_Service_Name] successfully.
```

Anwendungsdienst-Belastbarkeit

Einige Anwendungsdienste versuchen, eine erneute Verbindung zu Anwendungsdiensten, Anwendungs-Clients und externen Komponenten herzustellen, wenn ein temporärer Verbindungsfehler auftritt.

Basierend auf Ihrer Lizenz sind die folgenden Anwendungsdienste in Bezug auf temporäre Verbindungsfehler ihrer Clients belastbar:

Datenintegrationsdienst

Der Datenintegrationsdienst ist in Bezug auf Fehler bei temporären Verbindungen zu anderen Diensten, wie zum Beispiel dem Developer Tool-Client, belastbar.

PowerCenter-Integrationsdienst

Der PowerCenter-Integrationsdienst ist in Bezug auf Fehler bei temporären Verbindungen zu anderen Diensten, dem PowerCenter Client und externen Komponenten wie Datenbanken und FTP-Server belastbar.

PowerCenter-Repository-Dienst

Der PowerCenter-Repository-Dienst ist in Bezug auf Fehler bei temporären Verbindungen zu anderen Diensten, wie zum Beispiel dem PowerCenter-Integrationsdienst, belastbar. Er ist auch bei Fehlern bei temporären Verbindungen zur Repository-Datenbank belastbar.

Knoten-Belastbarkeit

Wenn eine Domäne mehrere Knoten enthält, sind die Knoten unempfindlich gegen temporäre Kommunikationsfehler von anderen Knoten der Domäne.

Knoten sind unempfindlich gegen die folgenden temporären Verbindungsfehler:

Ein Nicht-Master-Gateway-Knoten ist nicht mehr verfügbar.

Jeder Knoten in der Domäne sendet in regelmäßigen Abständen von 15 Sekunden ein Kommunikationssignal an den Master-Gateway-Knoten. Bei Knoten mit der Dienstrolle beinhaltet die Kommunikation eine Liste der Anwendungsdienste, die auf dem Knoten ausgeführt werden.

Alle Knoten haben ein Belastbarkeits-Timeout von 90 Sekunden. Wenn ein Knoten innerhalb des Zeitraums des Belastbarkeits-Timeouts keine Verbindung zum Master-Gateway-Knoten herstellen kann, markiert der Master-Gateway-Knoten diesen Knoten als nicht verfügbar. Wenn für den Knoten, der keine Verbindung herstellen kann, die Dienstrolle aktiviert ist, weist der Master-Gateway-Knoten zusätzlich die Anwendungsdienste dieses Knotens einem Backup-Knoten zu. Dadurch wird gewährleistet, dass Dienste auf einem Knoten unabhängig von Knotenfehlern weiterhin ausgeführt werden.

Der Master-Gateway-Knoten ist nicht mehr verfügbar.

Sie können mehr als einen Knoten als Gateway konfigurieren. Ist der Master-Gateway-Knoten nicht verfügbar, wählen die Dienstmanager auf den anderen Gateway-Knoten einen anderen Master-Gateway-Knoten aus.

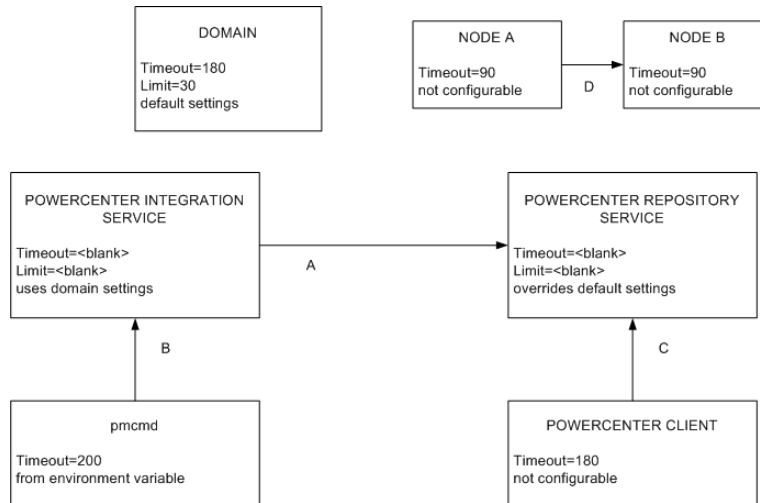
Wenn Sie nur einen Knoten als Gateway-Knoten konfigurieren und dieser nicht mehr verfügbar ist, werden alle anderen Knoten heruntergefahren.

Beispielkonfiguration für ein Belastbarkeits-Timeout

Bei einigen Belastbarkeits-Timeout-Werten handelt es sich um Standardwerte, andere wiederum können konfiguriert oder überschrieben werden.

Verwenden Sie das für die Domäne für PowerCenter-Anwendungsdienste konfigurierte Belastbarkeits-Timeout und den Grenzwert für das Belastbarkeits-Timeout, wenn Sie diesen nicht den Anwendungsdienst festgelegt haben. Befehlszeilenprogramme verwenden Sie das Dienstbelastbarkeits-Timeout. Ist der Dienstgrenzwert für das Belastbarkeits-Timeout niedriger als das Belastbarkeits-Timeout für den Client, der die Verbindung herstellt, nutzt der Client den Dienstgrenzwert als Belastbarkeits-Timeout.

In der folgenden Abbildung werden einige Beispiele für Verbindungen und Belastbarkeitskonfigurationen in einer Domäne mit PowerCenter-Anwendungsdiensten angezeigt:



Die folgende Tabelle beschreibt das Belastbarkeits-Timeout und die Grenzwerte aus der obigen Abbildung:

	Verbindung von	Verbindung zu	Beschreibung
A	PowerCenter-Integrationsdienst	PowerCenter-Repository-Dienst	Der PowerCenter-Integrationsdienst kann basierend auf dem Belastbarkeits-Timeout der Domäne maximal 30 Sekunden lang versuchen, eine Verbindung zum PowerCenter-Repository-Dienst herzustellen. Er ist nicht an den Grenzwert des PowerCenter-Repository-Diensts für das Belastbarkeits-Timeout von 60 Sekunden gebunden.
B	<i>pmcmd</i>	PowerCenter-Integrationsdienst	<i>pmcmd</i> ist an den Grenzwert des PowerCenter-Integrationsdiensts für das Belastbarkeits-Timeout von 180 Sekunden gebunden und kann das in <i>INFA_CLIENT_RESILIENCE_TIMEOUT</i> konfigurierte Belastbarkeits-Timeout von 200 Sekunden nicht nutzen.
C	PowerCenter Client	PowerCenter-Repository-Dienst	Der PowerCenter Client ist an den Grenzwert des PowerCenter-Repository-Diensts für ein Belastbarkeits-Timeout von 60 Sekunden gebunden. Das voreingestellte Belastbarkeits-Timeout von 180 Sekunden steht ihm nicht zur Verfügung.
D	Knoten A	Knoten B	Knoten A kann maximal 90 Sekunden lang versuchen, eine Verbindung zu Knoten B herzustellen. Die Dienstmanager auf Knoten A und Knoten B verwenden das standardmäßige Knotenbelastbarkeits-Timeout von 90 Sekunden.

Neustart und Failover

Um die Betriebszeit im Fehlerfall zu maximieren, kann die Informatica-Domäne den Neustart oder Failover über einen anderen Knoten ausführen.

Der Dienstmanager auf dem Master-Gateway-Knoten akzeptiert Anfragen des Anwendungsdienstes und verwaltet die Domäne. Wenn kein Master-Gateway-Knoten verfügbar ist, wird die Domäne heruntergefahren.

Um die Domäne für den Failover auf einen anderen Knoten zu konfigurieren, müssen Sie mehrere Gateway-Knoten konfigurieren.

Je nach Lizenz können Sie auch Backup-Knoten für Anwendungsdienste konfigurieren. Der Dienstmanager kann im Fehlerfall einen Neustart oder ein Failover für die folgenden Anwendungsdienste ausführen:

- Datenintegrationsdienst
- Modellrepository-Dienst
- PowerCenter-Integrationsdienst
- PowerCenter-Repository-Dienst
- PowerExchange-Listenerdienst
- PowerExchange-Protokollierungsdienst
- Ressourcenmanager-Dienst

Domänen-Failover

Der Dienstmanager auf dem Master-Gateway-Knoten nimmt Dienstanfragen entgegen und verwaltet die Domäne und die Dienste in der Domäne. Die Domäne kann ein Failover auf einen anderen Knoten durchführen, wenn die Domäne über mehrere Gateway-Knoten verfügt. Konfigurieren Sie mehrere Gateway-Knoten, um zu verhindern, dass die Domäne heruntergefahren wird, wenn der Master-Gateway-Knoten nicht verfügbar ist.

Der Master-Gateway-Knoten unterhält eine Verbindung zum Repository für die Domänenkonfiguration. Wenn das Domänenkonfigurations-Repository nicht mehr verfügbar ist, versucht der Master-Gateway-Knoten sich erneut zu verbinden, wenn ein Benutzer einen Vorgang durchführt. Wenn der Master-Gateway-Knoten keine Verbindung zum Domänenkonfigurations-Repository aufbauen kann, wird der Master-Gateway-Knoten möglicherweise heruntergefahren.

Wenn die Domäne über mehrere Gateway-Knoten verfügt und der Master-Gateway-Knoten nicht verfügbar ist, wählt der Dienstmanager auf den anderen Gateway-Knoten andere Master-Gateway-Knoten aus, um die Dienstanfragen zu akzeptieren. Die Domäne versucht bei jedem Gateway-Knoten, eine Verbindung zum Domänenkonfigurations-Repository herzustellen. Wenn keiner der Gateway-Knoten eine Verbindung herstellen kann, fährt die Domäne herunter und alle Domänenvorgänge schlagen fehl. Bei Failover des Master-Gateway rufen die Client-Tools Informationen über die alternativen Domänen-Gateways aus der Datei `domains.infa` ab.

Hinweis: Für Anwendungsdienste, die auf dem Master-Gateway-Knoten ausgeführt werden, findet kein Failover statt, wenn ein anderer Master-Gateway-Knoten ausgewählt ist. Dies trifft nicht zu, wenn für den Anwendungsdienst ein Backup-Knoten konfiguriert ist.

Anwendungsdienst - Neustart und Failover

Wenn ein Anwendungsdienstprozess nicht mehr verfügbar ist, kann der Dienstmanager den Anwendungsdienst neu starten oder ein Failover auf einen Backup-Knoten durchführen. Wenn der Dienstmanager ein Failover für einen Anwendungsdienst durchführt, startet er den Dienst auf einem anderen Knoten, für den der Dienst zur Ausführung konfiguriert ist.

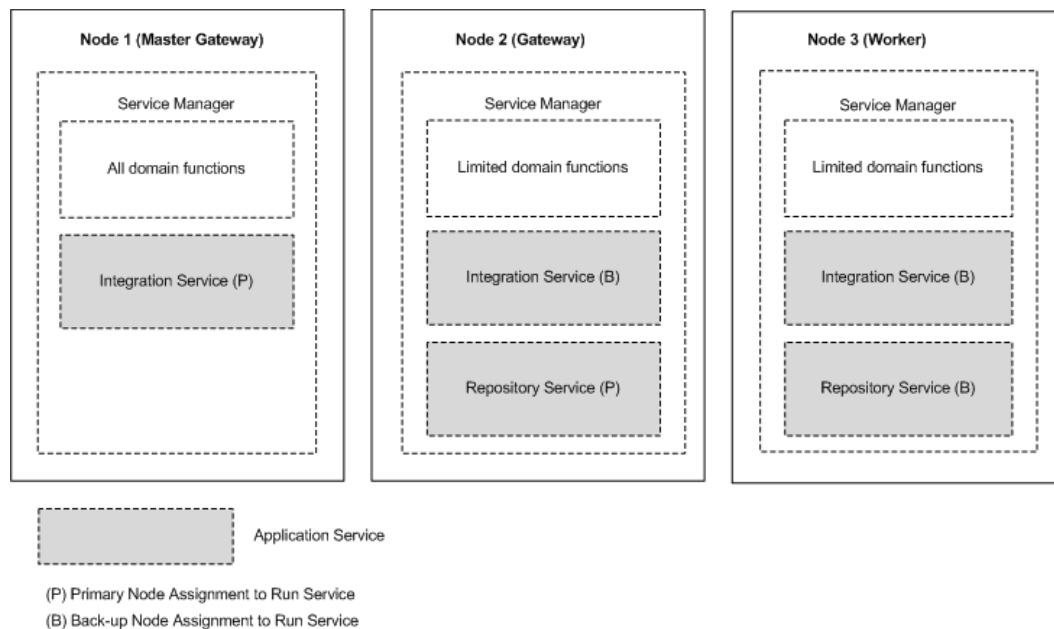
Die folgenden Situationen beschreiben, wie der Dienstmanager einen Anwendungsdienst neu startet oder wie er für diesen ein Failover durchführt:

- Wenn der primäre Knoten, auf dem der Dienstprozess ausgeführt wird, nicht mehr verfügbar ist, wechselt der Dienst auf einen Backup-Knoten. Der primäre Knoten kann möglicherweise nicht verfügbar sein, wenn er abgeschaltet wird oder die Verbindung zum Knoten nicht mehr verfügbar ist.

- Wenn der primäre Knoten, auf dem der Dienstprozess ausgeführt wird, verfügbar ist, versucht die Domäne, den Prozess gemäß den in den Domäneneigenschaften konfigurierten Neustart-Optionen neu zu starten. Wenn der Prozess nicht neu gestartet wird, kann der Dienstmanager den Prozess als fehlgeschlagen kennzeichnen. Der Dienst führt dann ein Failover auf einen Backup-Knoten durch und startet einen anderen Prozess. Wenn der Dienstmanager den Prozess als fehlgeschlagen kennzeichnet, muss der Administrator den Prozess nach Behebung möglicher Konfigurationsprobleme aktivieren.

Beim Failover eines Dienstprozesses auf einen Backup-Knoten wechselt er nicht zurück auf den primären Knoten, wenn dieser wieder verfügbar wird. Sie können den Dienstprozess auf dem Backup-Knoten deaktivieren, damit er wieder auf den primären Knoten wechselt.

Die folgende Abbildung zeigt, wie Sie primäre und Backup-Knoten für einen Anwendungsdienst konfigurieren können:



Wiederherstellung

Bei der Wiederherstellung handelt es sich um den Abschluss von Operationen, nachdem ein unterbrochener Dienst wiederhergestellt wurde. Der Betriebsstatus eines Dienstes enthält Informationen über den Dienstprozess.

Je nach Lizenz können die folgenden Komponenten wiederhergestellt werden, nachdem ein unterbrochener Dienst wieder hergestellt wurde:

Dienstmanager

Der Dienstmanager für jeden Knoten in der Domäne pflegt den Status der auf dem jeweiligen Knoten ausgeführten Dienstprozesse. Wenn das Master-Gateway heruntergefahren wird, erfasst das neu gewählte Master-Gateway die Zustandsinformationen jedes Knotens, um den Zustand der Domäne wiederherzustellen.

PowerCenter-Repository-Dienst

Der PowerCenter-Repository-Dienst pflegt den Betriebsstatus im Repository. Der Betriebsstatus enthält Informationen zu Repository-Sperren, laufenden Anfragen und verbundenen Clients. Nach einem

Neustart oder Failover kann der PowerCenter-Repository-Dienst den Betriebsstatus ab dem Zeitpunkt der Unterbrechung wiederherstellen.

PowerCenter-Integrationsdienst

Der PowerCenter-Integrationsdienst pflegt den Betriebsstatus im gemeinsam genutzten Speicher, der für den Dienst konfiguriert ist. Der Betriebsstatus enthält Informationen über geplante, laufende und abgeschlossene Aufgaben für den Dienst.

Der PowerCenter-Integrationsdienst pflegt den Betriebszustand von PowerCenter-Sitzungen und Arbeitsabläufen auf der Basis der Wiederherstellungsstrategie, die Sie für die Sitzung und den Arbeitsablauf konfigurieren. Wenn der PowerCenter-Integrationsdienst neu gestartet wird oder einen Failover für einen Dienstprozess ausführt, werden jene unterbrochenen Arbeitsabläufe automatisch wiederhergestellt, die für eine Wiederherstellung konfiguriert wurden.

Datenintegrationsdienst

Der Datenintegrationsdienst pflegt den Betriebsstatus im Modellrepository. Der Betriebsstatus enthält den Status des Arbeitsablaufs und der Aufgaben im Arbeitsablauf sowie die Werte der Arbeitsablaufvariablen und -parameter während der unterbrochenen Arbeitsablaufinstanz.

Wenn ein Datenintegrationsdienst einen Neustart oder Failover eines Dienstprozesses ausführt, können Sie unterbrochene Arbeitsabläufe, die für die Arbeitsablaufwiederherstellung aktiviert sind, manuell neu starten.

Konfiguration für einen hochverfügbare Domäne

Um die Systemausfallzeit zu minimieren, konfigurieren Sie Hochverfügbarkeit für die Informatica-Domänenkomponenten.

Sie können die folgenden Informatica-Domänenkomponenten als hoch verfügbar konfigurieren:

Domäne

Ein Knoten in der Domäne fungiert als Gateway für Dienstanforderungen von Clients und leitet sie an den entsprechenden Dienst und Knoten weiter. Um zu verhindern, dass die Domäne herunterfährt, wenn der Master-Gateway-Knoten nicht verfügbar ist, konfigurieren Sie mehr als einen Gateway-Knoten.

Knoten

Informatica-Dienste sind Prozesse, die auf jedem Knoten ausgeführt werden. Konfigurieren Sie Informatica-Dienste so, dass sie automatisch neu gestartet werden, wenn sie unerwartet beendet werden.

Anwendungsdienste

Die Anwendungsdienste werden auf Knoten in der Informatica-Domäne ausgeführt.

Basierend auf Ihrer Lizenz können Sie die folgenden Hochverfügbarkeitsfunktionen für Anwendungsdienste konfigurieren:

- Um die Ausfallzeit von Anwendungsdiensten zu minimieren, konfigurieren Sie Sicherungsknoten für Anwendungsdienste.
- Um den Belastbarkeitszeitraum für Anwendungsdienste anzugeben, überprüfen Sie die Einstellungen und konfigurieren Sie Zeiträume für das Belastbarkeits-Timeout für Anwendungsdienste.
- Um Failover und Wiederherstellung für den PowerCenter-Integrationsdienst sicherzustellen, konfigurieren Sie den PowerCenter-Integrationsdienst zum Speichern der Prozess-Statusinformationen in einem POSIX-kompatiblen gemeinsam genutzten Dateisystem oder in einer Datenbank.

Anwendungs-Clients

Anwendungs-Clients bieten Zugriff auf Informatica-Funktionen und werden auf Benutzercomputern ausgeführt. Anwendungs-Clients senden Anfragen an den Dienstmanager oder an Anwendungsdienste.

Sie können Zeiträume für das Belastbarkeits-Timeout für Befehlszeilenprogramme konfigurieren. Sie können kein Belastbarkeits-Timeout für PowerCenter Clients konfigurieren.

Externe Systeme

Verwenden Sie hoch verfügbare Versionen von externen Systemen, wie zum Beispiel Quell- und Zieldatenbanken, Meldungswarteschlangen und FTP-Server.

Netzwerk

Sorgen Sie für eine hohe Verfügbarkeit des Netzwerkes, indem Sie redundante Komponenten wie Router, Kabel und Netzwerkadapterkarten konfigurieren.

Konfiguration der Belastbarkeit für Anwendungsdienste

Wenn ein temporärer Netzwerkfehler auftritt, versuchen Anwendungsdienste, eine erneute Verbindung zu anderen Anwendungsdiensten für die Dauer des Belastbarkeits-Timeouts herzustellen. Sie können das Belastbarkeits-Timeout für Anwendungsdienste konfigurieren.

Wenn ein Anwendungsdienst eine Verbindung zu einem anderen Anwendungsdienst in der Domäne herstellt, handelt es sich bei dem Dienst, der die Verbindung initiiert, um einen Client eines anderen Diensts.

Sie können Belastbarkeits-Timeouts für Anwendungsdienste für die folgenden Anwendungsdienste konfigurieren:

PowerCenter-Anwendungsdienste

Sie können das Belastbarkeits-Timeout und Beschränkungen für das Belastbarkeits-Timeout in den erweiterten Eigenschaften des PowerCenter-Integrationsdiensts und des PowerCenter-Repository-Diensts konfigurieren. Das Belastbarkeits-Timeout für Anwendungsdienste, das eine Verbindung zu einem PowerCenter-Integrationsdienst oder PowerCenter-Repository-Dienst herstellt, wird durch einen der folgenden Werte bestimmt:

- Die Diensteigenschaft **Belastbarkeits-Timeout**. Das Belastbarkeits-Timeout für den Dienst können Sie in den Diensteigenschaften konfigurieren. Wenn Sie die Belastbarkeit für einen Dienst deaktivieren möchten, setzen Sie das Belastbarkeits-Timeout auf 0.
- Die Domäneneigenschaft **Belastbarkeits-Timeout**. Um das für die Domäne konfigurierte Belastbarkeits-Timeout zu verwenden, nehmen Sie im Feld für das Belastbarkeits-Timeout für den Dienst keine Eingabe vor.
- Die Diensteigenschaft **Grenzwert für Belastbarkeits-Timeout**. Ist der Dienstgrenzwert für das Belastbarkeits-Timeout niedriger als das Belastbarkeits-Timeout für den Client, der die Verbindung herstellt, nutzt der Client den Grenzwert als Belastbarkeits-Timeout. Um den Grenzwert für das für die Domäne konfigurierte Belastbarkeits-Timeout zu benutzen, nehmen Sie im Feld für den Grenzwert für Belastbarkeits-Timeout keine Eingabe vor.
- Die Domäneneigenschaft **Grenzwert des Belastbarkeits-Timeout**. Verwenden Sie das für die Domäne konfigurierte Belastbarkeits-Timeout und nehmen Sie im Feld für das Belastbarkeits-Timeout für den Dienst keine Eingabe vor.

Sie können das Belastbarkeits-Timeout für den SAP BW-Dienst in den allgemeinen Diensteigenschaften konfigurieren. Die Eigenschaft des Belastbarkeits-Timeouts für den SAP BW-Dienst Eigenschaft wird als **Wiederholungsperiode** bezeichnet.

Hinweis: Wenn Sie den Dienst im Administrator-Tool deaktivieren, kann der Client keine Belastbarkeit für Dienstunterbrechungen aufweisen. Wenn Sie den Dienstprozess deaktivieren, ist der Client in Bezug auf Dienstunterbrechung belastbar.

Failover-Konfiguration für einen Anwendungsdienst

Basierend auf Ihrer Lizenz können Sie Backup-Knoten so konfigurieren, dass Anwendungsdienste ein Failover zu einem anderen Knoten durchführen können, wenn der primäre Knoten fehlschlägt. Konfigurieren Sie Backup-Knoten beim Erstellen oder Aktualisieren eines Anwendungsdienstes.

Wenn Sie einen Backup-Knoten konfigurieren, stellen Sie sicher, dass der Knoten Zugriff auf Laufzeitdateien hat, die jeder Anwendungsdienst benötigt, um Datenintegrationsaufgaben wie Arbeitsabläufe und Mappings durchzuführen. Ein Arbeitsablauf benötigt möglicherweise Parameterdateien, Eingabedateien oder Ausgabedateien.

Konfiguration für Failover und Wiederherstellung des PowerCenter-Integrationsdienstes

Während Failover und Wiederherstellung muss der PowerCenter-Integrationsdienst auf Vorgangstatusdateien zugreifen und Statusinformationen verarbeiten können.

In den Vorgangstatusdateien wird der Status aller Arbeitsablauf- und Sitzungsvorgänge gespeichert. Der PowerCenter-Integrationsdienst speichert den Status aller Arbeitsablauf- und Sitzungsvorgänge in Dateien im Verzeichnis \$PMStorageDir des PowerCenter-Integrationsdienstprozesses.

In den Informationen zum Prozessstatus wird angegeben, welcher Knoten den PowerCenter-Hauptintegrationsdienst und welcher Knoten die jeweilige Sitzung ausgeführt hat. Sie können den PowerCenter-Integrationsdienst konfigurieren, um Informationen zum Prozessstatus in einem Cluster-Dateisystem oder in der PowerCenter-Repository-Datenbank zu speichern.

Speichern von Hochverfügbarkeits-Persistenz in einem Cluster-Dateisystem

Standardmäßig speichert der PowerCenter-Integrationsdienst Informationen zum Prozessstatus mit den Vorgangstatusdateien im Verzeichnis \$PMStorageDir des Integrationsdienstprozesses. Sie müssen das Verzeichnis \$PMStorageDir für jeden PowerCenter-Integrationsdienstprozess zur Verwendung desselben Verzeichnisses in einem Cluster-Dateisystem konfigurieren.

Knoten, auf denen der PowerCenter-Integrationsdienst ausgeführt wird, müssen sich im selben Cluster-Dateisystem befinden, um Ressourcen gemeinsam nutzen zu können. Darüber hinaus müssen Knoten innerhalb eines Clusters im Heartbeat-Netz des Cluster-Dateisystems liegen. Verwenden Sie ein Cluster-Dateisystem mit hoher Verfügbarkeit, das für I/O-Fencing konfiguriert ist. Die Hardwareanforderungen und Konfiguration einer I/O-Fencing-Lösung sind für jedes Dateisystem unterschiedlich.

Die folgenden Cluster-Dateisysteme sind von Informatica für den Einsatz bei PowerCenter-Integrationsdienst-Failover und -Sitzungswiederherstellung zertifiziert:

Storage Array Network

- Veritas Cluster Files System (VxFS)

- IBM General Parallel File System (GPFS)

Network Attached Storage mit NFS v3-Protokoll

- EMC UxFS, auf einem EMV Celerra NAS-Appliance gehostet

- NetApp WAFL auf einem NetApp NAS-Appliance gehostet

Wenden Sie sich direkt an die entsprechenden Anbieter der Dateisysteme, die Ihren Anforderungen entsprechen.

Speichern von Hochverfügbarkeits-Persistenz in einer Datenbank

Sie können den PowerCenter-Integrationsdienst so konfigurieren, dass Informationen zum Prozessstatus in Datenbanktabellen gespeichert werden. Wenn Sie den PowerCenter-Integrationsdienst zum Speichern von Informationen zum Prozessstatus in einer Datenbank konfigurieren, speichert der Dienst weiterhin den Status

aller Arbeitsablauf- und Sitzungsvorgänge in Dateien im Verzeichnis \$PMStorageDir. Sie können das Verzeichnis \$PMStorageDir zur Verwendung eines POSIX-konformen freigegebenen Dateisystems konfigurieren. Sie müssen kein Cluster-Dateisystem verwenden.

Konfigurieren Sie den PowerCenter-Integrationsdienst so, dass Informationen zum Prozessstatus in Datenbanktabellen in den erweiterten Eigenschaften gespeichert werden. Der PowerCenter-Integrationsdienst speichert Informationen zum Prozessstatus in persistenten Datenbanktabellen in der zugeordneten PowerCenter-Repository-Datenbank.

Beim Failover wird die automatische Wiederherstellung von Arbeitsabläufen wiederaufgenommen, sobald der Dienstprozess auf die Datenbanktabellen zugreifen kann.

Konfiguration der Belastbarkeit für Befehlszeilenprogramme

Sie können das Belastbarkeits-Timeout konfigurieren, das Befehlszeilenprogramme zum Ausführen von Domänen- und Service-Vorgängen verwenden.

Wenn Sie die Befehlszeilenprogramme `infacmd`, `pmcmd` oder `pmrep` zum Herstellen einer Verbindung zur Domäne oder zu einem Anwendungsdienst verwenden, wird das Belastbarkeits-Timeout durch die Befehlszeilenoption, eine Umgebungsvariable oder das Standardbelastbarkeits-Timeout festgelegt.

Verwenden Sie die folgenden Richtlinien, wenn Sie Befehlszeilenprogramm-Belastbarkeit konfigurieren:

Befehlszeilenoption

Sie können das Belastbarkeits-Timeout für `infacmd` festlegen, indem Sie beim Ausführen eines Befehls immer die Befehlszeilenoption `-ResilienceTimeout` verwenden. Sie können das Belastbarkeits-Timeout für `pmcmd` festlegen, indem Sie beim Ausführen eines Befehls immer die Befehlszeilenoption `-timeout` verwenden. Wenn Sie den `pmrep`-Befehl `"Connect"` zum Herstellen einer Verbindung zu einem Repository verwenden, können Sie die Befehlszeilenoption `-timeout` verwenden, um das Belastbarkeits-Timeout für `pmrep`-Befehle festzulegen, die die Verbindung verwenden.

Umgebungsvariable.

Wenn Sie die Timeout-Option nicht in der Befehlszeilensyntax `infacmd` und `pmcmd` festlegen, verwenden die Befehlszeilenprogramme `infacmd` und `pmcmd` den Wert der auf dem Client-Computer konfigurierten Umgebungsvariable `INFA_CLIENT_RESILIENCE_TIMEOUT`. Sollten Sie die Timeout-Option nicht festlegen, wenn Sie den `pmrep`-Befehl `"Connect"` zum Herstellen einer Verbindung zum Repository verwenden, verwenden `pmrep`-Befehle den Wert der auf dem Client-Computer konfigurierten Umgebungsvariable `INFA_CLIENT_RESILIENCE_TIMEOUT`.

Standardwert

Wenn Sie nicht die Befehlszeilenoption bzw. die Umgebungsvariable verwenden, verwenden die Befehlszeilenprogramme `pmcmd` und `pmrep` das Standard-Belastbarkeits-Timeout von 180 Sekunden. Wenn Sie nicht die Befehlszeilenoption bzw. die Umgebungsvariable verwenden, verwendet das Befehlszeilenprogramm `infacmd` den Wert der Domäneneigenschaft **Dienstebenen-Timeout** als Standard-Belastbarkeits-Timeout.

Grenzwert für Timeout

Wenn der Grenzwert für den Belastbarkeits-Timeout für den PowerCenter-Integrationsdienst oder den PowerCenter-Repository-Dienst kleiner als das Befehlszeilen-Belastbarkeits-Timeout ist, verwendet das Befehlszeilenprogramm den Grenzwert als Belastbarkeits-Timeout.

Hinweis: PowerCenter bietet keine Belastbarkeit für einen Repository-Client, wenn der PowerCenter-Repository-Dienst im exklusiven Modus ausgeführt wird.

Domänen-Failover-Konfiguration

Sie können mehrere Gateway-Knoten definieren, um zu verhindern, dass die Domäne heruntergefahren wird, wenn der Master-Gateway-Knoten nicht verfügbar ist.

Bei der Erstinstallation von Informatica-Diensten erstellen Sie einen Gateway-Knoten. Nach der Installation von Informatica können Sie weitere Gateway-Knoten definieren. Um einen Gateway-Knoten zu definieren, fügen Sie der Domäne einen Gateway-Knoten hinzu oder konfigurieren Sie einen Worker-Knoten, der als Gateway-Knoten eingesetzt wird.

Konfiguration des Knoten-Neustarts

Die Informatica-Dienste führen den Dienstmanager auf allen Knoten in der Domäne aus. Sie können die Informatica-Dienste so konfigurieren, dass sie beim unerwarteten Beenden und Starten eines Knotens automatisch starten.

Um die Informatica-Dienste bei Neustart eines Knotens neu zu starten, führen Sie die folgenden Schritte durch:

- Erstellen Sie in einer UNIX-Umgebung ein Skript, das die Informatica-Dienste automatisch startet, wenn der Knoten startet.
- Gehen Sie in einer Windows-Umgebung in die Systemsteuerung und konfigurieren Sie die Informatica-Dienste für einen automatischen Neustart.

Sie können den Neustart unabhängig von Knotentyp und Knotenrolle für alle Knoten konfigurieren.

Oracle RAC-Datenbank-Failover

Sie können Oracle Real Application Cluster (RAC) verwenden, um eine Verbindung mit einem Oracle-Dienst anzugeben, der mit Lastausgleich und hoher Verfügbarkeit aktiviert ist. Oracle RAC verteilt die Arbeitslast unter allen verfügbaren Knoten auf dem Cluster. Wenn ein Knoten ausfällt, wird die Arbeitslast des nicht verfügbaren Knotens auf einen verfügbaren Knoten übertragen. Verwenden Sie Oracle RAC-Lastausgleichsverbindungen in einer ausfallgesicherten Umgebung, um sicherzustellen, dass eine Datenbankverbindung verfügbar ist, auch wenn ein oder mehr RAC-Knoten ausfallen.

Die folgenden Vorgänge im PowerCenter-Repository-Dienst sind stabil gegenüber dem Datenbank-Failover beim Oracle RAC-Setup:

- ExecuteQuery
- ObjectExport
- ObjectImport
- PurgeVersion
- RollbackDeployment

Sie können keine Administratorvorgänge mit Oracle RAC-Datenbank-Failover für die Informatica-Domäne und den Modellrepository-Dienst ausführen.

Netzwerk, hohe Verfügbarkeit

Die Lösungen für die folgenden Situationen können Ihnen bei der hohen Verfügbarkeit helfen.

Ich bin mir nicht sicher, wo ich nach Informationen über den Status für Client-Verbindungen zum PowerCenter-Repository suchen kann.

In PowerCenter Client-Anwendungen, wie z. B. dem PowerCenter Designer und dem Workflow Manager, wird eine Fehlermeldung angezeigt, wenn die Verbindung nicht während des Zeitlimits aufgebaut werden kann. Detaillierte Informationen über Verbindungsfehler finden Sie im Ausgabe-Fenster. Wenn Sie *pmrep* verwenden, erscheinen die Informationen zu Verbindungsfehlern in der Befehlszeile. Wenn der PowerCenter Integration Service keine Verbindung zum Repository aufbauen kann, erscheint der Fehler im PowerCenter Integration Service-Log, im Arbeitsablauf-Log und im Sitzungs-Log.

Ich habe den falschen Verbindungsstring für eine Oracle-Datenbank eingegeben. Jetzt kann ich den PowerCenter Repository Service nicht aktivieren, obwohl ich die Eigenschaften des PowerCenter Repository Service bearbeitet habe, sodass der richtige Verbindungsstring verwendet wird.

Sie müssen warten, bis das Datenbank-Resistenz-Timeout abgelaufen ist, bevor Sie den PowerCenter Repository Service mit dem aktualisierten Verbindungsstring aktivieren können.

Ich verfüge über die Option für hohe Verfügbarkeit, aber mein FTP-Server ist bei einem Ausfall der Netzwerkverbindung nicht resistent.

Der FTP-Server ist ein externes System. Um eine hohe Verfügbarkeit für FTP-Übertragungen zu erreichen, müssen Sie einen hoch verfügbaren FTP-Server einsetzen. Zum Beispiel verfügt Microsoft IIS 6.0 nicht über eine native Unterstützung für den Neustart des Datei-Uploads oder Datei-Downloads. Das Neustarten von Dateien muss von dem Client verwaltet werden, der die Verbindung zum IIS-Server herstellt. Wenn die Übertragung einer Datei zum oder vom IIS 6.0-Server unterbrochen und innerhalb der Client-Belastbarkeits-Timeouts dann wiederhergestellt wird, wird die Übertragung nicht unbedingt wie erwartet fortgesetzt. Wenn der Schreibvorgang zu mehr als der Hälfte abgeschlossen ist, kann die Targetdatei abgelehnt werden.

Ich verfüge über die Option für hohe Verfügbarkeit, aber die Informatica-Domäne ist nicht resistent, wenn Computer über ein Netzwerk verbunden sind.

Wenn Sie mit einem Netzwerk-Switch für die Verbindung von Computern in der Domäne nutzen, müssen Sie die Auto-Select-Option für den Switch verwenden.

KAPITEL 8

Verbindungen

Dieses Kapitel umfasst die folgenden Themen:

- [Verbindungen - Übersicht, 121](#)
- [Verbindungsverwaltung, 121](#)
- [Pass-Through-Sicherheit, 125](#)
- [Poolingeigenschaften in Verbindungsobjekten, 126](#)

Verbindungen - Übersicht

Eine Verbindung ist ein Repository-Objekt, das eine Verbindung im Domänenkonfigurations-Repository definiert.

Der Datenintegrationsdienst verwendet Datenbankverbindungen, um Jobs für das Developer-Tool und das Analyst-Tool zu verarbeiten. Jobs beinhalten Mappings, Profile, Scorecards und SQL-Datendienste.

Sie können Verbindungen im Administrator-Tool, im Developer-Tool und im Analyst-Tool erstellen und verwalten.

Welche Aufgaben Sie jeweils in den einzelnen Tools ausführen können, hängt vom jeweiligen Tool ab. Beispiel: Sie können eine SAP NetWeaver-Verbindung im Developer-Tool erstellen und diese im Administrator-Tool verwalten; im Analyst-Tool hingegen können Sie diese Verbindung weder erstellen noch verwalten.

Hinweis: Diese Verbindungen sind unabhängig von den Verbindungen, die Sie im PowerCenter-Arbeitsablauf-Manager erstellen.

Verbindungsverwaltung

Nach dem Erstellen einer Verbindung können Sie die Verbindung anzeigen, die Verbindungseigenschaften konfigurieren und die Verbindung löschen.

Nachdem Sie eine Verbindung erstellt haben, können Sie die folgenden Aktionen ausführen:

Konfigurieren von Verbindungspooling.

Konfigurieren Sie Verbindungspooling, um die Verarbeitung für den Datenintegrationsdienst zu optimieren. Das Verbindungspooling ist ein Framework zu Cache-Verbindungen.

Anzeigen von Verbindungseigenschaften.

Zeigen Sie die Verbindungseigenschaften über die Ansicht **Verbindungen** auf der Registerkarte **Verwalten** an.

Bearbeiten der Verbindung.

Sie können den Namen und die Beschreibung für die Verbindung ändern. Sie können auch Verbindungsdetails wie den Benutzernamen, das Passwort und Verbindungszeichenfolgen bearbeiten. Wenn Sie eine Datenbankverbindung aktualisieren, die Verbindungspooling deaktiviert hat, werden alle Updates sofort wirksam.

Der Datenintegrationsdienst identifiziert Verbindungen anhand der Verbindungs-ID und nicht mit dem Namen der Verbindung. Wenn Sie eine Verbindung umbenennen, aktualisieren das Developer Tool und das Analyst Tool die Jobs, die die Verbindung verwenden.

Bereitgestellte Anwendungen und Parameterdateien identifizieren eine Verbindung nach Namen, nicht nach Verbindungs-ID. Beim Umbenennen einer Verbindung müssen Sie daher alle Anwendungen erneut bereitstellen, die die Verbindung verwenden. Außerdem müssen Sie alle Parameterdateien aktualisieren, die den Verbindungsparameter verwenden.

Löschen der Verbindung.

Wenn Sie eine Verbindung löschen, sind die Objekte, die diese Verbindung verwenden, nicht mehr gültig. Wenn Sie eine Verbindung versehentlich löschen, können Sie sie neu erstellen, indem Sie eine andere Verbindung mit derselben Verbindungs-ID wie die gelöschte Verbindung erstellen.

Aktualisieren der Verbindungsliste.

Sie können die Verbindungsliste aktualisieren, um eine Liste mit den neuesten Verbindungen für die Domäne anzuzeigen. Aktualisieren Sie die Verbindungsliste, nachdem ein Benutzer eine Verbindung im Developer Tool oder im Analyst Tool hinzugefügt, gelöscht oder umbenannt hat.

Erstellen einer Verbindung

Im Administrator Tool können Sie Verbindungen zu relationalen Datenbanken, sozialen Medien und Dateisystemen herstellen.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie auf die Ansicht **Verbindungen**.
3. Wählen Sie die Domäne im Navigator aus.
4. Klicken Sie im Navigator auf **Aktionen > Neu > Datenbankverbindung**.
Das Dialogfeld **Neue Datenbankverbindung** wird eingeblendet.
5. Wählen Sie im Dialogfeld **Neue Verbindung** den Verbindungstyp aus, und klicken Sie dann auf **OK**.
Die **Neue Verbindung** wird angezeigt.
6. Geben Sie die Verbindungseigenschaften ein.
Die Verbindungseigenschaften, die Sie eingeben, richten sich nach dem Verbindungstyp. Klicken Sie auf **Weiter**, um zur nächsten Seite im Assistenten **Neue Verbindung** zu wechseln.
7. Klicken Sie nach der Eingabe der Verbindungseigenschaften auf **Verbindung testen**, um die Verbindung zu testen.
8. Klicken Sie auf **Fertig stellen**.

Aktualisieren der Verbindungsliste

Aktualisieren Sie die Verbindungsliste, um die neueste Liste der Verbindungen in der Domäne anzuzeigen.

Das Administrator-Tool zeigt die neueste Verbindungsliste beim Starten des Administrator-Tool an. Wenn ein Benutzer eine Verbindung im Developer-Tool oder im Analyst-Tool hinzufügt, löscht oder umbenennt, ist eine Aktualisierung der Verbindungsliste empfehlenswert.

1. Klicken Sie im Administrator-Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie auf die Ansicht **Verbindungen**.
Der Navigator zeigt alle Verbindungen in der Domäne an.
3. Wählen Sie die Domäne im Navigator aus.
4. Klicken Sie auf **Aktionen > Aktualisieren**.

Anzeigen einer Verbindung

Mit den folgenden Schritten zeigen Sie Verbindungen im Administrator Tool an.

1. Klicken Sie im Administrator-Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie auf die Ansicht **Verbindungen**.
Der Navigator zeigt alle Verbindungen in der Domäne an.
3. Wählen Sie im Navigator die Domäne.
Der Inhaltsbereich zeigt alle Verbindungen der Domäne an.
4. Zum Filtern der im Inhaltsbereich angezeigten Verbindungen, geben Sie ein Filterkriterium ein und klicken auf die Schaltfläche Filter.
Der Inhaltsbereich zeigt die Verbindungen an, die dem Filterkriterium entsprechen.
5. Um das Filterkriterium zu entfernen, klicken Sie auf die Schaltfläche "Filter zurücksetzen".
Der Inhaltsbereich zeigt alle Verbindungen der Domäne an.
6. Sortieren Sie die Verbindungen, indem Sie in die Spaltenüberschrift klicken, anhand derer die Verbindungen sortiert werden sollen.
Standardmäßig sind die Verbindungen anhand des Namens sortiert.
7. Um Spalten aus dem Inhaltsbereich zu entfernen oder neue hinzuzufügen, klicken Sie die Spaltenüberschrift mit der rechten Maustaste an.
Wenn Sie eine Leseberechtigung für die Verbindung haben, können Sie die Daten in der Spalte **Erstellt durch** sehen. Andernfalls ist diese Spalte leer.
8. Um die Verbindungsdetails anzuzeigen, wählen Sie eine Verbindung im Navigator aus.
Der Inhaltsbereich zeigt die Verbindungsdetails an.

Konfigurieren des Pooling für eine Verbindung

Das Pooling für eine Verbindung wird im Administrator Tool konfiguriert.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie auf die Ansicht **Verbindungen**.
3. Wählen Sie im Domänen-Navigator eine Verbindung aus.
Der Inhaltsbereich zeigt die Verbindungseigenschaften an.
4. Klicken Sie im Inhaltsbereich auf die Ansicht **Pooling**

5. Klicken Sie im Bereich **Pooling-Eigenschaften** auf **Bearbeiten**.
Das Dialogfeld **Pooling-Eigenschaften bearbeiten** wird angezeigt.
6. Bearbeiten Sie die Pooling-Eigenschaften und klicken Sie auf **OK**.

Bearbeiten und Testen einer Verbindung

Im Administrator Tool können Sie Verbindungen bearbeiten, die Sie im Administrator Tool, im Analyst Tool, im Developer Tool oder mit dem `infacmd isp CreateConnection`-Befehl erstellt haben. Sie können relationale Datenbankverbindungen testen.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie auf die Ansicht **Verbindungen**.
Der Navigator zeigt alle Verbindungen in der Domäne an.
3. Wählen Sie im Navigator eine Verbindung aus.
Der Inhaltsbereich zeigt die Verbindungseigenschaften.
4. Wählen Sie im Inhaltsbereich die Ansicht **Eigenschaften** oder **Pooling** aus.
5. Um Eigenschaften in einem Abschnitt zu bearbeiten, klicken Sie auf **Bearbeiten**.
Bearbeiten Sie die Eigenschaften und klicken Sie auf **OK**.

Hinweis: Wenn Sie einen Verbindungsnamen ändern, müssen Sie alle Anwendungen, die die Verbindung verwenden, erneut bereitstellen. Außerdem müssen Sie alle Parameterdateien aktualisieren, die den Verbindungsparameter verwenden.

6. Um eine Datenbankverbindung zu überprüfen, wählen Sie die Verbindung im Navigator aus.
Klicken Sie auf **Aktionen > Testverbindung** auf der Registerkarte **Verwalten**.

Hinweis: Über die Schaltfläche **Testverbindung** wird die Verbindungszeichenfolge der Metadaten-Zugriffseigenschaften und nicht die der Datenzugriffseigenschaften getestet.

Das Testergebnis wird in einem Meldungsfenster angezeigt.

Löschen einer Verbindung

Sie können eine Datenbankverbindung im Administrator-Tool löschen.

Wenn Sie eine Datenbankverbindung im Administrator-Tool löschen, entfernen Sie diese auch aus dem Developer-Tool und dem Analyst-Tool.

1. Klicken Sie im Administrator-Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie auf die Ansicht **Verbindungen**.
Der Navigator zeigt alle Verbindungen in der Domäne an.
3. Wählen Sie im Navigator eine Verbindung aus.
4. Klicken Sie im Navigator auf **Aktionen > Löschen**.

Pass-Through-Sicherheit

Pass-Through-Sicherheit ist die Möglichkeit der Verbindung mit einem SQL-Datendienst oder einer externen Quelle unter Verwendung der Client-Anmeldeinformationen anstelle der Anmeldeinformationen eines Verbindungsobjekts.

Abhängig von ihrer Aufgabe im Unternehmen können Benutzer Zugriff auf verschiedene Gruppen von Daten haben. Client-Systeme beschränken den Zugriff auf Datenbanken anhand von Benutzernamen und Passwort. Wenn Sie einen SQL-Datendienst erstellen, können Sie Daten aus verschiedenen Systemen kombinieren und so eine einzige Ansicht der Daten erstellen. Wenn Sie jedoch die Verbindung zum SQL-Datendienst definieren, hat die Verbindung einen Benutzernamen und ein Passwort.

Wenn Sie die Pass-Through-Sicherheit konfigurieren, können Sie Benutzer bei einigen der Daten in einem SQL-Datendienst auf der Basis ihres Benutzernamens einschränken. Wenn sich ein Benutzer mit dem SQL-Datendienst verbindet, ignoriert der Datenintegrationsdienst den Benutzernamen und das Passwort im Verbindungsobjekt. Der Benutzer stellt die Verbindung mit dem Client-Benutzernamen oder dem LDAP-Benutzernamen her.

Das Mapping von Web-Dienstoperationen muss möglicherweise ein Verbindungsobjekt für den Zugriff auf Daten verwenden. Wenn Sie Pass-Through-Sicherheit konfigurieren und der Web-Dienst WS-Security nutzt, stellt das Mapping der Web-Dienstoperation eine Verbindung zu einer Quelle mit dem Benutzernamen und dem Passwort her, die in der SOAP-Anfrage des Web-Dienstes bereitgestellt wurden.

Konfigurieren Sie die Pass-Through-Sicherheit für eine Verbindung in den Verbindungseigenschaften des Administratortools oder mit `infacmd` die `UpdateServiceOptions`. Sie können die Pass-Through-Sicherheit für Verbindungen zu bereitgestellten Anwendungen festlegen. Sie können die Pass-Through-Sicherheit nicht im Developer Tool festlegen. Nur SQL-Datendienste und Webdienste erkennen die Pass-Through-Sicherheitskonfiguration.

Beispiel

Eine Organisation vereint Mitarbeiterdaten von mehreren Datenbanken, um eine einzelne Ansicht der Mitarbeiterdaten in einem SQL-Datendienst darzustellen. Der SQL-Datendienst enthält Daten aus den Datenbanken "Mitarbeiter" und "Vergütung". Die Datenbank "Mitarbeiter" enthält Informationen zu Namen, Adresse und Abteilung. Die Datenbank "Vergütung" enthält Informationen zu Gehalt und Aktienoptionen.

Ein Benutzer kann beispielsweise Zugriff auf die Mitarbeiterdatenbank, jedoch nicht auf die Vergütungsdatenbank haben. Wenn der Benutzer eine Abfrage auf den SQL-Datendienst ausführt, ersetzt der Datenintegrationsdienst die Anmeldeinformationen bei jeder Datenbankverbindung durch den Benutzernamen und das Benutzerpasswort. Die Abfrage schlägt fehl, wenn der Benutzer Gehaltsinformationen aus der Verbindung mit aufnimmt.

Pass-Through-Sicherheit mit Datenobjekt-Zwischenspeicherung

Für den Einsatz des Datenobjekt-Cache mit Pass-Through-Sicherheit müssen Sie Cache in den Pass-Through-Sicherheitseigenschaften für den Data Integration Service aktivieren.

Wenn Sie einen SQL-Datendienst oder einen Web-Dienst bereitstellen, können Sie wählen, ob Sie die logischen Datenobjekte in einer Datenbank zwischenspeichern möchten. Sie müssen die Datenbank zum Speichern des Datenobjekt-Cache angeben. Der Data Integration Service validiert die Benutzer-Anmeldedaten für den Zugriff auf die Cache-Datenbank. Ein Benutzer, der sich mit der Cache-Datenbank verbinden kann, hat Zugriff auf alle Tabellen im Cache-Speicher. Ist Cache aktiviert, führt der Data Integration Service keine Validierung der Benutzer-Anmeldedaten gegen die Quelldatenbanken durch.

Beispiel: Sie konfigurieren Cache für den EmployeeSQLDS SQL Datendienst und aktivieren Pass-Through-Sicherheit für Verbindungen. Der Data Integration Service speichert im Cache Tabellen aus den Kompensations- und Mitarbeiterdatenbanken. Unter Umständen hat ein Benutzer keinen Zugriff auf die

Kompensations-Datenbank. Hat der Benutzer jedoch Zugriff auf die Cache-Datenbank, kann er in einer SQL-Anfrage Kompensationsdaten auswählen.

Wenn Sie Pass-Through-Sicherheit konfigurieren, wird Datenobjekt-Cache per Standard nicht für die von Pass-Through-Verbindungen abhängigen Datenobjekte zugelassen. Aktivieren Sie Datenobjekt-Cache mit Pass-Through-Sicherheit, müssen Sie überprüfen, dass Sie keinen unbefugten Benutzern Zugriff auf einige der Daten im Cache gewähren. Falls Sie Cache für Verbindungen mit Pass-Through-Sicherheit aktivieren, ist Datenobjekt-Cache für alle Verbindungen mit Pass-Through-Sicherheit aktiviert.

Pass-Through-Sicherheit hinzufügen

Aktivieren Sie Pass-Through-Sicherheit für eine Verbindung in die Verbindungseigenschaften. Aktivieren Sie Datenobjekt-Caching für Pass-Through-Sicherheitsverbindungen in den Pass-Through-Sicherheitseigenschaften des Data Integration Service.

1. Wählen Sie eine Verbindung aus.
2. Klicken Sie auf die Ansicht **Eigenschaften**.
3. Bearbeiten Sie die Verbindungseigenschaften.
Das Dialogfeld **Verbindungseigenschaften bearbeiten** wird angezeigt.
4. Um Pass-Through-Sicherheit für die Verbindung auszuwählen, wählen Sie die Option **Pass-Through-Sicherheit aktivieren** aus.
5. Wählen Sie optional den Data Integration Service aus, für den Sie Datenobjekt-Caching für Pass-Through-Sicherheit aktivieren möchten.
6. Klicken Sie auf die Ansicht **Eigenschaften**.
7. Bearbeiten Sie die Pass-Through-Sicherheitsoptionen.
Das Dialogfeld **Pass-Through-Sicherheitsoptionen bearbeiten** wird angezeigt.
8. Wählen Sie **Caching zulassen** aus, um Datenobjekt-Caching für den SQL-Datendienst oder Web-Dienst zuzulassen. Dies gilt für alle Verbindungen.
9. Klicken Sie auf **OK**.

Sie müssen den Data Integration Service recyceln, damit Sie die Verbindungen zwischenspeichern können.

Poolingeigenschaften in Verbindungsobjekten

Sie können Poolingeigenschaften von Verbindungen in der Ansicht **Pooling** für eine Datenbankverbindung bearbeiten.

Die Anzahl der Verbindungspool-Bibliotheken hängt von der Anzahl der laufenden Datenintegrationsdienstprozesse oder der DTM-Prozesse ab. Jeder Datenintegrationsdienstprozess oder DTM-Prozess verwaltet eine eigene Verbindungspool-Bibliothek. Die Werte der Poolingeigenschaften gelten für jede Verbindungspool-Bibliothek.

Wenn Sie beispielsweise die maximale Anzahl von Verbindungen auf 15 einstellen, kann jede Verbindungspoolbibliothek maximal 15 inaktive Verbindungen im Pool haben. Wenn vom Datenintegrationsdienst Jobs in separaten lokalen Prozessen ausgeführt werden und drei DTM-Prozesse laufen, können maximal 45 inaktive Verbindungsinstanzen vorliegen.

Um die Gesamtanzahl inaktiver Verbindungsinstanzen zu verringern, legen Sie die Mindestanzahl an Verbindungen auf 0 fest und verringern Sie die maximal erlaubte inaktive Zeit für jede Datenbankverbindung.

Die folgende Liste beschreibt die Poolingeigenschaften der Datenbankverbindung, die Sie in der Ansicht **Pooling** für Datenbankverbindungen bearbeiten können:

Verbindungspooling aktivieren

Aktiviert das Verbindungspooling. Wenn Sie das Verbindungspooling aktivieren, behält jeder Verbindungspool inaktive Verbindungsinstanzen im Speicher. Um inaktive Verbindungen in den Pools zu löschen, müssen Sie den Datenintegrationsdienst neu starten.

Wenn das Verbindungspooling deaktiviert ist, stoppt der DTM-Prozess oder der Datenintegrationsdienst alle Poolingaktivitäten. Der DTM-Prozess oder der Datenintegrationsdienstprozess erstellt bei jeder Verarbeitung eines Jobs eine Verbindungsinstanz. Er löscht die Instanz, wenn er die Verarbeitung der Jobs beendet.

Standardwert ist aktiviert für DB2 für i5/OS-, DB2 für z/OS-, IBM DB2-, Microsoft SQL Server-, Oracle- und ODBC-Verbindungen. Die Standardeinstellung ist für Adabas-, IMS-, sequenzielle und VSAM-Verbindungen deaktiviert.

Mindestanzahl an Verbindungen

Die Mindestanzahl inaktiver Verbindungsinstanzen, die ein Pool für eine Datenbankverbindung aufrechterhält, nachdem die maximal erlaubte inaktive Zeit erreicht ist. Setzen Sie diesen Wert maximal auf die maximale Anzahl inaktiver Verbindungsinstanzen. Standardwert ist 0.

Maximale Anzahl an Verbindungen

Die maximale Anzahl inaktiver Verbindungsinstanzen, die ein Pool für eine Datenbankverbindung aufrechterhält, bevor die maximale inaktive Zeit erreicht ist. Legen Sie diesen Wert auf eine höhere Anzahl als die Mindestanzahl an inaktiven Verbindungsinstanzen fest. Standardwert ist 15.

Maximale Leerlaufzeit

Die Anzahl der Sekunden, die eine Verbindungsinstanz, welche die Mindestanzahl von Verbindungsinstanzen überschritten hat, inaktiv bleiben kann, bevor sie vom Verbindungspool gelöscht wird. Der Verbindungspool ignoriert die inaktive Zeit, wenn die Verbindungsinstanz die Mindestanzahl von inaktiven Verbindungsinstanzen nicht überschreitet. Standardwert ist 120.

KAPITEL 9

Verbindungseigenschaften

Dieses Kapitel umfasst die folgenden Themen:

- [Verbindungseigenschaften – Übersicht, 129](#)
- [Adabas-Verbindungseigenschaften, 130](#)
- [Amazon Redshift-Verbindungseigenschaften, 132](#)
- [Amazon S3-Verbindungseigenschaften, 136](#)
- [Eigenschaften der Blockchain-Verbindung, 139](#)
- [Cassandra-Verbindungseigenschaften, 140](#)
- [Confluent-Kafka-Verbindung, 142](#)
- [Databricks-Verbindungseigenschaften, 145](#)
- [Greenplum-Verbindungseigenschaften, 147](#)
- [Google Analytics-Verbindungseigenschaften, 148](#)
- [Google BigQuery-Verbindungseigenschaften, 149](#)
- [Google Cloud Spanner-Verbindungseigenschaften, 152](#)
- [Google Cloud Storage-Verbindungseigenschaften, 152](#)
- [Google PubSub-Verbindungseigenschaften, 153](#)
- [Hadoop-Verbindungseigenschaften, 154](#)
- [HBase-Verbindungseigenschaften, 163](#)
- [HDFS- oder ViewFS-Verbindungseigenschaften, 163](#)
- [HBase-Verbindungseigenschaften für MapR-DB, 165](#)
- [Hive-Verbindungseigenschaften, 166](#)
- [HTTP-Verbindungseigenschaften, 170](#)
- [Eigenschaften von IBM DB2-Verbindungen, 172](#)
- [Eigenschaften von IBM DB2 for i5/OS-Verbindungen, 175](#)
- [Eigenschaften von IBM DB2 for z/OS-Verbindungen, 179](#)
- [IMS-Verbindungseigenschaften, 182](#)
- [Eigenschaften der JDBC-Verbindung, 185](#)
- [Eigenschaften der JDBC V2-Verbindung, 187](#)
- [Eigenschaften der JD Edwards EnterpriseOne-Verbindung, 190](#)
- [Kafka-Verbindungseigenschaften, 191](#)
- [Kudu-Verbindungseigenschaften, 194](#)
- [Eigenschaften der LDAP-Verbindung, 195](#)

- [Eigenschaften der Microsoft Azure Blob Storage-Verbindung, 196](#)
- [Microsoft Azure Cosmos DB SQL API-Verbindungseigenschaften, 198](#)
- [Eigenschaften der Microsoft Azure Data Lake Storage Gen1-Verbindung, 198](#)
- [Eigenschaften der Microsoft Azure Data Lake Storage Gen2-Verbindung, 200](#)
- [Eigenschaften der Microsoft Azure SQL Data Warehouse-Verbindung, 201](#)
- [MS SQL Server-Verbindungseigenschaften, 203](#)
- [Eigenschaften von Netezza-Verbindungen, 207](#)
- [Eigenschaften von OData-Verbindungen, 208](#)
- [ODBC-Verbindungseigenschaften, 209](#)
- [Eigenschaften für Oracle-Verbindungen, 211](#)
- [Salesforce-Verbindungseigenschaften, 214](#)
- [Eigenschaften der Salesforce Marketing Cloud-Verbindung, 215](#)
- [SAP-Verbindungseigenschaften, 217](#)
- [Eigenschaften sequenzieller Verbindungen, 219](#)
- [Snowflake-Verbindungseigenschaften, 222](#)
- [Verbindungseigenschaften des parallelen Teradata-Transporters, 223](#)
- [Tableau-Verbindungseigenschaften, 225](#)
- [Tableau V3-Verbindungseigenschaften, 226](#)
- [Streaming-Verbindungseigenschaften für Twitter, 228](#)
- [VSAM-Verbindungseigenschaften, 229](#)
- [Verbindungseigenschaften von Webdiensten, 231](#)
- [Bezeichnereigenschaften in Datenbankverbindungen, 233](#)

Verbindungseigenschaften – Übersicht

Mithilfe der Verbindungseigenschaften kann der Informatica-Client eine Verbindung mit den Datenquellen herstellen.

Dieses Kapitel enthält Verbindungseigenschaften für jede der Verbindungen, die Sie über Informatica-Clients erstellen und verwalten können.

Adabas-Verbindungseigenschaften

Verwenden Sie eine Adabas-Verbindung, um auf eine Adabas-Datenbank zuzugreifen. Die Adabas-Verbindung ist ein Mainframe-Datenbank-Verbindungstyp. Sie erstellen eine Adabas-Verbindung im Developer-Tool. Sie können eine Adabas-Verbindung im Administrator-Tool oder im Developer-Tool verwalten.

In der folgenden Tabelle werden die Eigenschaften von Adabas-Verbindungen erläutert:

Option	Beschreibung
Speicherort	Knotenname für den Speicherort des PowerExchange-Listenerdiensts, der eine Verbindung zu Adabas herstellt. Der Knotenname ist im ersten Parameter der NODE-Anweisung in der PowerExchange-Konfigurationsdatei „dbmover.cfg“ definiert.
Benutzername	Benutzername für die Datenbank Wenn Sie für eine Datenbank auf einem unterstützten Linux- oder UNIX-System die LDAP-Benutzer-Authentifizierung für PowerExchange aktiviert haben, ist der Benutzername der Benutzername des Unternehmens. Weitere Informationen finden Sie im <i>PowerExchange-Referenzhandbuch</i> .
Passwort	Passwort für den Datenbankbenutzernamen oder eine gültige PowerExchange-Passphrase. Eine PowerExchange-Passphrase kann 9 bis 128 Zeichen lang sein und die folgenden Zeichen enthalten: <ul style="list-style-type: none">- Groß- und Kleinbuchstaben- Die Zahlen 0 bis 9- Leerzeichen- Die folgenden Sonderzeichen: ' - ; # \ , . / ! % & * () _ + { } : @ < > ? Hinweis: Das erste Zeichen ist ein Apostroph. Passphrasen dürfen keine einfachen Anführungszeichen ('), doppelten Anführungszeichen (") oder Währungssymbole enthalten. Stellen Sie vor der Verwendung von Passphrasen sicher, dass der PowerExchange-Listenerdienst im DBMOVER-Mitglied mit der Sicherheitseinstellung SECURITY=(1,N) oder höher ausgeführt wird. Weitere Informationen finden Sie unter „SECURITY-Anweisung“ im <i>PowerExchange-Referenzhandbuch</i> . Die zulässigen Zeichen beim Beenden von IBM IRRPHREX haben keine Auswirkungen auf die zulässigen Zeichen in PowerExchange-Passphrasen. Hinweis: Eine gültige RACF-Passphrase kann bis zu 100 Zeichen enthalten. PowerExchange schneidet Passphrases mit mehr als 100 Zeichen ab, wenn diese zur Validierung an RACF übergeben werden.
Codepage	Erforderlich. Name der Codepage für das Lesen aus oder Schreiben in die Datenquelle. Normalerweise ist dieser Wert ein ISO-Codepage-Name, z. B. ISO-8859-6.
Pass-Through-Sicherheit aktiviert	Aktiviert Pass-Through-Sicherheit für die Verbindung. Wenn Sie Pass-Through-Sicherheit für eine Verbindung aktivieren, verwendet die Domäne nicht die im Verbindungsobjekt definierten Anmeldeinformationen, sondern den Benutzernamen und das Passwort des Clients, um sich an der entsprechenden Datenbank anzumelden.

Option	Beschreibung
Verschlüsselungstyp	<p>Der Verschlüsselungstyp, den der Datenintegrationsdienst verwendet. Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> - Keine - AES <p>Standardwert ist „Keine“.</p> <p>Hinweis: Informatica empfiehlt die Verwendung von SSL-Authentifizierung (Secure Sockets Layer) statt der Konfiguration der Verbindungseigenschaften Verschlüsselungstyp und Ebene. SSL-Authentifizierung bietet striktere Sicherheit und wird von verschiedenen Informatica-Produkten verwendet.</p> <p>Weitere Informationen zum Implementieren von SSL-Authentifizierung in einem PowerExchange-Netzwerk finden Sie im <i>PowerExchange-Referenzhandbuch</i>.</p>
[Encryption]-Ebene	<p>Bei Verwendung von AES für Verschlüsselungstyp wählen Sie eine der folgenden Optionen aus, um die vom Datenintegrationsdienst verwendete Verschlüsselungsebene anzugeben:</p> <ul style="list-style-type: none"> - 1. Verwenden Sie einen 128-Bit-Verschlüsselungsschlüssel. - 2. Verwenden Sie einen 192-Bit-Verschlüsselungsschlüssel. - 3. Verwenden Sie einen 256-Bit-Verschlüsselungsschlüssel. <p>Wenn Sie als Verschlüsselungstyp nicht AES auswählen, wird diese Option ignoriert.</p> <p>Standard ist 1.</p>
Pacing-Größe	<p>Optional. Menge der Daten, die das Quellsystem an den PowerExchange-Listenerdienst übergeben kann. Legen Sie die Pacing-Größe fest, wenn eine externe Anwendung, eine Datenbank oder der Knoten mit dem Datenintegrationsdienst einen Engpass darstellt. Verwenden Sie niedrigere Werte für schnellere Leistung.</p> <p>Der Mindest- und Standardwert ist 0. Mit dem Wert 0 wird die beste Leistung erzielt.</p>
Als Zeilen interpretieren	<p>Optional. Wählen Sie diese Option, um die Pacing-Größe als Anzahl von Zeilen anzugeben. Löschen Sie diese Option, um die Pacing-Größe in Kilobyte anzugeben. Diese Option ist standardmäßig nicht ausgewählt und die Pacing-Größe wird in Kilobyte angegeben.</p>
Komprimierung	<p>Optional. Wählen Sie diese Option zum Aktivieren der Quelldatenkomprimierung aus. Durch die Komprimierung von Daten können Sie die Menge der Daten verringern, die Informatica-Anwendungen über das Netzwerk senden. Standardmäßig ist diese Option nicht ausgewählt und die Komprimierung ist deaktiviert.</p>
Offload-Verarbeitung	<p>Optional. Steuert, ob für die Verarbeitung von Stapeldaten vom Quellcomputer zum Datenintegrationsdienst-Computer Offload-Verarbeitung verwendet werden soll. Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> - AUTO. Der Datenintegrationsdienst bestimmt, ob Offload-Verarbeitung verwendet werden soll. - Ja. Offload-Verarbeitung wird verwendet. - Nein. Offload-Verarbeitung wird nicht verwendet. <p>Der Standardwert ist AUTO.</p>
Worker-Threads	<p>Optional. Anzahl der vom Datenintegrationsdienst verwendeten Threads, um Stapeldaten bei aktivierter Offload-Verarbeitung zu verarbeiten. Um eine optimale Leistung zu erzielen, sollte dieser Wert die Anzahl der verfügbaren Prozessoren auf dem Rechner des Datenintegrationsdienstes nicht überschreiten. Gültige Werte sind 1 bis 64. Der Standardwert ist 0, der Multithreading deaktiviert.</p>

Option	Beschreibung
Array-Größe	Optional. Die Anzahl der Datensätze im Speicher-Array für die Worker-Threads. Diese Option kann verwendet werden, wenn Sie die Option Worker-Threads auf einen Wert größer als 0 festlegen. Gültige Werte sind 1 bis 5000. Standardwert ist 25.
Schreibmodus	<p>Optional. Modus, in dem der Datenintegrationsdienst Daten an den PowerExchange-Listenerdienst sendet. Wählen Sie einen der folgenden Schreibmodi aus:</p> <ul style="list-style-type: none"> - CONFIRMWRITEON. Sendet Daten an den PowerExchange-Listenerdienst und wartet auf eine Antwort, bevor weitere Daten gesendet werden. Wählen Sie diese Option aus, wenn die Fehlerbehebung Priorität hat. Diese Option kann sich jedoch negativ auf die Leistung auswirken. - CONFIRMWRITEOFF. Sendet Daten an den PowerExchange-Listenerdienst, ohne auf eine Antwort zu warten. Verwenden Sie diese Option, wenn Sie die Zieltabelle im Fall eines Fehlers erneut laden können. - ASYNCHRONOUSWITHFAULTTOLERANCE. Sendet Daten an den PowerExchange-Listenerdienst, ohne auf eine Antwort zu warten. Diese Option aktiviert außerdem die Fehlererkennung. Diese Option kombiniert die Geschwindigkeit von CONFIRMWRITEOFF und die Datenintegrität von CONFIRMWRITEON. <p>Der Standardwert ist CONFIRMWRITEON.</p>

Amazon Redshift-Verbindungseigenschaften

Wenn Sie eine Amazon Redshift-Verbindung einrichten, müssen Sie die Verbindungseigenschaften konfigurieren.

In der folgenden Tabelle werden die Amazon Redshift-Verbindungseigenschaften beschrieben:

Eigenschaft	Beschreibung
Name	Der Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung ändern. Der Name darf maximal 128 Zeichen umfassen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * () - + = { [] \ ; " ' < , > . ? /
ID	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 4.000 Zeichen enthalten.
Speicherort	Die Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Der Verbindungstyp. Wählen Sie Amazon Redshift in der Datenbank aus.

Die Registerkarte **Details** enthält die Verbindungsattribute der Amazon Redshift-Verbindung. In der folgenden Tabelle werden die Verbindungsattribute beschrieben:

Eigenschaft	Beschreibung
Authentifizierungstyp	Die Authentifizierungsmethode zum Anmelden bei Amazon Redshift. Sie können eine der folgenden Authentifizierungsmethoden auswählen: <ul style="list-style-type: none"> - Standard. Verwendet den Benutzernamen und das Passwort, um eine Verbindung zu Amazon Redshift herzustellen. - Redshift-IAM-Authentifizierung über AssumeRole. Verwendet AssumeRole für die IAM-Authentifizierung, um eine Verbindung zu Amazon Redshift herzustellen.
Benutzername	Benutzername des Amazon Redshift-Kontos.
Passwort	Passwort für das Amazon Redshift-Konto.
Zugriffsschlüssel-ID	ID des Amazon S3-Bucket-Zugriffsschlüssels zum Zwischenspeichern von Daten im S3-Bucket mithilfe von Befehlen zum Entladen und Kopieren.
Geheimer Zugriffsschlüssel	ID des geheimen Amazon S3-Bucket-Zugriffsschlüssels zum Zwischenspeichern der Daten im S3-Bucket.
Symmetrischer Hauptschlüssel	Optional. Stellen Sie einen 256-Bit-AES-Verschlüsselungsschlüssel im Base64-Format bereit, wenn Sie die clientseitige Verschlüsselung aktivieren. Sie können einen Schlüssel mit einem Drittanbieter-Tool generieren. Wenn Sie einen Wert angeben, stellen Sie sicher, dass Sie den Verschlüsselungstyp in den erweiterten Zieleigenschaften als clientseitige Verschlüsselung angeben.
JDBC-URL	Verbindungs-URL für Amazon Redshift.

Eigenschaft	Beschreibung
Clusterregion	<p>Optional. Die AWS-Clusterregion, in der sich der Bucket befindet, auf den Sie zugreifen möchten.</p> <p>Wählen Sie eine Clusterregion aus, wenn Sie eine benutzerdefinierte JDBC-URL bereitstellen möchten, die keinen Clusterregionsnamen in der Verbindungseigenschaft JDBC-URL enthält.</p> <p>Wenn Sie eine Clusterregion in den Verbindungseigenschaften Clusterregion und JDBC-URL angeben, ignoriert der Datenintegrationsdienst die Clusterregion, die Sie in der Verbindungseigenschaft JDBC-URL festgelegt haben.</p> <p>Zur Verwendung des Clusterregionsnamens, den Sie in der Verbindungseigenschaft JDBC-URL angegeben haben, wählen Sie Keine als Clusterregion in dieser Eigenschaft aus.</p> <p>Wählen Sie eine der folgenden Clusterregionen aus:</p> <ul style="list-style-type: none"> - Asien-Pazifik (Mumbai) - Asien-Pazifik (Seoul) - Asien-Pazifik (Singapur) - Asien-Pazifik (Sydney) - Asien-Pazifik (Tokio) - AWS GovCloud (USA) - Kanada (Zentral) - China (Peking) - China (Ningxia) - EU (Irland) - EU (Frankfurt) - EU (London) - EU (Paris) - Südamerika (São Paulo) - USA, Osten (Ohio) - USA, Osten (Northern Virginia) - USA, Westen (Nordkalifornien) - USA, Westen (Oregon) <p>Standardwert ist „Kein“.</p> <p>Daten können nur in die Clusterregionen geschrieben oder aus den Clusterregionen gelesen werden, die von dem AWS-SDK unterstützt werden, das von PowerExchange for Amazon Redshift verwendet wird.</p>
Kunden-Master-Schlüssel-ID	<p>Optional. Geben Sie die ID des Kunden-Master-Schlüssels an, der von AWS Key Management Service (AWS KMS) oder dem Amazon Resource Name (ARN) Ihres benutzerdefinierten Schlüssels für kontoübergreifenden Zugriff verwendet wird. Sie müssen den Kunden-Master-Schlüssel entsprechend der Region erzeugen, in der sich das Amazon S3-Bucket befindet. Sie können einen der folgenden Werte angeben:</p> <p>Vom Kunden erzeugter Kunden-Master-Schlüssel</p> <p>Aktiviert client- oder serverseitige Verschlüsselung.</p> <p>Standardmäßiger Kunden-Master-Schlüssel</p> <p>Aktiviert client- oder serverseitige Verschlüsselung. Nur der Administratorbenutzer des Kontos kann die standardmäßige Kunden-Master-Schlüssel-ID verwenden, um clientseitige Verschlüsselung zu aktivieren.</p>
ARN der IAM-Rollenübernahme	<p>Die Amazon Resource Number bzw. der Amazon Resource Name (ARN) der IAM-Rolle, die der Benutzer annimmt, um die dynamisch generierten temporären Sicherheitsanmeldedaten zu verwenden.</p> <p>Legen Sie den Wert dieser Eigenschaft fest, wenn Sie die temporären Sicherheitsanmeldedaten für den Zugriff auf Amazon Redshift verwenden möchten.</p> <p>Weitere Informationen darüber, wie Sie den ARN der IAM-Rolle erhalten, finden Sie in der AWS-Dokumentation.</p>

Eigenschaft	Beschreibung
Clusterbezeichner	Die eindeutige ID des Clusters, der Amazon Redshift hostet, für das Sie die Sicherheitsanmeldedaten anfordern. Geben Sie den Clusternamen an.
Datenbankname	Name der Amazon Redshift-Datenbank.
Datenbankbenutzer automatisch erstellen	Wählen Sie diese Option aus, um zur Laufzeit einen neuen Amazon Redshift-Datenbankbenutzer zu erstellen. Standardwert ist „Deaktiviert“. Hinweis: Verwenden Sie diese Option, um einen neuen Amazon Redshift-Datenbankbenutzer zu erstellen. Wenn Sie einen neuen Benutzer direkt über die AWS-Befehlszeile erstellen, wird er nicht in Amazon Redshift erstellt.
Datenbankgruppe	Name der Datenbankgruppe. Nachdem Sie sich bei der Amazon Redshift-Datenbank angemeldet haben, geben Sie die Datenbankbenutzer- und Gruppendetails an. Hinweis: Wenn Sie keine Gruppe angeben, wird der Benutzer einer öffentlichen Gruppe hinzugefügt.
Ablaufzeit	Die Zeitdauer, in der das Passwort für den Amazon Redshift-Datenbankbenutzer abläuft. Geben Sie einen Wert zwischen 900 und 3.600 Sekunden an. Standardwert ist 900.
EC2-Rolle zum Übernehmen der Rolle verwenden	Wählen Sie diese Option aus, damit die EC2-Rolle eine andere IAM-Rolle übernehmen kann, die in der Option „ARN der IAM-Rollenübernahme“ angegeben ist.
IAM-Benutzerzugriffsschlüssel	Der Zugriffsschlüssel des IAM-Benutzers, der berechtigt ist, den ARN der IAM-Rollenübernahme zu übernehmen.
Geheimer IAM-Benutzerzugriffsschlüssel	Der geheime Zugriffsschlüssel des IAM-Benutzers, der berechtigt ist, den ARN der IAM-Rollenübernahme zu übernehmen.

Amazon S3-Verbindungseigenschaften

Wenn Sie eine Amazon S3-Verbindung einrichten, müssen Sie die Verbindungseigenschaften konfigurieren.

In der folgenden Tabelle werden die Amazon S3-Verbindungseigenschaften beschrieben:

Eigenschaft	Beschreibung
Name	Der Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung ändern. Der Name darf maximal 128 Zeichen umfassen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * () - + = { [] } \ ; , > . ? /
ID	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Optional. Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 4.000 Zeichen enthalten.
Speicherort	Die Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Der Amazon S3-Verbindungstyp.
Zugriffsschlüssel	<p>Zugriffsschlüssel für den Zugriff auf den Amazon S3-Bucket. Stellen Sie den Wert des Zugriffsschlüssels anhand der folgenden Authentifizierungsmethoden bereit:</p> <ul style="list-style-type: none">- Standardauthentifizierung: Bereitstellung des tatsächlichen Zugriffsschlüsselwerts.- IAM-Authentifizierung: Keine Bereitstellung des Zugriffsschlüsselwerts.- Temporäre Sicherheitsanmeldedaten mittels der übernommenen Rolle: Bereitstellung des Zugriffsschlüssels eines IAM-Benutzers ohne Berechtigung zum Zugriff auf den Amazon S3-Bucket.
Geheimer Schlüssel	<p>Geheimer Schlüssel für den Zugriff auf den Amazon S3-Bucket.</p> <p>Der geheime Schlüssel ist mit dem Zugriffsschlüssel verknüpft und identifiziert das Konto eindeutig. Stellen Sie den Wert des Zugriffsschlüssels anhand der folgenden Authentifizierungsmethoden bereit:</p> <ul style="list-style-type: none">- Standardauthentifizierung: Bereitstellung des tatsächlichen Werts des Zugriffsgeheimworts.- IAM-Authentifizierung: Keine Bereitstellung des Werts des Zugriffsgeheimworts.- Temporäre Sicherheitsanmeldedaten mittels der übernommenen Rolle: Bereitstellung des Zugriffsgeheimworts eines IAM-Benutzers ohne Berechtigung zum Zugriff auf den Amazon S3-Bucket.
ARN der IAM-Rolle	<p>Der ARN der IAM-Rolle, die der Benutzer annimmt, um die dynamisch generierten temporären Sicherheitsanmeldedaten zu verwenden.</p> <p>Geben Sie den Wert dieser Eigenschaft ein, wenn Sie die temporären Sicherheitsanmeldedaten für den Zugriff auf die AWS-Ressourcen verwenden möchten.</p> <p>Wenn Sie die temporären Sicherheitsanmeldedaten mit IAM-Authentifizierung verwenden möchten, geben Sie die Verbindungseigenschaften „Zugriffsschlüssel“ und „Geheimer Schlüssel“ nicht an. Wenn Sie die temporären Sicherheitsanmeldedaten ohne IAM-Authentifizierung verwenden möchten, müssen Sie den Wert der Verbindungseigenschaften „Zugriffsschlüssel“ und „Geheimer Schlüssel“ eingeben.</p> <p>Weitere Informationen darüber, wie Sie den ARN der IAM-Rolle erhalten, finden Sie in der AWS-Dokumentation.</p>

Eigenschaft	Beschreibung
Ordnerpfad	<p>Der vollständige Pfad zu Amazon S3-Objekten. Der Pfad muss den Namen des Buckets und etwaige Ordnernamen einschließen.</p> <p>Verwenden Sie keinen Schrägstrich am Ende des Ordnerpfads. Beispiel: <Bucket-Name>/<Ordnername>.</p>
Symmetrischer Hauptschlüssel	<p>Optional. Stellen Sie einen 256-Bit-AES-Verschlüsselungsschlüssel im Base64-Format bereit, wenn Sie die clientseitige Verschlüsselung aktivieren. Sie können mit einem Drittanbieter-Tool einen symmetrischen Hauptschlüssel generieren.</p>
S3-Kontotyp	<p>Der Typ des Amazon S3-Kontos.</p> <p>Wählen Sie Amazon S3-Speicher oder S3-kompatibler Speicher aus.</p> <p>Wählen Sie die Amazon S3-Speicheroption aus, um die Amazon S3-Dienste zu nutzen. Wählen Sie die S3-kompatible Speicheroption aus, um den Endpunkt für einen externen Speicheranbieter wie Scality RING anzugeben.</p> <p>Standardmäßig ist Amazon S3-Speicher ausgewählt.</p>
REST-Endpunkt	<p>Der S3-Speicherendpunkt.</p> <p>Geben Sie den S3-Speicherendpunkt im HTTP/HTTPS-Format an, wenn Sie die Option für den S3-kompatiblen Speicher auswählen. Beispiel: http://s3.isv.scality.com.</p>
Name der Region	<p>Wählen Sie die AWS-Region, in der sich der Bucket befindet, auf den Sie zugreifen möchten.</p> <p>Wählen Sie eine der folgenden Regionen aus:</p> <ul style="list-style-type: none"> - Asien-Pazifik (Mumbai) - Asien-Pazifik (Seoul) - Asien-Pazifik (Singapur) - Asien-Pazifik (Sydney) - Asien-Pazifik (Tokio) - AWS GovCloud (USA) - AWS GovCloud (östliche USA) - Kanada (Zentral) - China (Peking) - China (Hongkong) - China (Ningxia) - EU (Irland) - EU (Frankfurt) - EU (London) - EU (Paris) - EU (Stockholm) - Naher Osten (Bahrain) - Südamerika (São Paulo) - USA, Osten (Ohio) - USA, Osten (Northern Virginia) - USA, Westen (Nordkalifornien) - USA, Westen (Oregon) <p>Der Standardwert ist Östliche USA (N. Virginia).</p> <p>Gilt nicht für S3-kompatiblen Speicher.</p>

Eigenschaft	Beschreibung
Kunden-Master-Schlüssel-ID	<p>Optional. Geben Sie die ID des Kunden-Master-Schlüssels oder den Aliasnamen an, der von AWS Key Management Service (AWS KMS) oder dem Amazon Resource Name (ARN) Ihres benutzerdefinierten Schlüssels für kontoübergreifenden Zugriff verwendet wird. Sie müssen den Kunden-Master-Schlüssel für dieselbe Region erzeugen, in der sich das Amazon S3-Bucket befindet.</p> <p>Sie können einen der folgenden Werte angeben:</p> <p>Vom Kunden erzeugter Kunden-Master-Schlüssel</p> <p>Aktiviert client- oder serverseitige Verschlüsselung.</p> <p>Standardmäßiger Kunden-Master-Schlüssel</p> <p>Aktiviert client- oder serverseitige Verschlüsselung. Nur der Administratorbenutzer des Kontos kann die standardmäßige Kunden-Master-Schlüssel-ID verwenden, um clientseitige Verschlüsselung zu aktivieren.</p>
Verbund-SSO-IdP	<p>SAML 2.0-fähiger Identitätsanbieter für ein Single Sign-On von föderierten Benutzern zur Verwendung mit dem AWS-Konto.</p> <p>PowerExchange for Amazon S3 unterstützt nur den Identitätsanbieter ADFS 3.0.</p> <p>Wählen Sie <i>Kein</i>, wenn Sie kein Single Sign-On für föderierte Benutzer verwenden möchten.</p>

Verbindungseigenschaften für Single Sign-On für föderierte Benutzer

Konfigurieren Sie die folgenden Eigenschaften, wenn Sie ADFS 3.0 in **Föderierter SSO-IdP** auswählen:

Eigenschaft	Beschreibung
Name des föderierten Benutzers	Benutzername des föderierten Benutzers für den Zugriff auf das AWS-Konto über den Identitätsanbieter.
Passwort des föderierten Benutzers	Passwort des föderierten Benutzers für den Zugriff auf das AWS-Konto über den Identitätsanbieter.
IdP-SSO-URL	Single Sign-On-URL des Identitätsanbieters für AWS.
SAML-Identitätsanbieter-ARN	ARN des SAML-Identitätsanbieters, die der AWS-Administrator erstellt hat, um den Identitätsanbieter als vertrauenswürdigen Anbieter zu registrieren.
Rollen-ARN	ARN der vom föderierten Benutzer angenommenen IAM-Rolle.

Eigenschaften der Blockchain-Verbindung

Wenn Sie eine Blockchain-Verbindung einrichten, müssen Sie die Verbindungseigenschaften konfigurieren.

In der folgenden Tabelle werden die allgemeinen Verbindungseigenschaften für eine Blockchain-Verbindung beschrieben:

Eigenschaft	Beschreibung
Name	Der Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung ändern. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
ID	Die Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Die Beschreibung der Verbindung. Geben Sie eine Zeichenfolge ein, mit der Sie die Verbindung angeben können. Die Beschreibung darf nicht mehr als 4.000 Zeichen enthalten.
Swagger-Dateipfad	Der absolute Pfad des Swagger-Dateipfades, der die REST-API für die Kommunikation mit der Blockchain enthält. Die Swagger-Datei muss eine JSON-Datei sein, die auf dem Computer mit dem Datenintegrationsdienst gespeichert ist. Falls die Swagger-Datei in einem anderen Dateiformat wie beispielsweise YAML vorliegt, konvertieren Sie die Daten in das JSON-Format.
Basis-URL	Erforderlich. Die Basis-URL, die für den Zugriff auf Objekte in der Blockchain verwendet wird.
Authentifizierungstyp*	Authentifizierungsmethode, mit der sich die Laufzeit-Engine mit dem REST-Server verbindet. Sie können „none“, „basic“, „digest“ oder „OAuth“ verwenden.
Authentifizierungsbenutzer-ID*	Benutzername zur Authentifizierung beim REST-Server.
Authentifizierungspasswort*	Passwort für den Benutzernamen zur Authentifizierung beim REST-Server.
OAuth-Verbraucherschlüssel*	Für den OAuth-Authentifizierungstyp erforderlich. Clientschlüssel, der dem REST-Server zugeordnet ist.
OAuth-Verbrauchergeheimwort*	Für den OAuth-Authentifizierungstyp erforderlich. Clientpasswort für die Verbindung zum REST-Server.
OAuth-Token*	Für den OAuth-Authentifizierungstyp erforderlich. Zugriffstoken für die Verbindung zum REST-Server.
OAuth-Token-Geheimwort*	Für den OAuth-Authentifizierungstyp erforderlich. Passwort, das dem OAuth-Token zugeordnet ist.
Proxy-Typ*	Typ des Proxy. Sie können „no proxy“, „platform proxy“ oder „custom“ verwenden.
Proxy-Details*	Proxy-Konfiguration mit dem Format <host>:<port>.

Eigenschaft	Beschreibung
TrustStore-Dateipfad*	Der absolute Pfad für die Truststore-Datei, die das SSL-Zertifikat enthält.
TrustStore-Passwort*	Passwort für die TrustStore-Datei
Schlüsselspeicher-Dateipfad*	Der absolute Pfad der Schlüsselspeicherdatei, die die Schlüssel und Zertifikate enthält, die zum Herstellen einer sicheren Zwei-Wege-Verbindung mit dem REST-Server benötigt werden.
Schlüsselspeicherpasswort*	Passwort für die Schlüsselspeicherdatei
Erweiterte Eigenschaften	<p>Liste der erweiterten Eigenschaften für den Zugriff auf ein Objekt in der Blockchain. Geben Sie die erweiterten Eigenschaften anhand von Name/Wert-Paaren an, die durch ein Semikolon getrennt sind.</p> <p>Sie können die folgenden erweiterten Eigenschaften verwenden:</p> <ul style="list-style-type: none"> - BaseUrl. Erforderlich, wenn die Swagger-Datei nicht die Basis-URL enthält. Die Basis-URL, die für den Zugriff auf Objekte in der Blockchain verwendet wird. - X-API-KEY. Erforderlich, wenn Sie sich mithilfe eines API-Schlüssels beim REST-Server authentifizieren. <p>Die erweiterten Eigenschaften, die Sie in der Verbindung konfigurieren, überschreiben die Werte für die entsprechenden erweiterten Eigenschaften im Blockchain-Datenobjekt. Wenn beispielsweise sowohl die Verbindung als auch das Datenobjekt beide eine Basis-URL, überschreibt der Wert in der Verbindung den Wert im Datenobjekt.</p> <p>Hinweis: Die erweiterten Eigenschaften verfügen über die Vorrangstufe Betriebsebene > Objektebene > Verbindungsebene. Die auf der Betriebsebene konfigurierten Eigenschaften überschreiben die auf Objekt- oder Verbindungsebene konfigurierten Eigenschaften.</p>
Cookies	<p>Erforderlich, je nachdem, wie die REST-API implementiert ist. Liste der Cookie-Eigenschaften, um die Cookie-Informationen anzugeben, die an den REST-Server übergeben werden. Geben Sie die Eigenschaften anhand von Name/Wert-Paaren an, die durch ein Semikolon getrennt sind.</p> <p>Die Cookie-Eigenschaften, die Sie in der Verbindung konfigurieren, überschreiben die Werte für die entsprechenden Cookie-Eigenschaften im Blockchain-Datenobjekt.</p>
<p>* Die Eigenschaft wird ignoriert. Um die Funktionalität zu nutzen, konfigurieren Sie die Eigenschaft als erweiterte Eigenschaft und stellen Sie ein Name/Wert-Paar bereit, das auf dem Eigenschaftsnamen in der Swagger-Datei basiert. Konfigurieren Sie z. B. das folgende Name/Wert-Paar zur Verwendung der grundlegenden Autorisierung:</p> <pre>Authorization=Basic <credentials></pre> <p>Hinweis: Sie können die Testverbindung nicht verwenden, um eine Blockchain-Verbindung zu validieren.</p>	

Cassandra-Verbindungseigenschaften

Wenn Sie eine Cassandra-Verbindung einrichten, müssen Sie die Verbindungseigenschaften konfigurieren.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Cassandra-Verbindungseigenschaften beschrieben:

Eigenschaft	Beschreibung
Name	Der Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung ändern. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
ID	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Die ID darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Optional. Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 4.000 Zeichen enthalten.
Speicherort	Die Domäne, in der Sie die Verbindung erstellen möchten. Gilt nicht für Data Engineering Streaming.
Typ	Der Verbindungstyp. Wählen Sie Cassandra .
Hostname	Hostname oder IP-Adresse des Cassandra-Servers.
Port	Portnummer des Cassandra-Servers. Der Standardwert ist 9042.
Benutzername	Benutzername für den Zugriff auf den Cassandra-Server.
Passwort	Das zu dem Benutzernamen gehörende Passwort für den Zugriff auf den Cassandra-Server.
Standardschlüsselraum	Name des Cassandra-Schlüsselraums, der standardmäßig verwendet werden soll.
SQL-Kennungszeichen	Typ des Zeichens, mit dem die Datenbank begrenzte Bezeichner in SQL- oder CQL-Abfragen einschließt. Die verfügbaren Zeichen richten sich nach dem Datenbanktyp. Wählen Sie Keine , wenn die Datenbank reguläre Bezeichner verwendet. Wenn der Datenintegrationsdienst SQL- oder CQL-Abfragen generiert, platziert der Dienst keine Begrenzungszeichen um die Bezeichner. Wählen Sie ein Zeichen aus, wenn die Datenbank begrenzte Bezeichner verwendet. Wenn der Datenintegrationsdienst SQL- oder CQL-Abfragen generiert, umschließt der Dienst die Bezeichner mit diesen Zeichen.
SSL-Modus	Wählen Sie Deaktiviert . Nicht anwendbar auf PowerExchange for Cassandra JDBC. SSL-Modus, der den für die Verbindung zu verwendenden Verschlüsselungstyp angibt. Sie können einen Modus aus den folgenden SSL-Modi auswählen: <ul style="list-style-type: none"> - Deaktiviert - Unidirektional - Bidirektional

Eigenschaft	Beschreibung
SSL-TrustStore-Pfad	Gilt nicht für PowerExchange for Cassandra JDBC oder wenn der SSL-Modus Deaktiviert ausgewählt ist. Absoluter Pfad und Dateiname der SSL-Truststore-Datei, die Zertifikate des vertrauenswürdigen SSL-Servers enthält.
SSL-Truststore-Passwort	Gilt nicht für PowerExchange for Cassandra JDBC oder wenn der SSL-Modus Deaktiviert ausgewählt ist. Passwort für den SSL-Truststore.
SSL-Schlüsselspeicherpfad	Gilt nicht für PowerExchange for Cassandra JDBC oder wenn der SSL-Modus Deaktiviert ausgewählt ist. Absoluter Pfad und Dateiname der SSL-Schlüsselspeicherdatei, die private Schlüssel und Zertifikate für den SSL-Server enthält.
SSL-Schlüsselspeicherpasswort	Gilt nicht für PowerExchange for Cassandra JDBC oder wenn der SSL-Modus Deaktiviert ausgewählt ist. Passwort für den SSL-Schlüsselspeicher.
Zusätzliche Verbindungseigenschaften	Geben Sie einen oder mehrere JDBC-Verbindungsparameter in folgendem Format ein: <code><Param1>=<Wert>;<Param2>=<Wert>;<Param3>=<Wert></code> PowerExchange for Cassandra JDBC unterstützt die folgenden JDBC-Verbindungsparameter: <ul style="list-style-type: none"> - BinaryColumnLength - DecimalColumnScale - EnableCaseSensitive - EnableNullInsert - EnablePaging - RowsPerPage - StringColumnLength - VTTableNameSeparator

Confluent-Kafka-Verbindung

Bei der Confluent-Kafka-Verbindung handelt es sich um eine Messaging-Verbindung. Verwenden Sie die Confluent-Kafka-Verbindung, um auf einen Kafka-Broker oder einen Confluent-Kafka-Broker als Quelle oder Ziel zuzugreifen. Sie können eine Confluent-Kafka-Verbindung im Developer Tool oder durch `infacmd` erstellen und verwalten.

Wenn Sie eine Confluent-Kafka-Verbindung konfigurieren, konfigurieren Sie die folgenden Eigenschaften:

- Liste der Kafka-Broker oder Confluent-Kafka-Broker, von denen die Verbindung liest oder an die sie schreibt.
- Anzahl der Sekunden, die der Integrationsdienst versucht, eine erneute Verbindung zu der Datenbank herzustellen, wenn die Verbindung fehlschlägt.
- Die Version des Confluent-Kafka-Messaging-Brokers.

Allgemeine Eigenschaften

In der folgenden Tabelle werden die allgemeinen Verbindungseigenschaften für die Confluent-Kafka-Verbindung beschrieben:

Eigenschaft	Beschreibung
Name	Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung ändern. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * () - + = { [] \ : ; " ' < , > . ? /
ID	Die Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Beschreibung der Verbindung. Geben Sie eine Zeichenfolge ein, mit der Sie die Verbindung angeben können. Die Beschreibung darf nicht mehr als 4.000 Zeichen enthalten.
Speicherort	Die Domäne, in der Sie die Verbindung erstellen möchten. Wählen Sie den Domänennamen aus.
Typ	Verbindungstyp. Wählen Sie <code>Messaging/ConfluentKafka</code> aus.

Eigenschaften des Confluent-Kafka-Brokers

In der folgenden Tabelle werden die Kafka-Broker-Eigenschaften für die Confluent-Kafka-Verbindung beschrieben:

Eigenschaft	Beschreibung
Liste der Kafka Broker	Durch Kommas getrennte Liste der Confluent-Kafka-Broker, die die Konfiguration des Confluent-Kafka-Messaging-Brokers beibehalten. Verwenden Sie das folgende Format, um einen Confluent-Kafka-Broker anzugeben: <code><IP-Adresse>:<Port></code>
Timeout der Wiederholungen	Anzahl der Sekunden, nach denen der Datenintegrationsdienst versucht, erneut eine Verbindung zum Confluent-Kafka-Broker herzustellen, um Daten zu lesen oder zu schreiben. Ist die Quelle oder das Ziel für den angegebenen Zeitraum nicht verfügbar, wird die Zuordnungsausführung zur Vermeidung von Datenverlusten angehalten.
Kafka-Broker-Version	Die Version des Confluent-Kafka-Messaging-Brokers.
Zusätzliche Verbindungseigenschaften	Optional. Durch Kommas getrennte Liste der Verbindungseigenschaften, um eine Verbindung zum Kafka-Broker herzustellen.
URL der Schemaregistrierung	Speicherort und Port des Schemaregistrierungsanbieters, über den eine Verbindung hergestellt werden soll.

Zusätzliche Verbindungseigenschaften

Sie können die folgende Syntax verwenden, um die zusätzlichen Verbindungseigenschaften anzugeben:

```
request.timeout.ms=<value>,session.timeout.ms=<value>,  
fetch.max.wait.ms=<value>,heartbeat.interval.ms=<value>,  
security.protocol=SASL_PLAINTEXT,sasl.kerberos.  
service.name=<kerberos name>,sasl.mechanism=GSSAPI,  
sasl.jaas.config=com.sun.security.auth.module.  
Krb5Login Modulrequired useKeyTab=true  
doNotPrompt=true storeKey=true client=true  
keyTab="<Keytab Location>" principal="<principal>";
```

SSL-Eigenschaften

In der folgenden Tabelle werden die SSL-Eigenschaften für die Confluent-Kafka-Verbindung beschrieben:

Eigenschaft	Beschreibung
SSL-Modus	Optional. SSL-Modus, der den für die Verbindung zu verwendenden Verschlüsselungstyp angibt. Sie können einen der folgenden SSL-Modi wählen: <ul style="list-style-type: none">- Deaktiviert- Unidirektional- Bidirektional Der Standardwert ist <code>Deaktiviert</code> .
SSL-TrustStore-Dateipfad	Erforderlich, wenn der SSL-Modus <code>Unidirektional</code> ausgewählt ist. Absoluter Pfad und Dateiname der SSL-Truststore-Datei, die Zertifikate des vertrauenswürdigen SSL-Servers enthält.
SSL-Truststore-Passwort	Erforderlich, wenn der SSL-Modus <code>Unidirektional</code> ausgewählt ist. Passwort für den SSL-Truststore.
SSL-KeyStore-Dateipfad	Erforderlich, wenn der SSL-Modus <code>Bidirektional</code> ausgewählt ist. Absoluter Pfad und Dateiname der SSL-Schlüsselspeicherdatei, die private Schlüssel und Zertifikate für den SSL-Server enthält.
SSL-Schlüsselspeicherpasswort	Erforderlich, wenn der SSL-Modus <code>Bidirektional</code> ausgewählt ist. Passwort für den SSL-Schlüsselspeicher.
Zusätzliche Sicherheitseigenschaften	Optional. Durch Kommas getrennte Liste der Verbindungseigenschaften, um eine sichere Verbindung zum Confluent-Kafka-Broker herzustellen.

Erstellen einer Confluent-Kafka-Verbindung mit infacmd

Sie können das `infacmd`-Befehlszeilenprogramm verwenden, um eine Confluent-Kafka-Verbindung zu erstellen.

Führen Sie den folgenden Befehl aus, um eine Confluent-Kafka-Verbindung unter UNIX zu erstellen:

```
sh infacmd.sh createConnection -dn <domain name> -un <domain user> -pd <domain password>  
-cn <connection name> -cid <connection id> -ct ConfluentKafka -o  
"kfkBrkList='<host1:port1>,<host2:port2>,<host3:port3>' kfabrokerversion='<version>'  
schemaregistryurl='<schema registry URL>'"
```

Weitere Informationen zum Befehl „CreateConnection“ finden Sie in der *Informatica-Befehlsreferenz*.

Databricks-Verbindungseigenschaften

Verwenden Sie die Databricks-Verbindung zum Ausführen von Mappings auf einem Databricks-Cluster.

Eine Databricks-Verbindung ist eine Verbindung vom Typ „Cluster“. Sie können eine Databricks-Verbindung im Administrator Tool oder im Developer Tool verwalten. Sie können infacmd zum Erstellen einer Databricks-Verbindung verwenden. Konfigurieren Sie die Eigenschaften in der Databricks-Verbindung, um eine Kommunikation zwischen dem Datenintegrationsdienst und dem Databricks-Cluster zu ermöglichen.

In der folgenden Tabelle werden die allgemeinen Verbindungseigenschaften für die Databricks-Verbindung beschrieben:

Eigenschaft	Beschreibung
Name	Der Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung ändern. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten:~ ` ! \$ % ^ & * () - + = { [] } \ ; " ' < , > . ? /
ID	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Optional. Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 4.000 Zeichen enthalten.
Verbindungstyp	Wählen Sie Databricks.
Cluster-Konfiguration	Der Name der Clusterkonfiguration, der der Databricks-Umgebung zugeordnet ist. Erforderlich, wenn Sie die Cloud-Bereitstellung nicht konfigurieren.
Cloud-Bereitstellungskonfiguration	Der Name der Cloud-Bereitstellungskonfiguration, die einer Databricks-Cloud-Plattform zugeordnet ist. Erforderlich, wenn Sie die Clusterkonfiguration nicht konfigurieren.

Eigenschaft	Beschreibung
Staging-Verzeichnis	<p>Das Verzeichnis, in dem die Databricks-Spark-Engine Laufzeit-Staging-Dateien aufbewahrt.</p> <p>Wenn Sie ein Verzeichnis angeben, das nicht vorhanden ist, erstellt es der Datenintegrationsdienst zur Laufzeit.</p> <p>Wenn Sie keinen Verzeichnispfad angeben, werden die Laufzeit-Staging-Dateien in das Verzeichnis <code><cluster staging directory>/DATABRICKS</code> geschrieben.</p>
Erweiterte Eigenschaften	<p>Liste der erweiterten Eigenschaften, die nur für die Databricks-Umgebung gelten. Sie können Laufzeiteigenschaften für die Databricks-Umgebung im Datenintegrationsdienst und in der Databricks-Verbindung konfigurieren. Eine auf einer hohen Ebene konfigurierte Eigenschaft können Sie durch Festlegen des Werts auf einer unteren Ebene überschreiben. Wenn Sie beispielsweise eine Eigenschaft in den benutzerdefinierten Eigenschaften des Datenintegrationsdiensts konfigurieren, können Sie sie in der Databricks-Verbindung überschreiben. Der Datenintegrationsdienst verarbeitet Überschreibungen von Eigenschaften auf der Grundlage der folgenden Prioritäten:</p> <ol style="list-style-type: none"> 1. Erweiterte Databricks-Verbindungseigenschaften 2. Benutzerdefinierte Eigenschaften des Datenintegrationsdiensts <p>Hinweis: Bevor Sie sich nicht in der Drittanbieter- und Informatica-Dokumentation oder beim globalen Kundensupport von Informatica entsprechend informiert haben, rät Informatica von der Änderung dieser Eigenschaftswerte ab. Wenn Sie einen Wert ohne Kenntnis der Eigenschaft ändern, kann es zu Leistungseinbußen oder anderen unerwarteten Ergebnissen kommen.</p>

Erweiterte Eigenschaften

Konfigurieren Sie die folgenden Eigenschaften in den **Erweiterten Eigenschaften** des Abschnitts der Databricks-Konfiguration:

infaspark.json.parser.mode

Gibt an, wie der Parser beschädigte JSON-Datensätze behandeln soll. Sie können den Wert auf einen der folgenden Modi festlegen:

- **DROPMALFORMED.** Der Parser ignoriert alle beschädigten Datensätze. Standardmodus.
- **PERMISSIVE.** Der Parser akzeptiert die Nicht-Standard-Felder als Nullen in beschädigten Datensätzen.
- **FAILFAST.** Der Parser generiert eine Ausnahme, wenn er einen beschädigten Datensatz entdeckt, und die Spark-Anwendung wird beendet.

infaspark.json.parser.multiLine

Gibt an, ob der Parser einen mehrzeiligen Datensatz in einer JSON-Datei lesen kann. Sie können den Wert auf TRUE oder FALSE festlegen. Standardwert ist FALSE. Gilt nur für nicht-native Distributionen, die Spark Version 2.2.x oder höher verwenden.

infaspark.flatfile.writer.nullValue

Wenn die Databricks-Spark-Engine in ein Ziel schreibt, konvertiert sie Nullwerte in leere Zeichenfolgen (" "). Beispiel: 12, AB,"",23p09udj.

Die Databricks-Spark-Engine kann die leeren Zeichenfolgen in Zeichenfolgenspalten schreiben. Aber wenn sie versucht, eine leere Zeichenfolge in eine Nicht-Zeichenfolgenspalte zu schreiben, schlägt das Mapping mit einem Typenkonflikt fehl.

Damit die Databricks-Spark-Engine die leeren Zeichenfolgen in Nullwerte zurück konvertieren und ins Ziel schreiben kann, konfigurieren Sie die Eigenschaft in der Databricks-Spark-Verbindung.

Setzen Sie die Eigenschaft auf TRUE.

infaspark.pythontx.exec

Erforderlich, um eine Python-Umwandlung in der Databricks Spark-Engine auszuführen. Legen Sie sie auf den Speicherort der ausführbaren Python-Binärdatei auf den Worker-Knoten im Hadoop-Cluster fest.

Wenn Sie den Cluster zur Laufzeit bereitstellen, legen Sie diese Eigenschaft in der Cloud-Bereitstellungskonfiguration von Databricks fest. Legen Sie sie andernfalls in der Databricks-Verbindung fest.

Legen Sie die Eigenschaft z. B. fest auf:

```
infaspark.pythontx.exec=/databricks/python3/bin/python3
```

infaspark.pythontx.executorEnv.PYTHONHOME

Erforderlich, um eine Python-Umwandlung in der Databricks Spark-Engine auszuführen. Legen Sie sie auf den Speicherort des Python-Installationsverzeichnis auf den Worker-Knoten im Databricks-Cluster fest.

Wenn Sie den Cluster zur Laufzeit bereitstellen, legen Sie diese Eigenschaft in der Cloud-Bereitstellungskonfiguration von Databricks fest. Legen Sie sie andernfalls in der Databricks-Verbindung fest.

Legen Sie die Eigenschaft z. B. fest auf:

```
infaspark.pythontx.executorEnv.PYTHONHOME=/databricks/python3
```

Greenplum-Verbindungseigenschaften

Verwenden Sie eine Greenplum-Verbindung zum Herstellen einer Verbindung zur Greenplum-Datenbank. Die Greenplum-Verbindung ist ein relationaler Verbindungstyp. Sie können eine Greenplum-Verbindung im Administrator-Tool oder im Developer-Tool verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

Beim Erstellen einer Greenplum-Verbindung geben Sie Informationen für Metadaten und Datenzugriff ein.

In der folgenden Tabelle werden die Eigenschaften von Greenplum-Verbindungen erläutert:

Eigenschaft	Beschreibung
Name	Name der relationalen Greenplum-Verbindung.
ID	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Domäne, auf der die Verbindung erstellt werden soll.
Typ	Typ der Verbindung.

Benutzername, Passwort, Treibername und Verbindungszeichenfolge sind für das Importieren der Metadaten erforderlich. In der folgenden Tabelle werden die Eigenschaften für den Metadatenzugriff beschrieben:

Eigenschaft	Beschreibung
Benutzername	Benutzername mit Berechtigungen für den Zugriff auf die Greenplum-Datenbank.
Passwort	Passwort für die Verbindung zur Greenplum-Datenbank.
Treibername	Der Name des Greenplum JDBC-Treibers. Beispiel: <code>com.pivotal.jdbc.GreenplumDriver</code> Weitere Informationen über den Treiber finden Sie in der Greenplum-Dokumentation.
Verbindungszeichenfolge	Verwenden Sie die folgende Verbindungs-URL: <code>jdbc:pivotal:greenplum:// <hostname>:<port>;DatabaseName=<database_name></code> Weitere Informationen über die Verbindungs-URL finden Sie in der Greenplum-Dokumentation.

PowerExchange for Greenplum verwendet den Hostnamen, die Portnummer und den Datenbanknamen zum Erstellen einer Steuerdatei, in der Ladespezifikationen für das Greenplum-Bulk-Ladeprogramm `gpload` angegeben werden. Die Option zum Aktivieren von SSL und der Zertifikatspfad werden zum Einrichten sicherer Kommunikation mit dem Greenplum-Server über SSL verwendet.

In der folgenden Tabelle werden die Verbindungseigenschaften für den Datenzugriff beschrieben:

Eigenschaft	Beschreibung
Hostname	Hostname oder IP-Adresse des Greenplum-Servers.
Portnummer	Greenplum-Serverportnummer. Wenn Sie „0“ eingeben, liest das Dienstprogramm „gpload“ aus der Umgebungsvariable <code>\$PGPORT</code> . Standardwert ist 5432.
Datenbankname	Name der Datenbank
SSL aktivieren	Wählen Sie diese Option aus, um sichere Kommunikation zwischen dem Dienstprogramm <code>gpload</code> und dem Greenplum-Server über SSL einzurichten.
Zertifikatspfad	Pfad, in dem die SSL-Zertifikate für den Greenplum-Server gespeichert werden. Informationen zu den Dateien, die im Zertifikatspfad enthalten sein müssen, finden Sie in der <code>gpload</code> -Dokumentation.

Google Analytics-Verbindungseigenschaften

Wenn Sie eine Google Analytics-Verbindung einrichten, müssen Sie die Verbindungseigenschaften konfigurieren.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Google Analytics-Verbindungseigenschaften beschrieben:

Eigenschaft	Beschreibung
Name	Der Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung ändern. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * () - + = { [] \ : ; " ' < , > . ? /
ID	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Die ID darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Optional. Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 4.000 Zeichen enthalten.
Speicherort	Die Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Der Verbindungstyp. Wählen Sie Google Analytics .
Dienstkonto-ID	Gibt den Wert von „client_email“ in der JSON-Datei an, die Sie nach dem Erstellen eines Dienstkontos herunterladen.
Dienstkontoschlüssel	Gibt den Wert von „private_key“ in der JSON-Datei an, die Sie nach dem Erstellen eines Dienstkontos herunterladen.
APIVersion	API, die PowerExchange for Google Analytics zum Lesen der Google Analytics-Berichte verwendet. Wählen Sie Core Reporting API v3 . Hinweis: PowerExchange for Google Analytics unterstützt nicht Analytics Reporting API v4.

Google BigQuery-Verbindungseigenschaften

Wenn Sie eine Google BigQuery-Verbindung einrichten, müssen Sie die Verbindungseigenschaften konfigurieren.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Google BigQuery-Verbindungseigenschaften beschrieben:

Eigenschaft	Beschreibung
Dienstkonto-ID	Gibt den Wert von „client_email“ in der JSON-Datei an, die Sie nach dem Erstellen eines Dienstkontos in Google BigQuery herunterladen.
Dienstkontoschlüssel	Gibt den Wert von „private_key“ in der JSON-Datei an, die Sie nach dem Erstellen eines Dienstkontos in Google BigQuery herunterladen.

Eigenschaft	Beschreibung
Verbindungsmodus	<p>Der Modus, in dem Sie Daten von Google BigQuery lesen oder darin schreiben möchten. Wählen Sie einen der folgenden Verbindungsmodi aus:</p> <ul style="list-style-type: none"> - Einfach. Enthierarchisiert jedes Feld innerhalb des Felds mit dem Datentyp „Datensatz“ als separates Feld im Mapping. - Hybrid. Zeigt alle Felder der obersten Ebene in der Google BigQuery-Tabelle an, einschließlich der Felder mit dem Datentyp „Datensatz“. PowerExchange for Google BigQuery zeigt das Feld der obersten Ebene mit dem Datentyp „Datensatz“ im Mapping als einzelnes Feld mit dem Datentyp „Zeichenfolge“ an. - Komplex. Zeigt alle Spalten in der Google BigQuery-Tabelle als einzelnes Feld mit dem Datentyp „Zeichenfolge“ im Mapping an. <p>Der Standardwert ist „Einfach“.</p>
Dateipfad für die Schemadefinition	<p>Gibt ein Verzeichnis auf dem Client-Computer an, in dem der eine JSON-Datei mit dem Beispielschema der Google BigQuery-Tabelle erstellen muss. Der Name der JSON-Datei ist der gleiche wie der Name der Google BigQuery-Tabelle.</p> <p>Alternativ können Sie einen Speicherpfad in Google Cloud Storage angeben, in dem der eine JSON-Datei mit dem Beispielschema der Google BigQuery-Tabelle erstellen muss. Sie können die JSON-Datei vom angegebenen Speicherpfad in Google Cloud Storage auf einen lokalen Computer herunterladen.</p>
Projekt-ID	<p>Gibt den Wert von „project_id“ in der JSON-Datei an, die Sie nach dem Erstellen eines Dienstkontos in Google BigQuery herunterladen.</p> <p>Wenn Sie mehrere Projekte mit demselben Dienstkonto erstellt haben, geben Sie die ID des Projekts ein, das den Datensatz enthält, zu der Sie eine Verbindung herstellen möchten.</p>
Speicherpfad	<p>Diese Eigenschaft wird angewendet, wenn Sie große Datenmengen lesen oder schreiben. Pfad in Google Cloud Storage, in dem der eine lokale Stage-Datei zum vorübergehenden Speichern der Daten erstellt.</p> <p>Sie können entweder den Bucket-Namen oder den Bucket-Namen und den Ordnernamen eingeben.</p> <p>Geben Sie beispielsweise <code>gs://<Bucket-Name></code> oder <code>gs://<Bucket-Name>/<Ordnername></code> ein.</p>
Datensatz-ID	Gilt nicht für PowerExchange for Google BigQuery.
Legacy-SQL für benutzerdefinierte Abfrage verwenden	Gilt nicht für PowerExchange for Google BigQuery.
Datensatzname für benutzerdefinierte Abfrage	Gilt nicht für PowerExchange for Google BigQuery.
Staging-Datensatz	<p>Der Name des Google BigQuery-Datensatzes, in dem Sie die Staging-Tabelle erstellen möchten, um die Daten bereitzustellen. Sie können einen Google BigQuery-Datensatz definieren, das sich vom Quell- oder Zieldatensatz unterscheidet.</p>

Eigenschaft	Beschreibung
Bereichs-ID	<p>Regionsname, in der sich der Google BigQuery-Datensatz befindet.</p> <p>Wenn Sie beispielsweise eine Verbindung zu einem Google BigQuery-Datensatz herstellen möchten, der sich in der Region Las Vegas befindet, geben Sie us-west4 als Bereichs-ID an.</p> <p>Hinweis: Stellen Sie sicher, dass Sie in der Verbindungseigenschaft Speicherpfad einen Bucket-Namen oder den Bucket-Namen und den Ordernamen angeben, der bzw. die sich in derselben Region befinden wie der Datensatz in Google BigQuery.</p> <p>Weitere Informationen zu den von Google BigQuery unterstützten Regionen finden Sie in der folgenden Google BigQuery-Dokumentation: https://cloud.google.com/bigquery/docs/locations</p>
Optionale Eigenschaften	<p>Gibt an, ob Sie bestimmte Quell- und Zielfunktionen über benutzerdefinierte Eigenschaften konfigurieren können.</p> <p>Sie können eine der folgenden Optionen auswählen:</p> <ul style="list-style-type: none"> - Keine. Wählen Sie diese Option aus, wenn Sie keine benutzerdefinierten Eigenschaften konfigurieren möchten. - Erforderlich. Wählen Sie diese Option aus, wenn Sie benutzerdefinierte Eigenschaften angeben möchten, um die Quell- und Zielfunktionen zu konfigurieren. <p>Standardwert ist „Keine“.</p>
Optionale Eigenschaften bereitstellen	<p>Durch Kommas getrennte Schlüssel-Wert-Paare von benutzerdefinierten Eigenschaften, um bestimmte Quell- und Zielfunktionen zu aktivieren.</p> <p>Wird nur bei Auswahl Erforderlich in den optionalen Eigenschaften angezeigt.</p> <p>Weitere Informationen zur Liste der benutzerdefinierten Eigenschaften, die Sie angeben können, finden Sie in folgendem Artikel der Informatica-Wissensdatenbank: https://kb.informatica.com/faq/7/Pages/26/632722.aspx</p>

Verbindungsmodi

Sie können eine Google BigQuery-Verbindung so konfigurieren, dass sie einen der folgenden Verbindungsmodi verwendet:

Einfacher Modus

Wenn Sie den einfachen Modus verwenden, enthierarchisiert PowerExchange for Google BigQuery jedes Feld innerhalb des Felds mit dem Datentyp „Datensatz“ als ein separates Feld im Google BigQuery-Datenobjekt.

Hybrid-Modus

Wenn Sie den Hybrid-Modus verwenden, zeigt PowerExchange for Google BigQuery alle Felder der obersten Ebene in der Google BigQuery-Tabelle an, einschließlich der Felder mit dem Datentyp „Datensatz“. PowerExchange for Google BigQuery zeigt das Feld der obersten Ebene mit dem Datentyp „Datensatz“ im Google BigQuery-Datenobjekt als einzelnes Feld mit dem Datentyp „Zeichenfolge“ an.

Komplexer Modus

Wenn Sie den komplexen Modus verwenden, zeigt PowerExchange for Google BigQuery alle Spalten der Google BigQuery-Tabelle im Google BigQuery-Datenobjekt als einzelne Felder des Datentyps „Zeichenfolge“ an.

Sie können Google BigQuery-Ansichten für einfache, komplexe und hybride Verbindungsmodi verwenden.

Google Cloud Spanner-Verbindungseigenschaften

Wenn Sie eine Google Cloud Spanner-Verbindung einrichten, müssen Sie die Verbindungseigenschaften konfigurieren.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Google Cloud Spanner-Verbindungseigenschaften beschrieben:

Eigenschaft	Beschreibung
Name	Der Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung ändern. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * () - + = { [] \ : ; " ' < , > . ? /
ID	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Die ID darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Optional. Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 4.000 Zeichen enthalten.
Speicherort	Die Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Der Verbindungstyp. Wählen Sie Google Cloud Spanner aus.
Projekt-ID	Gibt den Wert von „project_id“ in der JSON-Datei an, die Sie nach dem Erstellen eines Dienstkontos herunterladen. Wenn Sie mehrere Projekte mit demselben Dienstkonto erstellt haben, geben Sie die ID des Projekts ein, das den Bucket enthält, zu dem Sie eine Verbindung herstellen möchten.
Dienstkonto-ID	Gibt den Wert von „client_email“ in der JSON-Datei an, die Sie nach dem Erstellen eines Dienstkontos herunterladen.
Dienstkontoschlüssel	Gibt den Wert von „private_key“ in der JSON-Datei an, die Sie nach dem Erstellen eines Dienstkontos herunterladen.
Instanz-ID	Name der Instanz, die Sie in Google Cloud Spanner erstellt haben.

Google Cloud Storage-Verbindungseigenschaften

Wenn Sie eine Google Cloud Storage-Verbindung einrichten, müssen Sie die Verbindungseigenschaften konfigurieren.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Google Cloud Storage-Verbindungseigenschaften beschrieben:

Eigenschaft	Beschreibung
Name	Der Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung ändern. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
ID	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Die ID darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Optional. Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 4.000 Zeichen enthalten.
Speicherort	Die Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Der Verbindungstyp. Wählen Sie Google Cloud Storage aus.
Projekt-ID	Gibt den Wert von „project_id“ in der JSON-Datei an, die Sie nach dem Erstellen eines Dienstkontos herunterladen. Wenn Sie mehrere Projekte mit demselben Dienstkonto erstellt haben, geben Sie die ID des Projekts ein, das den Bucket enthält, zu dem Sie eine Verbindung herstellen möchten.
Dienstkonto-ID	Gibt den Wert von „client_email“ in der JSON-Datei an, die Sie nach dem Erstellen eines Dienstkontos herunterladen.
Dienstkontoschlüssel	Gibt den Wert von „private_key“ in der JSON-Datei an, die Sie nach dem Erstellen eines Dienstkontos herunterladen.

Google PubSub-Verbindungseigenschaften

Wenn Sie eine Google PubSub-Verbindung erstellen, müssen Sie die Verbindungseigenschaften konfigurieren.

In der folgenden Tabelle werden die Google PubSub-Verbindungseigenschaften beschrieben:

Eigenschaft	Beschreibung
Name	Der Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Sie können diese Eigenschaft ändern, nachdem Sie die Verbindung erstellt haben. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
ID	Die Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.

Eigenschaft	Beschreibung
Beschreibung	Die Beschreibung der Verbindung. Geben Sie eine Zeichenfolge ein, mit der Sie die Verbindung angeben können. Die Beschreibung darf nicht mehr als 4.000 Zeichen enthalten.
Verbindungstyp	Der Verbindungstyp. Wählen Sie den Verbindungstyp PubSub aus.
Client-E-Mail	Der Wert <code>client_email</code> , der in der JSON-Datei verfügbar ist, die Sie nach dem Erstellen eines Dienstkontos herunterladen.
Client-ID	Der Wert <code>client_id</code> , der in der JSON-Datei verfügbar ist, die Sie nach dem Erstellen eines Dienstkontos herunterladen.
ID des privaten Schlüssels	Der Wert <code>private_key_id</code> , der in der JSON-Datei verfügbar ist, die Sie nach dem Erstellen eines Dienstkontos herunterladen.
Privater Schlüssel	Der Wert <code>private_key</code> , der in der JSON-Datei verfügbar ist, die Sie nach dem Erstellen eines Dienstkontos herunterladen.
Projekt-ID	Der Wert <code>private_id</code> , der in der JSON-Datei verfügbar ist, die Sie nach dem Erstellen eines Dienstkontos herunterladen.

Hadoop-Verbindungseigenschaften

Verwenden Sie die Hadoop-Verbindung, um Zuordnungen für die Ausführung auf einem Hadoop-Cluster zu konfigurieren. Bei einer Hadoop-Verbindung handelt es sich um eine Verbindung vom Typ „Cluster“. Sie können eine Hadoop-Verbindung im Administrator Tool oder im Developer Tool erstellen und verwalten. Sie können `infacmd` verwenden, um eine Hadoop-Verbindung zu erstellen. Hadoop-Verbindungseigenschaften unterscheiden zwischen Groß- und Kleinschreibung, sofern nicht anders angegeben.

Sie haben die Möglichkeit, Laufzeiteigenschaften für die Hadoop-Umgebung im Datenintegrationsdienst, in der Hadoop-Verbindung und im Mapping zu konfigurieren. Eine auf einer hohen Ebene konfigurierte Eigenschaft können Sie durch Festlegen des Werts auf einer unteren Ebene überschreiben. Wenn Sie z. B. eine Eigenschaft in den benutzerdefinierten Eigenschaften des Datenintegrationsdiensts konfigurieren, können Sie diese in der Hadoop-Verbindung oder im Mapping überschreiben. Der Datenintegrationsdienst verarbeitet Überschreibungen von Eigenschaften auf der Grundlage der folgenden Prioritäten:

1. Zuordnung der mit dem Befehl `infacmd ms runMapping` und der Option `-cp` festgelegten benutzerdefinierten Eigenschaften
2. Zuordnung der Laufzeiteigenschaften für die Hadoop-Umgebung
3. Erweiterte Eigenschaften der Hadoop-Verbindung für Laufzeit-Engines
4. Erweiterte allgemeine Eigenschaften, Umgebungsvariablen und Klassenpfade der Hadoop-Verbindung
5. Benutzerdefinierte Eigenschaften des Datenintegrationsdiensts

Hinweis: Wenn eine Zuordnung Hive-Server 2 zum Ausführen eines Jobs oder von Teilen eines Jobs verwendet, können Sie keine Eigenschaften überschreiben, die auf Cluster-Ebene in PreSQL- oder Post-SQL-Abfragen oder SQL-Überschreibungsanweisungen konfiguriert sind. Problemumgehung: Statt die Clusterkonfiguration in der Domäne zum Überschreiben von Cluster-Eigenschaften zu verwenden, übergeben Sie die Überschreibungseinstellungen an die JDBC-URL. Beispiel: `beeline -u "jdbc:hive2://<domain host>:<port_number>/tpch_text_100" --hiveconf hive.execution.engine=tez`

Eigenschaften des Hadoop-Clusters

Konfigurieren Sie Eigenschaften in der Hadoop-Verbindung, um Kommunikation zwischen dem Datenintegrationsdienst und dem Hadoop-Cluster zu ermöglichen.

In der folgenden Tabelle werden die allgemeinen Verbindungseigenschaften für die Hadoop-Verbindung beschrieben:

Eigenschaft	Beschreibung
Name	Der Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung ändern. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * () - + = { [] \ : ; " ' < , > . ? /
ID	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Die Beschreibung der Verbindung. Geben Sie eine Zeichenfolge ein, mit der Sie die Verbindung angeben können. Die Beschreibung darf nicht mehr als 4.000 Zeichen enthalten.
Cluster-Konfiguration	Der Name der mit der Hadoop-Umgebung verknüpften Cluster-Konfiguration. Erforderlich, wenn Sie die Cloud-Bereitstellungskonfiguration nicht konfigurieren.
Cloud-Bereitstellungskonfiguration	Name der Cloud-Bereitstellungskonfiguration, die einer Cloud-Plattform wie Amazon AWS oder Microsoft Azure zugeordnet ist. Erforderlich, wenn Sie die Cluster-Konfiguration nicht konfigurieren.

Eigenschaft	Beschreibung
Cluster-Umgebungsvariablen*	<p>Umgebungsvariablen, die vom Hadoop-Cluster verwendet werden.</p> <p>Konfigurieren Sie bei Verwendung eines Cloudera CDH 6.x- oder eines Cloudera CDP-Clusters die Gebietsschemaeinstellung als Cluster-Umgebungsvariablen. In Cloudera Manager müssen Sie darüber hinaus die Umgebungsvariablen zu folgender YARN-Eigenschaft hinzufügen:</p> <pre>yarn.nodemanager.env-whitelist</pre> <p>Die Variable ORACLE_HOME stellt beispielsweise das Verzeichnis dar, in dem die Software des Oracle-Datenbank-Clients installiert ist.</p> <p>Sie haben die Möglichkeit, Laufzeiteigenschaften für die Hadoop-Umgebung im Datenintegrationsdienst, in der Hadoop-Verbindung und im Mapping zu konfigurieren. Eine auf einer hohen Ebene konfigurierte Eigenschaft können Sie durch Festlegen des Werts auf einer unteren Ebene überschreiben. Wenn Sie z. B. eine Eigenschaft in den benutzerdefinierten Eigenschaften des Datenintegrationsdiensts konfigurieren, können Sie diese in der Hadoop-Verbindung oder im Mapping überschreiben. Der Datenintegrationsdienst verarbeitet Überschreibungen von Eigenschaften auf der Grundlage der folgenden Prioritäten:</p> <ol style="list-style-type: none"> 1. Zuordnung der mit dem Befehl <code>infacmd ms runMapping</code> und der Option <code>-cp</code> festgelegten benutzerdefinierten Eigenschaften 2. Zuordnung der Laufzeiteigenschaften für die Hadoop-Umgebung 3. Erweiterte Eigenschaften der Hadoop-Verbindung für Laufzeit-Engines 4. Erweiterte allgemeine Eigenschaften, Umgebungsvariablen und Klassenpfade der Hadoop-Verbindung 5. Benutzerdefinierte Eigenschaften des Datenintegrationsdiensts <p>Hinweis: Wenn eine Zuordnung Hive-Server 2 zum Ausführen eines Jobs oder von Teilen eines Jobs verwendet, können Sie keine Eigenschaften überschreiben, die auf Cluster-Ebene in PreSQL- oder Post-SQL-Abfragen oder SQL-Überschreibungsanweisungen konfiguriert sind. Problemumgehung: Statt die Clusterkonfiguration in der Domäne zum Überschreiben von Cluster-Eigenschaften zu verwenden, übergeben Sie die Überschreibungseinstellungen an die JDBC-URL. Beispiel: <code>beeline -u "jdbc:hive2://<domain host>:<port_number>/tpch_text_100" --hiveconf hive.execution.engine=tez</code></p>
Cluster-Bibliothekspfad*	<p>Der Pfad für freigegebene Bibliotheken auf dem Cluster.</p> <p>Die Variable <code>\$DEFAULT_CLUSTER_LIBRARY_PATH</code> enthält eine Liste der Standardverzeichnisse.</p>

Eigenschaft	Beschreibung
Cluster-Klassenpfad*	<p>Der Klassenpfad für den Zugriff auf die Hadoop-JAR-Dateien und die benötigten Bibliotheken.</p> <p>Die Variable \$DEFAULT_CLUSTER_CLASSPATH enthält eine Liste mit Pfaden der Standard-JAR-Dateien und Bibliotheken.</p> <p>Sie haben die Möglichkeit, Laufzeiteigenschaften für die Hadoop-Umgebung im Datenintegrationsdienst, in der Hadoop-Verbindung und im Mapping zu konfigurieren. Eine auf einer hohen Ebene konfigurierte Eigenschaft können Sie durch Festlegen des Werts auf einer unteren Ebene überschreiben. Wenn Sie z. B. eine Eigenschaft in den benutzerdefinierten Eigenschaften des Datenintegrationsdiensts konfigurieren, können Sie diese in der Hadoop-Verbindung oder im Mapping überschreiben. Der Datenintegrationsdienst verarbeitet Überschreibungen von Eigenschaften auf der Grundlage der folgenden Prioritäten:</p> <ol style="list-style-type: none"> 1. Zuordnung der mit dem Befehl <code>infacmd ms runMapping</code> und der Option <code>-cp</code> festgelegten benutzerdefinierten Eigenschaften 2. Zuordnung der Laufzeiteigenschaften für die Hadoop-Umgebung 3. Erweiterte Eigenschaften der Hadoop-Verbindung für Laufzeit-Engines 4. Erweiterte allgemeine Eigenschaften, Umgebungsvariablen und Klassenpfade der Hadoop-Verbindung 5. Benutzerdefinierte Eigenschaften des Datenintegrationsdiensts <p>Hinweis: Wenn eine Zuordnung Hive-Server 2 zum Ausführen eines Jobs oder von Teilen eines Jobs verwendet, können Sie keine Eigenschaften überschreiben, die auf Cluster-Ebene in PreSQL- oder Post-SQL-Abfragen oder SQL-Überschreibungsanweisungen konfiguriert sind. Problemumgehung: Statt die Clusterkonfiguration in der Domäne zum Überschreiben von Cluster-Eigenschaften zu verwenden, übergeben Sie die Überschreibungseinstellungen an die JDBC-URL. Beispiel: <code>beeline -u "jdbc:hive2://<domain host>:<port_number>/tpch_text_100" --hiveconf hive.execution.engine=tez</code></p>
Pfad der ausführbaren Datei des Clusters*	<p>Der Pfad für ausführbare Dateien auf dem Cluster.</p> <p>Die Variable \$DEFAULT_CLUSTER_EXEC_PATH enthält eine Liste mit Pfaden der ausführbaren Standarddateien.</p>
<p>* Bevor Sie sich nicht in der Drittanbieter- und Informatica-Dokumentation oder beim globalen Kundensupport von Informatica entsprechend informiert haben, rät Informatica von der Änderung dieser Eigenschaftswerte ab. Wenn Sie einen Wert ohne Kenntnis der Eigenschaft ändern, kann es zu Leistungseinbußen oder anderen unerwarteten Ergebnissen kommen.</p>	

Allgemeine Eigenschaften

In der folgenden Tabelle werden die allgemeinen Verbindungseigenschaften beschrieben, die Sie für die Hadoop-Verbindung konfigurieren:

Eigenschaft	Beschreibung
Benutzername für Identitätswechsel	<p>Erforderlich, wenn der Hadoop-Cluster die Kerberos-Authentifizierung verwendet. Benutzer für den Hadoop-Identitätswechsel. Der Benutzername, den der Datenintegrationsdienst zum Ausführen von Zuordnungen im Hadoop-Cluster verwendet.</p> <p>Data Engineering Integration unterstützt Betriebssystemprofile auf allen Hadoop-Distributionen. In der Hadoop-Laufzeitumgebung überträgt der Datenintegrationsdienst die Verarbeitung per Push an den Hadoop-Cluster und die Laufzeit-Engines führen Zuordnungen mit den vom Betriebssystemprofil angegebenen Hadoop-Identitätswechseleigenschaften aus.</p>
Temporärer Tabellen-Komprimierungs-Codec	<p>Hadoop-Komprimierungsbibliothek für einen Komprimierungs-Codec-Klassennamen.</p> <p>Hinweis: Die Spark-Engine unterstützt keine Komprimierungseinstellungen für temporäre Tabellen. Wenn Sie Zuordnungen in der Spark-Engine ausführen, speichert die Spark-Engine temporäre Tabellen in einem nicht komprimierten Dateiformat.</p>
Codec-Klassename	<p>Codec-Klassename, der die Datenkomprimierung aktiviert und die Leistung in temporären Staging-Tabellen verbessert.</p>
Name der Hive-Staging-Datenbank	<p>Namespace für Hive-Staging-Tabellen. Verwenden Sie den Namen <code>default</code> für Tabellen, bei denen kein Datenbankname angegeben wurde.</p> <p>Wenn Sie keinen Namespace konfigurieren, verwendet der Datenintegrationsdienst den Namen der Hive-Datenbank in der Hive-Zielverbindung, um Staging-Tabellen zu erstellen.</p> <p>Wenn Sie ein Mapping in der nativen Umgebung ausführen, um Daten in Hive zu schreiben, müssen Sie den Namen der Hive-Staging-Datenbank in der Hive-Verbindung konfigurieren. Der Datenintegrationsdienst ignoriert den Wert, den Sie in der Hadoop-Verbindung konfigurieren.</p>
Umgebungs-SQL	<p>SQL-Befehle zum Einrichten der Hadoop-Umgebung. Der Datenintegrationsdienst führt die Umgebungs-SQL am Anfang jedes Hive-Skripts aus, das von einem HiveServer2-Job erzeugt wurde.</p> <p>Die folgenden Regeln und Richtlinien gelten für die Verwendung von Umgebungs-SQL:</p> <ul style="list-style-type: none"> - Sie können Umgebungs-SQL zum Definieren von Hadoop- oder Hive-Parametern verwenden, die Sie in den PreSQL-Befehlen oder in benutzerspezifischen Abfragen nutzen möchten. - Wenn Sie mehrere Werte für die Eigenschaft „Umgebungs-SQL“ verwenden, stellen Sie sicher, dass sich zwischen den Werten keine Leerzeichen befinden.

Eigenschaft	Beschreibung
Engine-Typ	<p>Der Datenintegrationsdienst verwendet HiveServer2, um Teile von einigen Jobs zu verarbeiten, indem HiveServer2-Aufgaben auf der Spark-Engine ausgeführt werden. Wenn Sie die Clusterkonfiguration über das Administrator Tool importieren, können Sie Verbindungen erstellen. Die Engine-Typeigenschaft wird standardmäßig basierend auf der Distribution aufgefüllt.</p> <p>Wenn Sie eine Verbindung manuell erstellen, müssen Sie den Engine-Typ konfigurieren. Sie können den Engine-Typ basierend auf den folgenden Hadoop-Distributionen angeben:</p> <ul style="list-style-type: none"> - Amazon EMR. Tez - Azure HDI. Tez - Cloudera CDH. MRv2 - Cloudera CDP. Tez - Dataproc MRv2 - Hortonworks HDP. Tez - MapR. MRv2
Erweiterte Eigenschaften	<p>Liste der erweiterten Eigenschaften, die nur für die Hadoop-Umgebung gelten. Die Eigenschaften gelten für die Blaze- und die Spark-Engine. Die erweiterten Eigenschaften enthalten eine Liste der Standardeigenschaften.</p> <p>Sie haben die Möglichkeit, Laufzeiteigenschaften für die Hadoop-Umgebung im Datenintegrationsdienst, in der Hadoop-Verbindung und im Mapping zu konfigurieren. Eine auf einer hohen Ebene konfigurierte Eigenschaft können Sie durch Festlegen des Werts auf einer unteren Ebene überschreiben. Wenn Sie z. B. eine Eigenschaft in den benutzerdefinierten Eigenschaften des Datenintegrationsdiensts konfigurieren, können Sie diese in der Hadoop-Verbindung oder im Mapping überschreiben. Der Datenintegrationsdienst verarbeitet Überschreibungen von Eigenschaften auf der Grundlage der folgenden Prioritäten:</p> <ol style="list-style-type: none"> 1. Zuordnung der mit dem Befehl <code>infacmd ms runMapping</code> und der Option <code>-cp</code> festgelegten benutzerdefinierten Eigenschaften 2. Zuordnung der Laufzeiteigenschaften für die Hadoop-Umgebung 3. Erweiterte Eigenschaften der Hadoop-Verbindung für Laufzeit-Engines 4. Erweiterte allgemeine Eigenschaften, Umgebungsvariablen und Klassenpfade der Hadoop-Verbindung 5. Benutzerdefinierte Eigenschaften des Datenintegrationsdiensts <p>Hinweis: Wenn eine Zuordnung Hive-Server 2 zum Ausführen eines Jobs oder von Teilen eines Jobs verwendet, können Sie keine Eigenschaften überschreiben, die auf Cluster-Ebene in PreSQL- oder Post-SQL-Abfragen oder SQL-Überschreibungsanweisungen konfiguriert sind. Problemumgehung: Statt die Clusterkonfiguration in der Domäne zum Überschreiben von Cluster-Eigenschaften zu verwenden, übergeben Sie die Überschreibungseinstellungen an die JDBC-URL. Beispiel: <code>beeline -u "jdbc:hive2://<domain host>:<port_number>/tpch_text_100" --hiveconf hive.execution.engine=tez</code></p> <p>Hinweis: Bevor Sie sich nicht in der Drittanbieter- und Informatica-Dokumentation oder beim globalen Kundensupport von Informatica entsprechend informiert haben, rät Informatica von der Änderung dieser Eigenschaftswerte ab. Wenn Sie einen Wert ohne Kenntnis der Eigenschaft ändern, kann es zu Leistungseinbußen oder anderen unerwarteten Ergebnissen kommen.</p>

Eigenschaften des Ablehnungsverzeichnisses

In der folgenden Tabelle werden die Verbindungseigenschaften beschrieben, die Sie für das Hadoop-Ablehnungsverzeichnis konfigurieren.

Eigenschaft	Beschreibung
Ablehnungsdateien in Hadoop schreiben	Wenn Sie die Blaze-Engine zum Ausführen von Zuordnungen verwenden, aktivieren Sie das Kontrollkästchen zur Angabe eines Speicherorts, in den Ablehnungsdateien verschoben werden. Bei aktiviertem Kontrollkästchen verschiebt der Datenintegrationsdienst die Ablehnungsdateien in den HDFS- Speicherort oder den ViewFS-Speicherort (View File System), der in der Eigenschaft „Verzeichnis der Ablehnungsdatei“ aufgeführt ist. Standardmäßig speichert der Datenintegrationsdienst die Ablehnungsdateien basierend auf dem RejectDir-Systemparameter.
Verzeichnis der Ablehnungsdatei	Das Verzeichnis für Hadoop-Zuordnungsdateien auf HDFS oder ViewFS, wenn Sie Zuordnungen ausführen.

Blaze-Konfiguration

In der folgenden Tabelle werden die Verbindungseigenschaften beschrieben, die Sie für die Blaze-Engine konfigurieren:

Eigenschaft	Beschreibung
Blaze-Staging-Verzeichnis	Der HDFS-Dateipfad des Verzeichnisses, das von der Blaze-Engine zum Speichern temporärer Dateien verwendet wird. Stellen Sie sicher, dass das Verzeichnis vorhanden ist. Der YARN-Benutzer, der Benutzer der Blaze-Engine und der Benutzer für Identitätswechsel von Zuordnungen müssen über Schreibberechtigungen für dieses Verzeichnis verfügen. Standardwert ist <code>/blaze/workdir</code> . Wenn Sie diese Eigenschaft löschen, werden die Staging-Dateien in das Hadoop-Staging-Verzeichnis <code>/tmp/blaze_<Benutzername></code> geschrieben.
Blaze-Benutzername	Der Eigentümer des Blaze-Dienstes und der Blaze-Dienstprotokolle. Wenn der Hadoop-Cluster die Kerberos-Authentifizierung verwendet, ist der standardmäßige Benutzer der SPN-Benutzer des Datenintegrationsdiensts. Wenn der Hadoop-Cluster die Kerberos-Authentifizierung nicht verwendet und der Blaze-Benutzer nicht konfiguriert ist, ist der standardmäßige Benutzer der Datenintegrationsdienst-Benutzer.
Niedrigste Portnummer	Der Minimalwert für den Portnummernbereich der Blaze-Engine. Standardwert ist 12300.
Höchste Portnummer	Der Maximalwert für den Portnummernbereich der Blaze-Engine. Standardwert ist 12600.
Name der YARN-Warteschlange	Der von der Blaze-Engine verwendete Warteschlangenname des YARN-Schedulers, der verfügbare Ressourcen auf einem Cluster angibt. Hinweis: Wenn vorzeitige YARN-Entfernung auf dem Cluster aktiviert ist, vergewissern Sie sich beim Hadoop-Administrator, dass vorzeitige Entfernung in der mit der Blaze-Engine verknüpften Warteschlange deaktiviert ist.

Eigenschaft	Beschreibung
Adresse der Blaze-Job-Überwachung	<p>Der Hostname und die Portnummer für die Blaze-Job-Überwachung. Verwenden Sie das folgende Format: <code><hostname>:<port></code></p> <p>Wobei</p> <ul style="list-style-type: none"> - <code><hostname></code> ist der Hostname oder die IP-Adresse des Servers der Blaze-Job-Überwachung. - <code><port></code> ist der Port, den die Blaze-Job-Überwachung auf Remoteprozeduraufrufe (RPC) abhört. <p>Geben Sie beispielsweise Folgendes ein: <code>myhostname:9080</code></p>
Blaze YARN-Knotenbezeichnung	<p>Knotenbezeichnung, die den Knoten auf dem Hadoop-Cluster bestimmt, auf dem die Blaze-Engine läuft. Wenn Sie keine Knotenbezeichnung angeben, läuft die Blaze-Engine auf den Knoten in der Standardpartition.</p> <p>Wenn der Hadoop-Cluster logische Operatoren für Knotenbezeichnungen unterstützt, können Sie eine Liste von Knotenbezeichnungen angeben. Um die Knotenbezeichnungen aufzulisten, verwenden Sie die Operatoren <code>&&</code> (UND), <code> </code> (ODER) und <code>!</code> (NICHT).</p> <p>Hinweis: Sie können keine Knotenbezeichnungen für einen Cloudera CDH-Cluster verwenden.</p>
Erweiterte Eigenschaften	<p>Liste der erweiterten Eigenschaften, die nur für die Blaze-Engine gelten. Die erweiterten Eigenschaften enthalten eine Liste der Standardeigenschaften.</p> <p>Sie haben die Möglichkeit, Laufzeiteigenschaften für die Hadoop-Umgebung im Datenintegrationsdienst, in der Hadoop-Verbindung und im Mapping zu konfigurieren. Eine auf einer hohen Ebene konfigurierte Eigenschaft können Sie durch Festlegen des Werts auf einer unteren Ebene überschreiben. Wenn Sie z. B. eine Eigenschaft in den benutzerdefinierten Eigenschaften des Datenintegrationsdiensts konfigurieren, können Sie diese in der Hadoop-Verbindung oder im Mapping überschreiben. Der Datenintegrationsdienst verarbeitet Überschreibungen von Eigenschaften auf der Grundlage der folgenden Prioritäten:</p> <ol style="list-style-type: none"> 1. Zuordnung der mit dem Befehl <code>infacmd ms runMapping</code> und der Option <code>-cp</code> festgelegten benutzerdefinierten Eigenschaften 2. Zuordnung der Laufzeiteigenschaften für die Hadoop-Umgebung 3. Erweiterte Eigenschaften der Hadoop-Verbindung für Laufzeit-Engines 4. Erweiterte allgemeine Eigenschaften, Umgebungsvariablen und Klassenpfade der Hadoop-Verbindung 5. Benutzerdefinierte Eigenschaften des Datenintegrationsdiensts <p>Hinweis: Wenn eine Zuordnung Hive-Server 2 zum Ausführen eines Jobs oder von Teilen eines Jobs verwendet, können Sie keine Eigenschaften überschreiben, die auf Cluster-Ebene in PreSQL- oder Post-SQL-Abfragen oder SQL-Überschreibungsanweisungen konfiguriert sind. Problemumgehung: Statt die Clusterkonfiguration in der Domäne zum Überschreiben von Cluster-Eigenschaften zu verwenden, übergeben Sie die Überschreibungseinstellungen an die JDBC-URL. Beispiel: <code>beeline -u "jdbc:hive2://<domain host>:<port_number>/tpch_text_100" --hiveconf hive.execution.engine=tez</code></p> <p>Hinweis: Bevor Sie sich nicht in der Drittanbieter- und Informatica-Dokumentation oder beim globalen Kundensupport von Informatica entsprechend informiert haben, rät Informatica von der Änderung dieser Eigenschaftswerte ab. Wenn Sie einen Wert ohne Kenntnis der Eigenschaft ändern, kann es zu Leistungseinbußen oder anderen unerwarteten Ergebnissen kommen.</p>

Spark-Konfiguration

In der folgenden Tabelle werden die Verbindungseigenschaften beschrieben, die Sie für die Spark-Engine konfigurieren:

Eigenschaft	Beschreibung
Spark-Staging-Verzeichnis	<p>Der HDFS-Dateipfad des Verzeichnisses, das von der Spark-Engine zum Speichern temporärer Dateien für die Ausführung von Jobs verwendet wird. Der YARN-Benutzer, Datenintegrationsdienst-Benutzer und Zuordnungs-Identitätswechsel-Benutzer müssen über Schreibberechtigung für dieses Verzeichnis verfügen.</p> <p>Wenn Sie keinen Dateipfad angeben, werden die temporären Dateien standardmäßig in das Hadoop-Staging-Verzeichnis <code>/tmp/SPARK_<Benutzername></code> geschrieben.</p> <p>Wenn Sie Sqoop-Jobs auf der Spark-Engine ausführen, erstellt der Datenintegrationsdienst ein Sqoop-Staging-Verzeichnis unter dem Spark-Staging-Verzeichnis, um temporäre Dateien zu speichern: <code><Spark-Staging-Verzeichnis>/sqoop_staging</code></p>
Verzeichnis des Spark-Ereignisprotokolls	Optional. Der HDFS-Dateipfad des Verzeichnisses, das die Spark-Engine zur Protokollierung von Ereignissen verwendet.
Name der YARN-Warteschlange	Der von der Spark-Engine verwendete Name der YARN-Scheduler-Warteschlange, der verfügbare Ressourcen auf einem Cluster angibt. Bei diesem Namen wird zwischen Groß- und Kleinschreibung unterschieden.
Erweiterte Eigenschaften	<p>Liste der erweiterten Eigenschaften, die nur für die Spark-Engine gelten. Die erweiterten Eigenschaften enthalten eine Liste der Standardeigenschaften.</p> <p>Sie haben die Möglichkeit, Laufzeiteigenschaften für die Hadoop-Umgebung im Datenintegrationsdienst, in der Hadoop-Verbindung und im Mapping zu konfigurieren. Eine auf einer hohen Ebene konfigurierte Eigenschaft können Sie durch Festlegen des Werts auf einer unteren Ebene überschreiben. Wenn Sie z. B. eine Eigenschaft in den benutzerdefinierten Eigenschaften des Datenintegrationsdiensts konfigurieren, können Sie diese in der Hadoop-Verbindung oder im Mapping überschreiben. Der Datenintegrationsdienst verarbeitet Überschreibungen von Eigenschaften auf der Grundlage der folgenden Prioritäten:</p> <ol style="list-style-type: none"> 1. Zuordnung der mit dem Befehl <code>infacmd ms runMapping</code> und der Option <code>-cp</code> festgelegten benutzerdefinierten Eigenschaften 2. Zuordnung der Laufzeiteigenschaften für die Hadoop-Umgebung 3. Erweiterte Eigenschaften der Hadoop-Verbindung für Laufzeit-Engines 4. Erweiterte allgemeine Eigenschaften, Umgebungsvariablen und Klassenpfade der Hadoop-Verbindung 5. Benutzerdefinierte Eigenschaften des Datenintegrationsdiensts <p>Hinweis: Wenn eine Zuordnung Hive-Server 2 zum Ausführen eines Jobs oder von Teilen eines Jobs verwendet, können Sie keine Eigenschaften überschreiben, die auf Cluster-Ebene in PreSQL- oder Post-SQL-Abfragen oder SQL-Überschreibungsanweisungen konfiguriert sind. Problemumgehung: Statt die Clusterkonfiguration in der Domäne zum Überschreiben von Cluster-Eigenschaften zu verwenden, übergeben Sie die Überschreibungseinstellungen an die JDBC-URL. Beispiel: <code>beeline -u "jdbc:hive2://<domain host>:<port_number>/tpch_text_100" --hiveconf hive.execution.engine=tez</code></p> <p>Hinweis: Bevor Sie sich nicht in der Drittanbieter- und Informatica-Dokumentation oder beim globalen Kundensupport von Informatica entsprechend informiert haben, rät Informatica von der Änderung dieser Eigenschaftswerte ab. Wenn Sie einen Wert ohne Kenntnis der Eigenschaft ändern, kann es zu Leistungseinbußen oder anderen unerwarteten Ergebnissen kommen.</p>

HBase-Verbindungseigenschaften

Verwenden Sie eine HBase-Verbindung für den Zugriff auf HBase. Die HBase-Verbindung ist eine NoSQL-Verbindung. Sie können eine HBase-Verbindung im Administrator Tool oder im Developer Tool erstellen und verwalten. HBase-Verbindungseigenschaften unterscheiden zwischen Groß- und Kleinschreibung, sofern nicht anders angegeben.

In der folgenden Tabelle werden die Eigenschaften von HBase-Verbindungen erläutert:

Eigenschaft	Beschreibung
Name	Der Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung ändern. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
ID	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 4.000 Zeichen enthalten.
Speicherort	Die Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Der Verbindungstyp. Wählen Sie HBase.
Datenbanktyp	Der Typ der Datenbank, mit der eine Verbindung hergestellt werden soll. Wählen Sie HBase , um eine Verbindung für eine HBase-Tabelle herzustellen.

HDFS- oder ViewFS-Verbindungseigenschaften

Verwenden Sie eine HDFS-Verbindung (Hadoop File System) bzw. eine ViewFS-Verbindung (View File System) zum Zugriff auf Daten im Hadoop-Cluster. Die HDFS- oder ViewFS-Verbindung ist ein Dateisystem-Verbindungstyp. Sie können eine HDFS- oder ViewFS-Verbindung im Administrator Tool, im Analyst Tool oder im Developer Tool erstellen und verwalten. HDFS- oder ViewFS-Verbindungseigenschaften unterscheiden zwischen Groß- und Kleinschreibung, sofern nicht anders angegeben.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Eigenschaften von HDFS-Verbindungen erläutert:

Eigenschaft	Beschreibung
Name	Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
ID	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Die Domäne, in der Sie die Verbindung erstellen möchten. Nicht gültig für das Analyst-Tool.
Typ	Der Verbindungstyp. Die Standardeinstellung ist Hadoop-Dateisystem.
Benutzername	Benutzername für den Zugriff auf HDFS.
NameNode URI	Der URI für den Zugriff auf das Speichersystem. Der Wert für <code>fs.defaultFS</code> befindet sich im Konfigurationssatz <code>core-site.xml</code> der Cluster-Konfiguration. Wenn Sie beim Importieren der Cluster-Konfiguration Verbindungen erstellen, wird die NameNode-URI-Eigenschaft standardmäßig aufgefüllt und jedes Mal aktualisiert, wenn Sie die Cluster-Konfiguration aktualisieren. Wenn Sie einen Cloudera CDP Public Cloud-Computing-Cluster verwenden und sich das HDFS in einem Cloudera Data Lake-Cluster befindet, legen Sie die Eigenschaft <code>spark.yarn.access.hadoopFileSystems</code> in den Spark-Eigenschaften der Hadoop-Verbindung auf den gleichen Wert wie hier festgelegt fest.

Zugreifen auf mehrere Speichertypen

Verwenden Sie die NameNode-URI-Eigenschaft in den Verbindungsparametern, um eine Verbindung mit verschiedenen Speichertypen herzustellen. In der folgenden Tabelle sind der Speichertyp und das NameNode-URI-Format für den Speichertyp aufgeführt:

Speicher	NameNode-URI-Format
HDFS	<code>hdfs://<namenode>:<port></code> Dabei gilt Folgendes: - <code><namenode></code> ist der Hostname bzw. die IP-Adresse von NameNode. - <code><port></code> ist der Port, den NameNode auf Remoteprozeduraufrufe (RPC) abhört. <code>hdfs://<nameservice></code> im Falle einer NameNode-Hochverfügbarkeit.
View File System (ViewFS)	<code>viewfs://<clusterX></code> , wobei <code>clusterX</code> die Mount-Tabelle für den Cluster ist.
MapR-FS	<code>maprfs:///</code>

Speicher	NameNode-URI-Format
WASB in HDInsight	<p>wasb://<container_name>@<account_name>.blob.core.windows.net/<path></p> <p>Dabei gilt Folgendes:</p> <ul style="list-style-type: none"> - <Containername> identifiziert einen spezifischen Azure Storage Blob-Container. <p>Hinweis: <Containername> ist optional.</p> <ul style="list-style-type: none"> - <Kontoname> identifiziert das Azure Storage Blob-Objekt. <p>Beispiel:</p> <p>wasb://infabdmoffering1storage.blob.core.windows.net/infabdmoffering1cluster/mr-history</p>
ADLS in HDInsight	adl://home

Wenn Sie eine Clusterkonfiguration anhand eines Azure-HDInsight-Clusters erstellen, verwendet die Clusterkonfiguration entweder ADLS oder WASB als primären Speicher. Sie können keine Cluster-Konfiguration mit ADLS oder WASB als sekundärem Speicher erstellen. Sie können die NameNode-URI-Eigenschaft in der HDFS- oder ViewFS-Verbindung bearbeiten, um eine Verbindung mit einem lokalen HDFS- oder ViewFS-Speicherort herzustellen.

HBase-Verbindungseigenschaften für MapR-DB

Verwenden Sie eine HBase-Verbindung, um eine Verbindung zu einer MapR-DB-Tabelle herzustellen. Die HBase-Verbindung ist eine NoSQL-Verbindung. Sie können eine HBase-Verbindung im Administrator Tool oder im Developer Tool erstellen und verwalten. HBase-Verbindungseigenschaften unterscheiden zwischen Groß- und Kleinschreibung, sofern nicht anders angegeben.

In der folgenden Tabelle werden die HBase-Verbindungseigenschaften für MapR-DB beschrieben:

Eigenschaft	Beschreibung
Name	<p>Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung ändern. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten:</p> <p>~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /</p>
ID	<p>Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.</p>
Beschreibung	<p>Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 4.000 Zeichen enthalten.</p>
Speicherort	<p>Die Domäne, in der Sie die Verbindung erstellen möchten.</p>
Typ	<p>Verbindungstyp. Wählen Sie HBase aus.</p>

Eigenschaft	Beschreibung
Datenbanktyp	Der Typ der Datenbank, mit der eine Verbindung hergestellt werden soll. Wählen Sie MapR-DB aus, um eine Verbindung für eine MapR-DB-Tabelle herzustellen.
Cluster-Konfiguration	Der Name der mit der Hadoop-Umgebung verknüpften Cluster-Konfiguration.
MapR-DB-Datenbankpfad	<p>Der Datenbankpfad mit der MapR-DB-Tabelle, mit der eine Verbindung hergestellt werden soll. Geben Sie einen gültigen MapR-Clusterpfad ein.</p> <p>Wenn Sie ein HBase-Datenobjekt für MapR-DB erstellen, können Sie nur Tabellen durchsuchen, die in dem MapR-DB-Pfad vorhanden sind, den Sie im Feld-Datenbankpfad angeben. Sie können nicht auf Tabellen zugreifen, die in Unterverzeichnissen im angegebenen Pfad verfügbar sind.</p> <p>Wenn Sie z. B. den Pfad als <code>/user/customers/</code> angeben, können Sie auf die Tabellen im Verzeichnis <code>customers</code> zugreifen. Wenn das Verzeichnis <code>customers</code> jedoch ein Unterverzeichnis mit dem Namen <code>regions</code> enthält, können Sie nicht auf die Tabellen im folgenden Verzeichnis zugreifen:</p> <p><code>/user/customers/regions</code></p>

Hive-Verbindungseigenschaften

Verwenden Sie die Hive-Verbindung, um auf Hive-Daten zuzugreifen. Eine Hive-Verbindung ist ein Datenbank-Verbindungstyp. Sie können eine Hive-Verbindung im Administrator Tool, im Analyst Tool oder im Developer Tool erstellen und verwalten. Hive-Verbindungseigenschaften unterscheiden zwischen Groß- und Kleinschreibung, sofern nicht anders angegeben.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Eigenschaften von Hive-Verbindungseigenschaften erläutert:

Eigenschaft	Beschreibung
Name	Der Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung ändern. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
ID	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 4000 Zeichen enthalten.
Speicherort	Die Domäne, in der Sie die Verbindung erstellen möchten. Nicht gültig für das Analyst Tool.

Eigenschaft	Beschreibung
Typ	Der Verbindungstyp. Wählen Sie „Hive“ aus.
LDAP-Benutzername	<p>LDAP-Benutzername, den der Datenintegrationsdienst zum Ausführen von Zuordnungen in einem Hadoop-Cluster verwendet. Der Benutzername richtet sich nach der JDBC-Verbindungszeichenfolge, die Sie in der Metadaten- oder Datenzugriffs-Verbindungszeichenfolge für die native Umgebung angegeben haben.</p> <p>Wenn der Hadoop-Cluster Kerberos-Authentifizierung verwendet, müssen der Prinzipalname der JDBC-Verbindungszeichenfolge und der Benutzername identisch sein. Andernfalls hängt der Benutzername vom Verhalten des JDBC-Treibers ab. Mit dem Hive-JDBC-Treiber können Sie einen Benutzernamen auf viele Arten angeben. Der Benutzername kann zudem Teil der JDBC-URL werden.</p> <p>Wenn der Hadoop-Cluster keine Kerberos-Authentifizierung verwendet, hängt der Benutzername vom Verhalten des JDBC-Treibers ab.</p> <p>Wenn Sie keinen Benutzernamen eingeben, authentifiziert der Hadoop-Cluster Jobs basierend auf den folgenden Kriterien:</p> <ul style="list-style-type: none"> - Der Hadoop-Cluster verwendet keine Kerberos-Authentifizierung. Er authentifiziert Jobs basierend auf dem Benutzernamen des Betriebssystemprofils des Computers, auf dem der Datenintegrationsdienst ausgeführt wird. - Der Hadoop-Cluster verwendet Kerberos-Authentifizierung. Er authentifiziert Jobs basierend auf dem SPN des Datenintegrationsdiensts. Der LDAP-Benutzername wird ignoriert.
Passwort	Passwort für den LDAP-Benutzernamen.
Umgebungs-SQL	<p>SQL-Befehle zum Einrichten der Hadoop-Umgebung. Im nativen Umgebungstyp führt der Datenintegrationsdienst die Umgebungs-SQL jedes Mal aus, wenn er eine Verbindung zu einem Hive-Metastore herstellt. Wenn Sie die Hive-Verbindung zum Ausführen von Profilen in einem Hadoop-Cluster verwenden, führt der Datenintegrationsdienst die Umgebungs-SQL am Anfang jeder Hive-Sitzung aus.</p> <p>Die folgenden Regeln und Richtlinien gelten für die Verwendung von Umgebungs-SQL in beiden Verbindungsmodi:</p> <ul style="list-style-type: none"> - Verwenden Sie die Umgebungs-SQL, um Hive-Abfragen anzugeben. - Verwenden Sie die Umgebungs-SQL, um den Klassenpfad für benutzerdefinierte Hive-Funktionen einzustellen, und verwenden Sie dann Umgebungs-SQL oder PreSQL, um die benutzerdefinierten Hive-Funktionen anzugeben. Sie können PreSQL nicht in den Datenobjekteigenschaften zur Angabe des Klassenpfads verwenden. Wenn Sie benutzerdefinierte Hive-Funktionen verwenden, müssen Sie die JAR-Dateien in das folgende Verzeichnis kopieren: <pre><Informatica-Installationsverzeichnis>/services/shared/hadoop/<Name der Hadoop-Distribution>/extras/hive-auxjars</pre> <ul style="list-style-type: none"> - Sie können Umgebungs-SQL zum Definieren von Hadoop- oder Hive-Parametern verwenden, die Sie in den PreSQL-Befehlen oder in benutzerspezifischen Abfragen nutzen möchten. - Wenn Sie mehrere Werte für die Eigenschaft „Umgebungs-SQL“ verwenden, stellen Sie sicher, dass sich zwischen den Werten keine Leerzeichen befinden.
SQL-Kennungszeichen	<p>Der Zeichentyp, der zur Kennzeichnung von Sonderzeichen und reservierten SQL-Schlüsselwörtern, wie WHERE, verwendet wird. Der Datenintegrationsdienst schließt mit dem ausgewählten Zeichen Sonderzeichen und reservierte SQL-Schlüsselwörter ein. Außerdem nutzt der Datenintegrationsdienst dieses Zeichen für die Eigenschaft Unterstützte Kennungen für gemischte Groß-/Kleinschreibung.</p>

Eigenschaften für den Zugriff auf Hive als Quelle oder Ziel

Die folgende Tabelle beschreibt die Verbindungseigenschaften, die Sie konfigurieren, um auf Hive als Quelle oder Ziel zuzugreifen:

Eigenschaft	Beschreibung
JDBC-Treiberklassenname	Name der Hive JDBC-Treiberklasse. Wenn Sie diese Option leer lassen, verwendet das Developer Tool den standardmäßigen Apache Hive JDBC-Treiber, der mit der Verteilung ausgeliefert wird. Wenn der standardmäßige Apache Hive JDBC-Treiber nicht Ihren Anforderungen entspricht, können Sie den Apache Hive JDBC-Treiber mit einem Drittanbieter-Hive JDBC-Treiber überschreiben, indem Sie den Treiberklassennamen angeben.
Metadaten-Verbindungszeichenfolge	<p>Die JDBC-Verbindungs-URI für den Zugriff auf die Metadaten des Hadoop-Servers. Sie können PowerExchange for Hive zum Kommunizieren mit einem HiveServer-Dienst oder mit einem HiveServer2-Dienst verwenden. Zum Herstellen einer Verbindung zu HiveServer geben Sie den Verbindungsstring im folgenden Format ein:</p> <pre>jdbc:hive2://<hostname>:<port>/<db></pre> <p>Wobei</p> <ul style="list-style-type: none">- <hostname> der Name bzw. die IP-Adresse des Computers ist, auf dem HiveServer2 ausgeführt wird.- <port> die Nummer des Ports ist, den der HiveServer2 abhört.- <db> der Name der Datenbank ist, zu der Sie eine Verbindung herstellen möchten. Wenn Sie den Datenbanknamen nicht zur Verfügung stellen, verwendet der Datenintegrationsdienst die standardmäßigen Datenbank-Details. <p>Zum Herstellen einer Verbindung zu HiveServer2 verwenden Sie das Verbindungsstringformat, das Apache Hive für diese bestimmte Hadoop-Distribution implementiert. Weitere Informationen über Apache Hive-Verbindungsstringformate finden Sie in der Apache Hive-Dokumentation.</p> <p>Für den Benutzeridentitätswechsel müssen Sie <code>hive.server2.proxy.user=<xyz></code> zum JDBC-Verbindungs-URI hinzufügen. Wenn Sie den Benutzeridentitätswechsel nicht konfigurieren, werden die Anmeldeinformationen des aktuellen Benutzers verwendet, um eine Verbindung zum HiveServer2 herzustellen.</p> <p>Wenn der Hadoop-Cluster die SSL- oder TLS-Authentifizierung verwendet, müssen Sie dem JDBC-Verbindungs-URI <code>ssl=true</code> hinzufügen. Beispiel: <code>jdbc:hive2://<hostname>:<port>/<db>;ssl=true</code></p> <p>Wenn Sie für die SSL- oder TLS-Authentifizierung ein selbstsigniertes Zertifikat verwenden, vergewissern Sie sich, dass die Zertifikatsdatei auf dem Client-Computer und dem Datenintegrationsdienst-Computer verfügbar ist. Weitere Informationen hierzu finden Sie im <i>Data Engineering Integration-Handbuch</i>.</p>
Hive-JDBC-Server umgehen	<p>JDBC-Treibermodus. Aktivieren Sie das Kontrollkästchen, um den eingebetteten JDBC-Treibermodus zu verwenden.</p> <p>Zur Verwendung des eingebetteten JDBC-Modus führen Sie folgende Aufgaben durch:</p> <ul style="list-style-type: none">- Stellen Sie sicher, dass Hive-Client und Informatica-Dienste auf demselben Computer installiert sind.- Konfigurieren Sie die Eigenschaften der Hive-Verbindung, um Zuordnungen in einem Hadoop-Cluster auszuführen. <p>Wenn Sie den nicht eingebetteten Modus wählen, müssen Sie den Verbindungszeichenfolge für Datenzugriff konfigurieren.</p> <p>Informatica empfiehlt die Verwendung des eingebetteten JDBC-Modus.</p>

Eigenschaft	Beschreibung
Differenzierte Autorisierung	<p>Wenn Sie die Option zum Berücksichtigen der differenzierten Autorisierung in einer Hive-Quelle auswählen, wird beim Mapping Folgendes berücksichtigt:</p> <ul style="list-style-type: none"> - Einschränkungen auf Zeilen- und Spaltenebene. Anwendung auf Hadoop-Cluster, in denen die Sicherheitsmodi „Sentry“ oder „Ranger“ aktiviert sind. - Datenmaskierungsregeln. Anwendung auf festgelegte Maskierungsregeln bei Spalten, die sensible Daten per Dynamic Data Masking enthalten. <p>Wenn Sie die Option nicht auswählen, ignorieren die Blaze- und die Spark-Engine die Einschränkungen und Maskierungsregeln, sodass die Ergebnisse eingeschränkte oder sensible Daten enthalten.</p>
Verbindungszeichenfolge für Datenzugriff	<p>Die Verbindungszeichenfolge zum Zugriff auf Daten aus dem Hadoop-Datenspeicher. Zum Herstellen einer Verbindung zu HiveServer geben Sie den Verbindungsstring des nicht eingebetteten JDBC-Modus im folgenden Format ein:</p> <pre>jdbc:hive2://<hostname>:<port>/<db></pre> <p>Wobei</p> <ul style="list-style-type: none"> - <hostname> der Name bzw. die IP-Adresse des Computers ist, auf dem HiveServer2 ausgeführt wird. - <port> die Nummer des Ports ist, den der HiveServer2 abhört. - <db> die Datenbank ist, zu der Sie eine Verbindung herstellen möchten. Wenn Sie den Datenbanknamen nicht zur Verfügung stellen, verwendet der Datenintegrationsdienst die standardmäßigen Datenbank-Details. <p>Zum Herstellen einer Verbindung zu HiveServer2 verwenden Sie das Verbindungsstringformat, das Apache Hive für die spezifische Hadoop-Verteilung implementiert. Weitere Informationen über Apache Hive-Verbindungsstringformate finden Sie in der Apache Hive-Dokumentation.</p> <p>Für den Benutzeridentitätswechsel müssen Sie <code>hive.server2.proxy.user=<xyz></code> zum JDBC-Verbindungs-URI hinzufügen. Wenn Sie den Benutzeridentitätswechsel nicht konfigurieren, werden die Anmeldeinformationen des aktuellen Benutzers verwendet, um eine Verbindung zum HiveServer2 herzustellen.</p> <p>Wenn der Hadoop-Cluster die SSL- oder TLS-Authentifizierung verwendet, müssen Sie dem JDBC-Verbindungs-URI <code>ssl=true</code> hinzufügen. Beispiel: <code>jdbc:hive2://<hostname>:<port>/<db>;ssl=true</code></p> <p>Wenn Sie für die SSL- oder TLS-Authentifizierung ein selbstsigniertes Zertifikat verwenden, vergewissern Sie sich, dass die Zertifikatsdatei auf dem Client-Computer und dem Datenintegrationsdienst-Computer verfügbar ist. Weitere Informationen hierzu finden Sie im <i>Data Engineering Integration-Handbuch</i>.</p>
Hive-Staging-Verzeichnis auf HDFS	<p>HDFS-Verzeichnis für Hive-Staging-Tabellen. Sie müssen dem Hadoop-Identitätswechselbenutzer und den Mapping-Identitätswechselbenutzern die Ausführungsberechtigung gewähren.</p> <p>Diese Option ist anwendbar und erforderlich, wenn Sie Daten in ein Hive-Ziel in der nativen Umgebung schreiben.</p>
Name der Hive-Staging-Datenbank	<p>Namespace für Hive-Staging-Tabellen.</p> <p>Der Name der Hive-Staging-Datenbank wird automatisch anhand der Verbindungszeichenfolge für den Datenzugriff aktualisiert. Wenn Sie den Standardnamen überschreiben möchten, müssen Sie den Namen der Hive-Staging-Datenbank in der Hive-Verbindung konfigurieren.</p> <p>Diese Option ist relevant, wenn Sie Mappings in der nativen Umgebung ausführen, um Daten in ein Hive-Ziel zu schreiben.</p> <p>Wenn Sie Mappings auf der Blaze- oder Spark-Engine ausführen, ist es nicht erforderlich, den Namen der Hive-Staging-Datenbank in der Hive-Verbindung zu konfigurieren. Der Datenintegrationsdienst verwendet den Wert, den Sie in der Hadoop-Verbindung konfigurieren.</p>

HTTP-Verbindungseigenschaften

Verwenden Sie eine HTTP-Verbindung, um eine Verbindung von einer REST-Webdienst-Verbraucher-Umwandlung zu einem Webdienst herzustellen. Die HTTP-Verbindung ist ein Web-Verbindungstyp. Sie erstellen eine HTTP-Verbindung im Developer Tool. Sie können eine HTTP-Verbindung im Administrator Tool oder im Developer Tool verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Eigenschaften von HTTP-Verbindungen erläutert:

Eigenschaft	Beschreibung
Name	Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
ID	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Benutzername	Benutzername, der mit dem Web-Dienst verbunden werden soll. Geben Sie einen Benutzernamen ein, wenn Sie die HTTP-Authentifizierung oder die WS-Security aktiviert haben. Wenn die Web-Dienst-Verbraucher-Umwandlung WS-Security-Ports enthält, erhält die Umwandlung einen dynamischen Benutzernamen durch einen Eingangsport. Der Datenintegrationsdienst überschreibt den Benutzernamen, der in der Verbindung definiert ist.
Passwort	Passwort für den Benutzernamen. Geben Sie ein Passwort ein, wenn Sie die HTTP-Authentifizierung oder die WS-Security aktiviert haben. Wenn die Web-Dienst-Verbraucher-Umwandlung WS-Security-Ports enthält, erhält die Umwandlung ein dynamisches Passwort durch einen Eingangsport. Der Datenintegrationsdienst überschreibt das Passwort, das in der Verbindung definiert ist.
Endpunkt-URL	URL für den Web-Dienst, auf den zugegriffen werden soll. Der Datenintegrationsdienst überschreibt die URL, die in der WSDL-Datei definiert ist. Wenn die Web-Dienst-Verbraucher-Umwandlung einen Endpunkt-URL-Port enthält, erhält die Umwandlung die URL durch einen Eingangsport. Der Datenintegrationsdienst überschreibt die URL, die in der Verbindung definiert ist.
Timeout	Dauer in Sekunden, die der Datenintegrationsdienst auf eine Antwort vom Webdienst-Provider wartet, ehe die Verbindung geschlossen wird. Geben Sie einen Timeout-Wert zwischen 1 und 10.000 Sekunden an.

Eigenschaft	Beschreibung
HTTP-Authentifizierungstyp	<p>Art der Benutzer-Authentifizierung via HTTP. Wählen Sie einen der folgenden Werte aus:</p> <ul style="list-style-type: none"> - Keine. Keine Authentifizierung. - Automatisch. Der Datenintegrationsdienst wählt den Authentifizierungstyp, den der Webdienst-Provider verwendet. - Basis Sie müssen der Domäne des Webdienst-Providers einen Benutzernamen und ein Passwort bereitstellen. Der Datenintegrationsdienst sendet den Benutzernamen und das Passwort zur Authentifizierung an den Webdienst-Provider. - zusammengefasst Sie müssen der Domäne des Webdienst-Providers einen Benutzernamen und ein Passwort bereitstellen. Der Datenintegrationsdienst generiert eine verschlüsselte Meldungszusammenfassung aus dem Benutzernamen und dem Passwort und sendet diese an den Webdienst-Provider. Der Provider generiert einen temporären Wert für den Benutzernamen und das Passwort und speichert diesen in seinem Active Directory auf dem Domänen-Controller. Er vergleicht den Wert mit der Meldungszusammenfassung. Wenn beide übereinstimmen, authentifiziert Sie der Webdienst-Provider. - NTLM Sie müssen einen Domänennamen, einen Servernamen oder einen Standardbenutzernamen und ein Passwort bereitstellen. Der Webdienst-Provider authentifiziert Sie anhand der Domäne, mit der Sie verbunden sind. Er erhält den Benutzernamen und das Passwort vom Windows Domain Controller und vergleicht sie mit dem Benutzernamen und Passwort, das Sie bereitgestellt haben. Wenn beide übereinstimmen, authentifiziert Sie der Webdienst-Provider. Bei der NTLM-Authentifizierung werden keine verschlüsselten Passwörter im Active Directory des Domain Controllers gespeichert.
Trust-Zertifikatsdatei	<p>Die Datei enthält ein Bundle aus vertrauenswürdigen Zertifikaten, die der Datenintegrationsdienst verwendet, wenn er das SSL-Zertifikat des Web-Dienstes authentifiziert. Geben Sie den Dateinamen und den kompletten Verzeichnispfad ein.</p> <p>Voreinstellung ist <Informatica-Installationsverzeichnis>/services/shared/bin/ca-bundle.crt.</p>
Dateiname des Clientzertifikats	<p>Clientzertifikat, das der Web-Dienst verwendet, um einen Client zu authentifizieren. Geben Sie die Clientzertifikatsdatei an, wenn der Web-Dienst den Datenintegrationsdienst authentifizieren muss.</p>
Passwort des Clientzertifikats	<p>Passwort des Clientzertifikats Geben Sie das Passwort des Clientzertifikats an, wenn der Web-Dienst den Datenintegrationsdienst authentifizieren muss.</p>
Clientzertifikat - Typ	<p>Format der Clientzertifikatsdatei. Wählen Sie einen der folgenden Werte aus:</p> <ul style="list-style-type: none"> - PEM. Dateien mit der Dateiendung .pem. - DER. Dateien mit der Dateiendung .cer oder .der <p>Geben Sie den Clientzertifikatstyp an, wenn der Webdienst den Datenintegrationsdienst authentifizieren muss.</p>
Dateiname des privaten Schlüssels	<p>Der private Schlüssel für das Clientzertifikat. Geben Sie den Dateinamen des privaten Schlüssels an, wenn der Web-Dienst den Datenintegrationsdienst authentifizieren muss.</p>
Passwort des privaten Schlüssels	<p>Passwort für den privaten Schlüssel des Clientzertifikats. Geben Sie das Passwort des privaten Schlüssels an, wenn der Web-Dienst den Datenintegrationsdienst authentifizieren muss.</p>
Privater Schlüssel - Typ	<p>Typ des privaten Schlüssels. Der unterstützte Typ ist PEM.</p>

Eigenschaften von IBM DB2-Verbindungen

Verwenden Sie eine IBM DB2-Verbindung für den Zugriff auf IBM DB2. Eine IBM DB2-Verbindung ist eine relationale Datenbankverbindung. Sie können eine IBM DB2-Verbindung im Administrator tool, Developer tool oder Analyst Tool erstellen und verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die DB2-Verbindungseigenschaften beschrieben:

Eigenschaft	Beschreibung
Datenbanktyp	Der Datenbanktyp.
Name	Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
ID	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Benutzername	Der Benutzername der Datenbank.
Passwort	Das Passwort für den Benutzernamen der Datenbank.
Pass-Through-Sicherheit aktiviert	Aktiviert Pass-Through-Sicherheit für die Verbindung. Wenn Sie Pass-Through-Sicherheit für eine Verbindung aktivieren, verwendet die Domäne nicht die im Verbindungsobjekt definierten Anmeldeinformationen, sondern den Benutzernamen und das Passwort des Clients, um sich an der entsprechenden Datenbank anzumelden.
Verbindungszeichenfolge für den Datenzugriff	DB2-Verbindungs-URL für den Zugriff auf Metadaten in der Datenbank. dbname Wobei <code>dbname</code> der im DB2-Client konfigurierte Alias ist.

Eigenschaft	Beschreibung
Eigenschaften für den Metadaten-Zugriff: Verbindungszeichenfolge	<p>Verwenden Sie die folgende URL für die Verbindungszeichenfolge für Metadaten:</p> <pre>jdbc:informatica:db2:// <Hostname>:<Port>;DatabaseName=<Datenbankname></pre> <p>Beim Importieren einer Tabelle werden standardmäßig alle Tabellennamen unterhalb des Namens des Standardschemas angezeigt. Um Tabellen unterhalb eines bestimmten Schemas anstelle des Standardschemas anzuzeigen, können Sie den Namen des Schemas angeben, aus dem Sie die Tabelle importieren möchten. Schließen Sie den Parameter „ischemaName“ in die URL ein, um den Schemanamen anzugeben. Beispiel: Mit der folgenden Syntax wird eine Tabelle aus einem bestimmten Schema importiert:</p> <pre>jdbc:informatica:db2:// <Hostname>:<Port>;DatabaseName=<Datenbankname>;ischemaName=<Schema_Name></pre> <p>Um eine Tabelle in mehreren Schemas zu suchen und zu importieren, können Sie die Namen mehrerer Schemas im Parameter „ischemaName“ festlegen. Beim Namen eines Schemas wird die Groß-/Kleinschreibung beachtet. Wenn Sie mehrere Schemanamen angeben, können Sie keine Sonderzeichen verwenden. Trennen Sie Schemanamen durch senkrechte Striche () voneinander. Beispiel: Mit der folgenden Syntax können Sie eine Tabelle in drei Schemas suchen und importieren:</p> <pre>jdbc:informatica:db2:// <Hostname>:<Port>;DatabaseName=<Datenbankname>;ischemaName=<schema_name1> <schema_name2> <schema_name3></pre> <p>Wenn Sie mehrere Schemanamen angeben, müssen Sie die Option Nur Standardschema anzeigen deaktivieren, um die Tabellen unter dem angegebenen Schemanamen anzuzeigen.</p>

Eigenschaft	Beschreibung
AdvancedJDBCSecurityOptions	<p>Datenbankparameter für Metadata-Zugriff auf eine sichere Datenbank. Informatica behandelt den Wert des AdvancedJDBCSecurityOptions-Felds als vertrauliche Daten und speichert die Parameterzeichenfolge als Verschlüsselung.</p> <p>Um eine Verbindung zu einer sicheren Datenbank herzustellen, beziehen Sie die folgenden Parameter mit ein:</p> <ul style="list-style-type: none"> - EncryptionMethod. Erforderlich. Gibt an, ob Daten bei der Netzwerkübertragung verschlüsselt werden. Dieser Parameter muss auf SSL festgelegt werden. - ValidateServerCertificate. Optional. Gibt an, ob Informatica das Zertifikat validiert, das vom Datenbankserver gesendet wird. <p>Wenn dieser Parameter auf TRUE festgelegt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat. Wenn Sie den HostNameInCertificate-Parameter angeben, validiert Informatica ebenfalls den Hostnamen im Zertifikat.</p> <p>Wenn dieser Parameter auf "false" festgelegt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat nicht. Informatica ignoriert alle Truststore-Informationen, die Sie angeben.</p> <ul style="list-style-type: none"> - HostNameInCertificate. Optional. Hostname des Computers, auf dem die sichere Datenbank gehostet wird. Wenn Sie einen Hostnamen angeben, validiert Informatica den Hostnamen in der Verbindungszeichenfolge mit dem Hostnamen im SSL-Zertifikat. - cryptoProtocolVersion. Optional. Wenn Sie TLS für die IBM DB2-Instanz aktivieren, legen Sie den Parameter cryptoProtocolVersion wie folgt fest: cryptoProtocolVersion=TLSv<version number>. Beispiel: cryptoProtocolVersion=TLSv1.2 <p>Hinweis: Die Versionsnummer muss mit der TLS-Version übereinstimmen, die für den Server konfiguriert wurde.</p> <ul style="list-style-type: none"> - TrustStore. Erforderlich. Pfad und Dateiname der Truststore-Datei. <p>Hinweis: Wenn Sie SSL oder TLS konfigurieren und nur den Dateinamen angeben, müssen Sie die Truststore-Datei in das folgende Verzeichnis kopieren, um die Verbindung zu testen: <Informatica server installation directory>/tomcat/bin</p> <ul style="list-style-type: none"> - TrustStorePassword Erforderlich. Passwort der Truststore-Datei für die sichere Datenbank. <p>Hinweis: Informatica hängt die sichere JDBC-Parameter an die Verbindungszeichenfolge an. Wenn Sie die sicheren JDBC-Parameter direkt in der Verbindungszeichenfolge einschließen, geben Sie keinen Parameter in das Feld AdvancedJDBCSecurityOptions ein.</p>
Eigenschaften für den Datenzugriff: Verbindungszeichenfolge	<p>Die Verbindungszeichenfolge für den Zugriff auf Daten in der Datenbank.</p> <p>Für IBM DB2 ist dies <Datenbankname></p>
Codepage	<p>Die Codepage, die zum Lesen aus einer Quelldatenbank oder zum Schreiben in eine Zieldatenbank oder Zielfeld verwendet wird.</p>
Umgebungs-SQL	<p>SQL-Befehle zum Einrichten der Datenbankumgebung beim Herstellen einer Verbindung zur Datenbank. Der Datenintegrationsdienst führt die Verbindungsumgebungs-SQL bei jeder Verbindung mit der Datenbank aus.</p>
Transaktions-SQL	<p>SQL-Befehle zum Einrichten der Datenbankumgebung beim Herstellen einer Verbindung zur Datenbank. Der Datenintegrationsdienst führt die Verbindungsumgebungs-SQL zu Beginn jeder Transaktion aus.</p>
Wiederholungszeitraum	<p>Diese Eigenschaft ist für die zukünftige Verwendung reserviert.</p>

Eigenschaft	Beschreibung
Tablespace	Der Tablespace-Name der Datenbank.
SQL-Bezeichnerzeichen	<p>Art des Zeichens, das von der Datenbank verwendet wird, um Delimiter-IDs in SQL-Abfragen einzuschließen. Die verfügbaren Zeichen richten sich nach dem Datenbanktyp.</p> <p>Wählen Sie (Keine) aus, wenn die Datenbank reguläre IDs verwendet. Wenn der Datenintegrationsdienst SQL-Abfragen erzeugt, schließt der Dienst IDs nicht in Delimiter-Zeichen ein.</p> <p>Wählen Sie ein Zeichen aus, wenn die Datenbank Delimiter-IDs verwendet. Wenn der Datenintegrationsdienst SQL-Abfragen erzeugt, schließt der Dienst Delimiter-IDs in dieses Zeichen ein.</p>
Bezeichner mit gemischter Groß-/Kleinschreibung unterstützen	<p>Aktivieren Sie diese Eigenschaft, wenn die Datenbank IDs für gemischte Groß-/Kleinschreibung verwendet. Bei aktivierter Eigenschaft schließt der Datenintegrationsdienst alle IDs innerhalb des Zeichens ein, das für die Eigenschaft SQL-Kennungszeichen ausgewählt wurde.</p> <p>Wenn die Eigenschaft SQL-Kennungszeichen auf „Kein“ festgelegt ist, wird die Eigenschaft Unterstützte IDs für gemischte Groß-/Kleinschreibung deaktiviert.</p>
ODBC-Provider	<p>ODBC. Der Datenbanktyp, zu dem ODBC eine Verbindung herstellt. Geben Sie zur Pushdown-Optimierung den Datenbanktyp an, damit der Datenintegrationsdienst die native Datenbank-SQL generieren kann. Mögliche Werte:</p> <ul style="list-style-type: none"> - Andere - Sybase - Microsoft_SQL_Server <p>Standardwert ist „Andere“.</p>

Eigenschaften von IBM DB2 for i5/OS-Verbindungen

Verwenden Sie eine IBM DB2 for i5/OS -Verbindung für den Zugriff auf Tabellen in IBM DB2 for i5/OS. Eine IBM DB2 for i5/OS-Verbindung ist ein relationaler Datenbank-Verbindungstyp. Sie können eine IBM DB2 for i5/OS-Verbindung im Administrator Tool oder im Developer Tool erstellen und verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Eigenschaften von DB2 for i5/OS-Verbindungen erläutert:

Eigenschaft	Beschreibung
Name	<p>Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten:</p> <p>~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /</p>
ID	<p>Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.</p>

Eigenschaft	Beschreibung
Beschreibung	Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 255 Zeichen enthalten.
Verbindungstyp	Der Verbindungstyp (DB2I).
Benutzername	Ein Datenbank-Benutzername.
Passwort	<p>Ein Passwort für den angegebenen Benutzernamen oder eine gültige PowerExchange-Passphrase.</p> <p>Eine PowerExchange-Passphrase kann zwischen 9 und 31 Zeichen lang sein und die folgenden Zeichen enthalten:</p> <ul style="list-style-type: none"> - Groß- und Kleinbuchstaben - Die Zahlen 0 bis 9 - Leerzeichen - Die folgenden Sonderzeichen: ' - ; # \ , . / ! % & * () _ + { } : @ < > ? <p>Hinweis: Das erste Zeichen ist ein Apostroph.</p> <p>Passphrasen dürfen keine einfachen Anführungszeichen ('), doppelten Anführungszeichen (") oder Währungssymbole enthalten.</p> <p>Stellen Sie vor der Verwendung von Passphrasen sicher, dass der PowerExchange-Listenerdienst im DBMOVER-Mitglied mit der Sicherheitseinstellung SECURITY=(1,N) oder höher ausgeführt wird. Weitere Informationen finden Sie unter "SECURITY-Anweisung" im <i>PowerExchange-Referenzhandbuch</i>.</p>
Pass-Through-Sicherheit aktiviert	Aktiviert Pass-Through-Sicherheit für die Verbindung.
Datenbankname	Der Name der Datenbankinstanz.
Speicherort	Knotenname des Speicherorts des PowerExchange-Listenerdiensts, der mit DB2 verbunden ist. Der Knotenname ist im ersten Parameter der NODE-Anweisung in der PowerExchange-Konfigurationsdatei „dbmover.cfg“ definiert.
Umgebungs-SQL	SQL-Befehle zum Einrichten der Datenbankumgebung beim Herstellen einer Verbindung zur Datenbank. Der Datenintegrationsdienst führt die SQL-Befehle zur Verbindungsumgebung jedes Mal aus, wenn er eine Verbindung zur Datenbank herstellt.

Eigenschaft	Beschreibung
Datenbankdateiüberschreibungen	<p>Gibt die i5/OS-Datenbankdateiüberschreibung im folgenden Format an:</p> <pre>from_file/to_library/to_file/to_member</pre> <p>Wobei:</p> <ul style="list-style-type: none"> - <i>from_file</i> ist die zu überschreibende Datei. - <i>to_library</i> ist die zu verwendende neue Bibliothek. - <i>to_file</i> ist die zu verwendende Datei in der neuen Bibliothek. - <i>to_member</i> optional ist und das zu verwendende Elemente in der neuen Bibliothek und Datei darstellt. *FIRST wird verwendet, wenn keine Angabe gemacht wird. <p>Sie können bis zu acht eindeutige Dateiüberschreibungen für eine einzelne Verbindung angeben. Eine einfache Überschreibung gilt für eine einzelne Datei oder ein einzelnes Ziel. Wenn Sie mehr als eine Dateiüberschreibung angeben, umschließen Sie die Zeichenfolge der Dateiüberschreibungen mit doppelten Anführungszeichen (") und platzieren Sie ein Leerzeichen zwischen jeder Dateiüberschreibung.</p> <p>Hinweis: Wenn Sie sowohl Bibliotheksliste und Datenbankdateiüberschreibungen angeben und beide eine Tabelle enthalten, haben Datenbankdateiüberschreibungen Priorität.</p>
Bibliotheksverzeichnis	<p>Liste der Bibliotheken, die PowerExchange durchsucht, um den Tabellennamen für die Anweisungen „Auswählen“, „Einfügen“, „Löschen“, „Aktualisieren“ zu bestimmen. PowerExchange durchsucht die Liste, wenn der Tabellename unvollständig ist.</p> <p>Trennen Sie Bibliotheken mit Kommas.</p> <p>Hinweis: Wenn Sie sowohl Bibliotheksliste und Datenbankdateiüberschreibungen angeben und beide eine Tabelle enthalten, haben Datenbankdateiüberschreibungen Priorität.</p>
Codepage	<p>Die Codepage, die zum Lesen aus einer Quelldatenbank oder zum Schreiben in eine Zieldatenbank oder Zieldatei verwendet wird.</p>
Zu verwendende SQL-Bezeichnerzeichen	<p>Art des Zeichens, das von der Datenbank verwendet wird, um Delimiter-IDs in SQL-Abfragen einzuschließen. Die verfügbaren Zeichen richten sich nach dem Datenbanktyp.</p> <p>Wählen Sie (Keine) aus, wenn die Datenbank reguläre IDs verwendet. Wenn der Datenintegrationsdienst SQL-Abfragen erzeugt, schließt der Dienst IDs nicht in Delimiter-Zeichen ein.</p> <p>Wählen Sie ein Zeichen aus, wenn die Datenbank Delimiter-IDs verwendet. Wenn der Datenintegrationsdienst SQL-Abfragen erzeugt, schließt der Dienst Delimiter-IDs in dieses Zeichen ein.</p>
Unterstützte Bezeichner für gemischte Groß-/Kleinschreibung	<p>Aktivieren Sie diese Eigenschaft, wenn die Datenbank IDs für gemischte Groß-/Kleinschreibung verwendet. Bei aktivierter Eigenschaft schließt der Datenintegrationsdienst alle IDs innerhalb des Zeichens ein, das für die Eigenschaft SQL-Kennungszeichen ausgewählt wurde.</p> <p>Wenn die Eigenschaft SQL-Kennungszeichen auf „Kein“ festgelegt ist, wird die Eigenschaft Unterstützte IDs für gemischte Groß-/Kleinschreibung deaktiviert.</p>

Eigenschaft	Beschreibung
Isolationsebene	<p>Commit-Bereich der Transaktion. Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> - Keine - CS. Cursorstabilität. - RR. Repeatable Read. - CHG. Ändern. - ALL <p>Der Standardwert ist CS.</p>
Verschlüsselungstyp	<p>Optional. Der Verschlüsselungstyp, den der Datenintegrationsdienst verwendet. Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> - Keine - AES <p>Standardwert ist „Keine“.</p> <p>Hinweis: Informatica empfiehlt die Verwendung von SSL-Authentifizierung (Secure Sockets Layer) statt der Konfiguration der Verbindungseigenschaften Verschlüsselungstyp und Verschlüsselungsebene. SSL-Authentifizierung bietet striktere Sicherheit und wird von verschiedenen Informatica-Produkten verwendet.</p> <p>Weitere Informationen zum Implementieren von SSL-Authentifizierung in einem PowerExchange-Netzwerk finden Sie im <i>PowerExchange-Referenzhandbuch</i>.</p>
Verschlüsselungsebene	<p>Bei Verwendung von AES für Verschlüsselungstyp wählen Sie eine der folgenden Optionen aus, um die vom Datenintegrationsdienst verwendete Verschlüsselungsebene anzugeben:</p> <ul style="list-style-type: none"> - 1. Verwenden Sie einen 128-Bit-Verschlüsselungsschlüssel. - 2. Verwenden Sie einen 192-Bit-Verschlüsselungsschlüssel. - 3. Verwenden Sie einen 256-Bit-Verschlüsselungsschlüssel. <p>Wenn Sie als Verschlüsselungstyp nicht AES auswählen, wird diese Option ignoriert.</p> <p>Standardwert ist 1.</p>
Pacing-Größe	<p>Optional. Menge der Daten, die das Quellsystem an den PowerExchange-Listenerdienst übergeben kann. Legen Sie die Pacing-Größe fest, wenn eine externe Anwendung, eine Datenbank oder der Knoten mit dem Datenintegrationsdienst einen Engpass darstellt. Verwenden Sie niedrigere Werte für schnellere Leistung.</p> <p>Der Mindest- und Standardwert ist 0. Der Wert 0 bietet die beste Leistung.</p>
Als Zeilen interpretieren	<p>Optional. Wählen Sie diese Option, um die Pacing-Größe als Anzahl von Zeilen anzugeben. Löschen Sie diese Option, um die Pacing-Größe in Kilobyte anzugeben. Diese Option ist standardmäßig nicht ausgewählt und die Pacing-Größe wird in Kilobyte angegeben.</p>
Komprimierung	<p>Optional. Wählen Sie diese Option zum Aktivieren der Quelldatenkomprimierung aus. Durch die Komprimierung von Daten können Sie die Menge der Daten verringern, die Informatica-Anwendungen über das Netzwerk senden. Standardmäßig ist diese Option nicht ausgewählt und die Komprimierung ist deaktiviert.</p>
Array-Größe	<p>Optional. Die Anzahl der Datensätze im Speicher-Array für die Worker-Threads. Diese Option kann verwendet werden, wenn Sie die Option Worker-Threads auf einen Wert größer als 0 festlegen. Gültige Werte sind 25 bis 5000. Standardwert ist 25.</p>

Eigenschaft	Beschreibung
Schreibmodus	<p>Optional. Modus, in dem der Datenintegrationsdienst Daten zum PowerExchange-Listenerdienst sendet. Wählen Sie einen der folgenden Schreibmodi aus:</p> <ul style="list-style-type: none"> - CONFIRMWRITEON. Sendet Daten an den PowerExchange-Listenerdienst und wartet auf eine Antwort, bevor weitere Daten gesendet werden. Wählen Sie diese Option aus, wenn die Fehlerbehebung Priorität hat. Diese Option kann sich jedoch negativ auf die Leistung auswirken. - CONFIRMWRITEOFF. Sendet Daten an den PowerExchange-Listenerdienst, ohne auf eine Antwort zu warten. Verwenden Sie diese Option, wenn Sie die Zieltabelle im Fall eines Fehlers erneut laden können. - ASYNCHRONOUSWITHFAULTTOLERANCE. Sendet Daten an den PowerExchange-Listenerdienst, ohne auf eine Antwort zu warten. Diese Option aktiviert außerdem die Fehlererkennung. Diese Option kombiniert die Geschwindigkeit von CONFIRMWRITEOFF und die Datenintegrität von CONFIRMWRITEON. <p>Der Standardwert ist CONFIRMWRITEON.</p>
Ablehnungsdatei	<p>Überschreibt das Standard-Präfix von PWXR für die Ablehnungsdatei. PowerExchange erstellt die Ablehnungsdatei auf dem Zielcomputer, wenn der Schreibmodus ASYNCHRONOUSWITHFAULTTOLERANCE lautet. Geben Sie PWXDISABLE ein, um die Erstellung der Ablehnungsdateien zu verhindern.</p>

Eigenschaften von IBM DB2 for z/OS-Verbindungen

Verwenden Sie eine IBM DB2 for z/OS-Verbindung für den Zugriff auf Tabellen in IBM DB2 for z/OS. Eine IBM DB2 for z/OS-Verbindung ist ein relationaler Datenbank-Verbindungstyp. Sie können eine IBM DB2 for z/OS-Verbindung im Administrator Tool oder im Developer Tool erstellen und verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Eigenschaften von DB2 for z/OS-Verbindungen erläutert:

Eigenschaft	Beschreibung
Name	<p>Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten:</p> <p>~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /</p>
ID	<p>Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.</p>
Beschreibung	<p>Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 255 Zeichen enthalten.</p>
Verbindungstyp	<p>Verbindungstyp (DB2Z).</p>

Eigenschaft	Beschreibung
Benutzername	Benutzername für die Datenbank
Passwort	<p>Passwort für den angegebenen Benutzernamen oder eine gültige PowerExchange-Passphrase.</p> <p>Eine PowerExchange-Passphrase kann 9 bis 128 Zeichen lang sein und die folgenden Zeichen enthalten:</p> <ul style="list-style-type: none"> - Groß- und Kleinbuchstaben - Die Zahlen 0 bis 9 - Leerzeichen - Die folgenden Sonderzeichen: ' - ; # \ , . / ! % & * () _ + { } : @ < > ? <p>Hinweis: Das erste Zeichen ist ein Apostroph.</p> <p>Passphrasen dürfen keine einfachen Anführungszeichen (') , doppelten Anführungszeichen (") oder Währungssymbole enthalten.</p> <p>Stellen Sie vor der Verwendung von Passphrasen sicher, dass der PowerExchange-Listenerdienst im DBMOVER-Mitglied mit der Sicherheitseinstellung SECURITY=(1,N) oder höher ausgeführt wird. Weitere Informationen finden Sie unter "SECURITY-Anweisung" im <i>PowerExchange-Referenzhandbuch</i>.</p> <p>Die zulässigen Zeichen beim Beenden von IBM IRRPHREX haben keine Auswirkungen auf die zulässigen Zeichen in PowerExchange-Passphrasen.</p> <p>Hinweis: Eine gültige RACF-Passphrase kann bis zu 100 Zeichen enthalten. PowerExchange schneidet Passphrases mit mehr als 100 Zeichen ab, wenn diese zur Validierung an RACF übergeben werden.</p>
Pass-Through-Sicherheit aktiviert	Aktiviert Pass-Through-Sicherheit für die Verbindung.
DB2-Subsystem-ID	Name des DB2-Subsystems.
Speicherort	Knotenname des Speicherorts des PowerExchange-Listenerdiensts, der mit DB2 verbunden ist. Der Knotenname ist im ersten Parameter der NODE-Anweisung in der PowerExchange-Konfigurationsdatei „dbmover.cfg“ definiert.
Umgebungs-SQL	SQL-Befehle zum Einrichten der Datenbankumgebung beim Herstellen einer Verbindung zur Datenbank. Der Datenintegrationsdienst führt die SQL-Befehle zur Verbindungsumgebung jedes Mal aus, wenn er eine Verbindung zur Datenbank herstellt.
Korrelations-ID	Mit dem Präfix PWX zu verknüpfender Wert für die Bildung der DB2-Korrelations-ID bei DB2-Anfragen.
Codepage	Codepage, die zum Lesen aus einer Quell-Datenbank oder zum Schreiben auf eine Target-Datenbank oder -Datei verwendet wird.
Zu verwendende SQL-Bezeichnerzeichen	<p>Art des Zeichens, das von der Datenbank verwendet wird, um Delimiter-IDs in SQL-Abfragen einzuschließen. Die verfügbaren Zeichen richten sich nach dem Datenbanktyp.</p> <p>Wählen Sie (Keine) aus, wenn die Datenbank reguläre IDs verwendet. Wenn der Datenintegrationsdienst SQL-Abfragen erzeugt, schließt der Dienst IDs nicht in Delimiter-Zeichen ein.</p> <p>Wählen Sie ein Zeichen aus, wenn die Datenbank Delimiter-IDs verwendet. Wenn der Datenintegrationsdienst SQL-Abfragen erzeugt, schließt der Dienst Delimiter-IDs in dieses Zeichen ein.</p>

Eigenschaft	Beschreibung
Unterstützte Bezeichner für gemischte Groß-/ Kleinschreibung	<p>Aktivieren Sie diese Eigenschaft, wenn die Datenbank IDs für gemischte Groß-/ Kleinschreibung verwendet. Bei aktivierter Eigenschaft schließt der Datenintegrationsdienst alle IDs innerhalb des Zeichens ein, das für die Eigenschaft SQL-Kennungszeichen ausgewählt wurde.</p> <p>Wenn die Eigenschaft SQL-Kennungszeichen auf „Kein“ festgelegt ist, wird die Eigenschaft Unterstützte IDs für gemischte Groß-/Kleinschreibung deaktiviert.</p>
Verschlüsselungstyp	<p>Optional. Der Verschlüsselungstyp, den der Datenintegrationsdienst verwendet. Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> - Keine - AES <p>Standardwert ist „Keine“.</p> <p>Hinweis: Informatica empfiehlt die Verwendung von SSL-Authentifizierung (Secure Sockets Layer) statt der Konfiguration der Verbindungseigenschaften Verschlüsselungstyp und Ebene. SSL-Authentifizierung bietet striktere Sicherheit und wird von verschiedenen Informatica-Produkten verwendet.</p> <p>Weitere Informationen zum Implementieren von SSL-Authentifizierung in einem PowerExchange-Netzwerk finden Sie im <i>PowerExchange-Referenzhandbuch</i>.</p>
Verschlüsselungsebene	<p>Bei Verwendung von AES für Verschlüsselungstyp wählen Sie eine der folgenden Optionen aus, um die vom Datenintegrationsdienst verwendete Verschlüsselungsebene anzugeben:</p> <ul style="list-style-type: none"> - 1. Verwenden Sie einen 128-Bit-Verschlüsselungsschlüssel. - 2. Verwenden Sie einen 192-Bit-Verschlüsselungsschlüssel. - 3. Verwenden Sie einen 256-Bit-Verschlüsselungsschlüssel. <p>Wenn Sie als Verschlüsselungstyp nicht AES auswählen, wird diese Option ignoriert. Standardwert ist 1.</p>
Pacing-Größe	<p>Optional. Menge der Daten, die das Quellsystem an den PowerExchange-Listenerdienst übergeben kann. Legen Sie die Pacing-Größe fest, wenn eine externe Anwendung, eine Datenbank oder der Knoten mit dem Datenintegrationsdienst einen Engpass darstellt. Verwenden Sie niedrigere Werte für schnellere Leistung.</p> <p>Der Mindest- und Standardwert ist 0. Der Wert 0 bietet die beste Leistung.</p>
Als Zeilen interpretieren	<p>Optional. Wählen Sie diese Option, um die Pacing-Größe als Anzahl von Zeilen anzugeben. Löschen Sie diese Option, um die Pacing-Größe in Kilobyte anzugeben. Diese Option ist standardmäßig nicht ausgewählt und die Pacing-Größe wird in Kilobyte angegeben.</p>
Komprimierung	<p>Optional. Wählen Sie diese Option zum Aktivieren der Quelldatenkomprimierung aus. Durch die Komprimierung von Daten können Sie die Menge der Daten verringern, die Informatica-Anwendungen über das Netzwerk senden. Standardmäßig ist diese Option nicht ausgewählt und die Komprimierung ist deaktiviert.</p>
Offload-Verarbeitung	<p>Optional. Steuert, ob für die Verarbeitung von Stapeldaten vom Quellcomputer zum Datenintegrationsdienst-Computer Offload-Verarbeitung verwendet werden soll. Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> - AUTO. Der Datenintegrationsdienst bestimmt, ob Offload-Verarbeitung verwendet werden soll. - Ja. Offload-Verarbeitung wird verwendet. - Nein. Offload-Verarbeitung wird nicht verwendet. <p>Der Standardwert ist Nein.</p>

Eigenschaft	Beschreibung
Worker-Threads	Optional. Anzahl der vom Datenintegrationsdienst verwendeten Threads, um Stapeldaten bei aktivierter Offload-Verarbeitung zu verarbeiten. Um eine optimale Leistung zu erzielen, sollte dieser Wert die Anzahl der verfügbaren Prozessoren auf dem Rechner des Datenintegrationsdienstes nicht überschreiten. Gültige Werte sind 1 bis 64. Der Standardwert ist 0, der Multithreading deaktiviert.
Array-Größe	Optional. Die Anzahl der Datensätze im Speicher-Array für die Worker-Threads. Diese Option kann verwendet werden, wenn Sie die Option Worker-Threads auf einen Wert größer als 0 festlegen. Gültige Werte sind 1 bis 5000. Standardwert ist 25.
Schreibmodus	<p>Modus, in dem der Datenintegrationsdienst Daten zum PowerExchange-Listenerdienst sendet. Konfigurieren Sie einen der folgenden Schreibmodi:</p> <ul style="list-style-type: none"> - CONFIRMWRITEON. Sendet Daten an den PowerExchange-Listenerdienst und wartet auf eine Antwort, bevor weitere Daten gesendet werden. Wählen Sie diese Option, wenn die Fehlerbehebung Priorität hat. Diese Option kann die Leistung verringern. - CONFIRMWRITEOFF. Sendet Daten an den PowerExchange-Listenerdienst, ohne auf eine Antwort zu warten. Verwenden Sie diese Option, wenn Sie die Zieltabelle im Fall eines Fehlers erneut laden können. - ASYNCHRONOUSWITHFAULTTOLERANCE. Sendet Daten an den PowerExchange-Listenerdienst, ohne auf eine Antwort zu warten. Diese Option bietet auch die Möglichkeit zur Fehlererkennung. Hiermit wird die Geschwindigkeit von Confirm Write Off mit der Datenintegrität von Confirm Write On kombiniert. Der Standardwert ist CONFIRMWRITEON.
Ablehnungsdatei	Überschreibt das Standard-Präfix von PWXR für die Ablehnungsdatei. PowerExchange erstellt die Ablehnungsdatei auf dem Zielcomputer, wenn der Schreibmodus ASYNCHRONOUSWITHFAULTTOLERANCE lautet. Geben Sie PWXDISABLE ein, um die Erstellung von Ablehnungsdateien zu verhindern.

IMS-Verbindungseigenschaften

Verwenden Sie eine IMS-Verbindung, um auf eine IMS-Datenbank zuzugreifen. Die IMS-Verbindung ist eine nicht-relationaler Mainframe-Datenbank-Verbindungstyp. Der Datenintegrationsdienst stellt über PowerExchange eine Verbindung mit IMS her. Sie erstellen eine IMS-Verbindung im Developer-Tool. Sie können eine IMS-Verbindung im Administrator-Tool oder im Developer-Tool verwalten.

In der folgenden Tabelle werden die Eigenschaften von IMS-Verbindungen erläutert:

Option	Beschreibung
Speicherort	Knotenname für den Speicherort des PowerExchange-Listenerdiensts, der eine Verbindung zu IMS herstellt. Der Knotenname ist im ersten Parameter der NODE-Anweisung in der PowerExchange-Konfigurationsdatei „dbmover.cfg“ definiert.
Benutzername	Benutzername für die Datenbank

Option	Beschreibung
Passwort	<p>Passwort für den angegebenen Datenbankbenutzernamen oder eine gültige PowerExchange-Passphrase.</p> <p>Eine PowerExchange-Passphrase kann 9 bis 128 Zeichen lang sein und die folgenden Zeichen enthalten:</p> <ul style="list-style-type: none"> - Groß- und Kleinbuchstaben - Die Zahlen 0 bis 9 - Leerzeichen - Die folgenden Sonderzeichen: ' - ; # \ , . / ! % & * () _ + { } : @ < > ? <p>Hinweis: Das erste Zeichen ist ein Apostroph.</p> <p>Passphrasen dürfen keine einfachen Anführungszeichen ('), doppelten Anführungszeichen (") oder Währungssymbole enthalten.</p> <p>Die zulässigen Zeichen beim Beenden von IBM IRRPHREX haben keine Auswirkungen auf die zulässigen Zeichen in PowerExchange-Passphrasen.</p> <p>Hinweis: Eine gültige RACF-Passphrase kann bis zu 100 Zeichen enthalten. PowerExchange schneidet Passphrases mit mehr als 100 Zeichen ab, wenn diese zur Validierung an RACF übergeben werden.</p> <p>Um Passphrases für IMS-Verbindungen zu verwenden, stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind:</p> <ul style="list-style-type: none"> - Der PowerExchange-Listenedienst muss mit der Sicherheitseinstellung SECURITY=(1,N) oder höher im DBMOVER-Mitglied ausgeführt werden. Weitere Informationen finden Sie unter „SECURITY-Anweisung“ im <i>PowerExchange-Referenzhandbuch</i>. - Sie müssen ODBA-Zugriff auf IMS wie im <i>PowerExchange-Navigator-Benutzerhandbuch</i> erläutert konfigurieren. - Sie müssen IMS-Daten-Mappings verwenden, die IMS ODBA als Zugriffsmethode angeben. Verwenden Sie keine Daten-Mappings, die die DL/1 BATCH-Zugriffsmethode angeben, da diese Zugriffsmethode die Verwendung von Netport-Jobs erfordert, die keine Unterstützung für Passphrases bieten. - Die IMS-Datenbank muss im IMS-Kontrollbereich online sein, um ODBA-Zugriff auf IMS zu verwenden.
Codepage	<p>Erforderlich. Name der Codepage für das Lesen aus oder Schreiben in die Datenquelle. Normalerweise ist dieser Wert ein ISO-Codepage-Name, z. B. ISO-8859-6.</p>
Pass-Through-Sicherheit aktiviert	<p>Aktiviert Pass-Through-Sicherheit für die Verbindung.</p>
Verschlüsselungstyp	<p>Der Verschlüsselungstyp, den der Datenintegrationsdienst verwendet. Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> - Keine - AES <p>Standardwert ist „Keine“.</p> <p>Hinweis: Informatica empfiehlt die Verwendung von SSL-Authentifizierung (Secure Sockets Layer) statt der Konfiguration der Verbindungseigenschaften Verschlüsselungstyp und Ebene. SSL-Authentifizierung bietet striktere Sicherheit und wird von verschiedenen Informatica-Produkten verwendet.</p> <p>Weitere Informationen zum Implementieren von SSL-Authentifizierung in einem PowerExchange-Netzwerk finden Sie im <i>PowerExchange-Referenzhandbuch</i>.</p>

Option	Beschreibung
[Encryption]-Ebene	<p>Bei Verwendung von AES für Verschlüsselungstyp wählen Sie eine der folgenden Optionen aus, um die vom Datenintegrationsdienst verwendete Verschlüsselungsebene anzugeben:</p> <ul style="list-style-type: none"> - 1. Verwenden Sie einen 128-Bit-Verschlüsselungsschlüssel. - 2. Verwenden Sie einen 192-Bit-Verschlüsselungsschlüssel. - 3. Verwenden Sie einen 256-Bit-Verschlüsselungsschlüssel. <p>Wenn Sie als Verschlüsselungstyp nicht AES auswählen, wird diese Option ignoriert. Standard ist 1.</p>
Pacing-Größe	<p>Optional. Menge der Daten, die das Quellsystem an den PowerExchange-Listenerdienst übergeben kann. Legen Sie die Pacing-Größe fest, wenn eine externe Anwendung, eine Datenbank oder der Knoten mit dem Datenintegrationsdienst einen Engpass darstellt. Verwenden Sie niedrigere Werte für schnellere Leistung.</p> <p>Der Mindest- und Standardwert ist 0. Der Wert 0 bietet die beste Leistung.</p>
Als Zeilen interpretieren	<p>Optional. Wählen Sie diese Option, um die Pacing-Größe als Anzahl von Zeilen anzugeben. Löschen Sie diese Option, um die Pacing-Größe in Kilobyte anzugeben. Diese Option ist standardmäßig nicht ausgewählt und die Pacing-Größe wird in Kilobyte angegeben.</p>
Komprimierung	<p>Optional. Wählen Sie diese Option zum Aktivieren der Quelldatenkomprimierung aus. Durch die Komprimierung von Daten können Sie die Menge der Daten verringern, die Informatica-Anwendungen über das Netzwerk senden. Standardmäßig ist diese Option nicht ausgewählt und die Komprimierung ist deaktiviert.</p>
Offload-Verarbeitung	<p>Optional. Steuert, ob für die Verarbeitung von Stapeldaten vom Quellcomputer zum Datenintegrationsdienst-Computer Offload-Verarbeitung verwendet werden soll. Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> - AUTO. Der Datenintegrationsdienst bestimmt, ob Offload-Verarbeitung verwendet werden soll. - Ja. Offload-Verarbeitung wird verwendet. - Nein. Offload-Verarbeitung wird nicht verwendet. <p>Der Standardwert ist AUTO.</p>
Worker-Threads	<p>Optional. Anzahl der vom Datenintegrationsdienst verwendeten Threads, um Stapeldaten bei aktivierter Offload-Verarbeitung zu verarbeiten. Um eine optimale Leistung zu erzielen, sollte dieser Wert die Anzahl der verfügbaren Prozessoren auf dem Rechner des Datenintegrationsdienstes nicht überschreiten. Gültige Werte sind 1 bis 64. Der Standardwert ist 0, der Multithreading deaktiviert.</p>
Array-Größe	<p>Optional. Die Anzahl der Datensätze im Speicher-Array für die Worker-Threads. Diese Option kann verwendet werden, wenn Sie die Option Worker-Threads auf einen Wert größer als 0 festlegen. Gültige Werte sind 1 bis 5000. Standardwert ist 25.</p>
Schreibmodus	<p>Optional. Modus, in dem der Datenintegrationsdienst Daten an den PowerExchange-Listenerdienst sendet. Wählen Sie einen der folgenden Schreibmodi aus:</p> <ul style="list-style-type: none"> - CONFIRMWRITEON. Sendet Daten an den PowerExchange-Listenerdienst und wartet auf eine Antwort, bevor weitere Daten gesendet werden. Wählen Sie diese Option aus, wenn die Fehlerbehebung Priorität hat. Diese Option kann sich jedoch negativ auf die Leistung auswirken. - CONFIRMWRITEOFF. Sendet Daten an den PowerExchange-Listenerdienst, ohne auf eine Antwort zu warten. Verwenden Sie diese Option, wenn Sie die Zieltabelle im Fall eines Fehlers erneut laden können. - ASYNCHRONOUSWITHFAULTTOLERANCE. Sendet Daten an den PowerExchange-Listenerdienst, ohne auf eine Antwort zu warten. Diese Option aktiviert außerdem die Fehlererkennung. Diese Option kombiniert die Geschwindigkeit von CONFIRMWRITEOFF und die Datenintegrität von CONFIRMWRITEON. <p>Der Standardwert ist CONFIRMWRITEON.</p>

Eigenschaften der JDBC-Verbindung

Sie können eine JDBC-Verbindung für den Zugriff auf Tabellen in einer Datenbank verwenden. Sie können eine JDBC-Verbindung im Administrator tool, Developer tool oder Analyst Tool erstellen und verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Eigenschaften von JDBC-Verbindungen erläutert:

Eigenschaft	Beschreibung
Datenbanktyp	Der Datenbanktyp.
Name	Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
ID	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Benutzername	Der Benutzername der Datenbank.
Passwort	Das Passwort für den Benutzernamen der Datenbank.
JDBC-Treiberklassenname	<p>Name der JDBC-Treiberklasse.</p> <p>Die folgende Liste enthält den Treiberklassennamen, den Sie für den entsprechenden Datenbanktyp eingeben können:</p> <ul style="list-style-type: none">- DataDirect-JDBC-Treiberklassenname für Oracle: <code>com.informatica.jdbc.oracle.OracleDriver</code>- DataDirect-JDBC-Treiberklassenname für IBM DB2: <code>com.informatica.jdbc.db2.DB2Driver</code>- DataDirect-JDBC-Treiberklassenname für Microsoft SQL Server: <code>com.informatica.jdbc.sqlserver.SQLServerDriver</code>- DataDirect-JDBC-Treiberklassenname für Sybase ASE: <code>com.informatica.jdbc.sybase.SybaseDriver</code>- DataDirect-JDBC-Treiberklassenname für Informix: <code>com.informatica.jdbc.informix.InformixDriver</code>- DataDirect-JDBC-Treiberklassenname für MySQL: <code>com.informatica.jdbc.mysql.MySQLDriver</code>- JDBC-Treiber für Databricks Delta Lake: der Name des aus Databricks heruntergeladenen Treibers. Informationen zum Treiber finden Sie im Thema zur Konfiguration des Speicherzugriffs im Kapitel „Vorbereitung der Databricks-Integration“ des <i>Data Engineering Integration-Handbuch</i>. <p>Weitere Informationen zu den mit bestimmten Datenbanken zu verwendenden Treiberklassen finden Sie in der Dokumentation des Herstellers.</p>

Eigenschaft	Beschreibung
Verbindungszeichenfolge	<p>Verbindungszeichenfolge für die Verbindung zur Datenbank. Verwenden Sie die folgende Verbindungszeichenfolge:</p> <pre>jdbc:<subprotocol>:<subname></pre> <p>Weitere Informationen über die Verbindungszeichenfolge, die mit bestimmten Treibern verwendet werden soll, finden Sie in der Dokumentation des Anbieters.</p>
Umgebungs-SQL	<p>Optional. Geben Sie die SQL-Befehle zum Einrichten der Datenbankumgebung ein, wenn Sie eine Verbindung zur Datenbank herstellen. Der Datenintegrationsdienst führt die SQL-Befehle zur Verbindungsumgebung jedes Mal aus, wenn er eine Verbindung zur Datenbank herstellt.</p> <p>Hinweis: Wenn Sie Sqoop aktivieren, ignoriert Sqoop diese Eigenschaft.</p>
Transaktions-SQL	<p>Optional. Geben Sie die SQL-Befehle zum Einrichten der Datenbankumgebung ein, wenn Sie eine Verbindung zur Datenbank herstellen. Der Datenintegrationsdienst führt die Transaktionsumgebungs-SQL am Anfang jeder Transaktion aus.</p> <p>Hinweis: Wenn Sie Sqoop aktivieren, ignoriert Sqoop diese Eigenschaft.</p>
SQL-Bezeichnerzeichen	<p>Art des Zeichens, das von der Datenbank verwendet wird, um Delimiter-IDs in SQL-Abfragen einzuschließen. Die verfügbaren Zeichen richten sich nach dem Datenbanktyp. Wählen Sie (Keine) aus, wenn die Datenbank reguläre IDs verwendet. Wenn der Datenintegrationsdienst SQL-Abfragen erzeugt, schließt der Dienst IDs nicht in Delimiter-Zeichen ein.</p> <p>Wählen Sie ein Zeichen aus, wenn die Datenbank Delimiter-IDs verwendet. Wenn der Datenintegrationsdienst SQL-Abfragen erzeugt, schließt der Dienst Delimiter-IDs in dieses Zeichen ein.</p> <p>Hinweis: Wenn Sie Sqoop aktivieren, ignoriert Sqoop diese Eigenschaft.</p>
Bezeichner mit gemischter Groß-/Kleinschreibung unterstützen	<p>Aktivieren Sie diese Eigenschaft, wenn die Datenbank IDs für gemischte Groß-/Kleinschreibung verwendet. Bei aktivierter Eigenschaft schließt der Datenintegrationsdienst alle IDs innerhalb des Zeichens ein, das für die Eigenschaft SQL-Kennungszeichen ausgewählt wurde.</p> <p>Wenn die Eigenschaft SQL-Kennungszeichen auf „Kein“ festgelegt ist, wird die Eigenschaft Unterstützte IDs für gemischte Groß-/Kleinschreibung deaktiviert.</p> <p>Hinweis: Wenn Sie Sqoop konfigurieren, beachtet das Sqoop-Programm diese Eigenschaft, wenn Sie ein DDL-Skript generieren und ausführen, um ein Ziel zur Laufzeit zu erstellen oder zu ersetzen. In allen anderen Szenarios ignoriert Sqoop diese Eigenschaft.</p>

Eigenschaft	Beschreibung
Sqoop-Connector verwenden	<p>Aktiviert Sqoop-Konnektivität für das Datenobjekt, das die JDBC-Verbindung verwendet. Der Datenintegrationsdienst führt das Mapping in der Hadoop-Laufzeitumgebung über Sqoop aus.</p> <p>Sie können Sqoop-Konnektivität für relationale Datenobjekte, benutzerdefinierte Datenobjekte und logische Datenobjekte konfigurieren, die auf einer JDBC-fähigen Datenbank basieren.</p> <p>Wählen Sie Sqoop v1.x aus, um Sqoop-Konnektivität zu aktivieren.</p> <p>Standardwert ist Keine.</p>
Sqoop-Argumente	<p>Geben Sie die Argumente ein, die von Sqoop zum Herstellen einer Verbindung zur Datenbank verwendet werden müssen. Trennen Sie mehrere Argumente durch ein Leerzeichen.</p> <p>Zur Ausführung der Zuordnung auf der Blaze-Engine mit den spezialisierten TDCH-Konnektoren (Teradata Connector for Hadoop) für Sqoop müssen Sie die TDCH-Klasse der Verbindungs-Factory in den Sqoop-Argumenten definieren. Die Klasse der Verbindungs-Factory richtet sich nach dem TDCH-Sqoop-Konnektor, der verwendet werden soll.</p> <ul style="list-style-type: none"> - Um Cloudera Connector Powered by Teradata zu verwenden, konfigurieren Sie das folgende Sqoop-Argument: <ul style="list-style-type: none"> - <code>Dsqoop.connection.factories=com.cloudera.connector.teradata.TeradataManagerFactory</code> - Um Hortonworks Connector for Teradata (unterstützt vom Teradata Connector for Hadoop) zu verwenden, konfigurieren Sie das folgende Sqoop-Argument: <ul style="list-style-type: none"> - <code>Dsqoop.connection.factories=org.apache.sqoop.teradata.TeradataManagerFactory</code> <p>Zur Ausführung der Zuordnung auf der Spark-Engine müssen Sie die TDCH-Klasse der Verbindungs-Factory nicht in den Sqoop-Argumenten definieren. Der Datenintegrationsdienst ruft standardmäßig den Cloudera Connector Powered by Teradata und den Hortonworks Connector for Teradata (unterstützt vom Teradata Connector for Hadoop) auf.</p> <p>Hinweis: Zur Ausführung der Zuordnung mit einem generischen JDBC-Konnektor anstelle des spezialisierten Cloudera- oder Hortonworks-Konnektors müssen Sie die Sqoop-Argumente <code>--driver</code> und <code>--connection-manager</code> in der JDBC-Verbindung definieren. Wenn Sie die Argumente <code>--driver</code> und <code>--connection-manager</code> in der Lese- oder Schreibumwandlung der Zuordnung definieren, ignoriert Sqoop die Argumente.</p> <p>Wenn Sie keine Sqoop-Argumente eingeben, erstellt der Datenintegrationsdienst den Sqoop-Befehl basierend auf den JDBC-Verbindungseigenschaften.</p>

Eigenschaften der JDBC V2-Verbindung

Wenn Sie eine JDBC V2-Verbindung einrichten, müssen Sie die Verbindungseigenschaften konfigurieren.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die JDBC V2-Verbindungseigenschaften beschrieben:

Eigenschaft	Beschreibung
Name	Der Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung ändern. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * () - + = { [] \ : ; " ' < , > . ? /
ID	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 4.000 Zeichen enthalten.
Speicherort	Die Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Der Verbindungstyp. Wählen Sie „JDBC V2“ aus.

Die Registerkarte **Details** enthält die Verbindungsattribute der JDBC V2-Verbindung. In der folgenden Tabelle werden die Verbindungsattribute beschrieben:

Eigenschaft	Beschreibung
Benutzername	Der Benutzername der Datenbank. Benutzername mit Berechtigungen zum Zugriff auf die Datenbank, die den JDBC-Treiber vom Typ 4 unterstützt.
Passwort	Das Passwort für den Benutzernamen der Datenbank.
Schemaname	Optional. Der Schemaname zum Herstellen einer Verbindung mit der Datenbank. Wenn Sie den Schemanamen nicht angeben, werden alle in der Datenbank verfügbaren Schemas aufgelistet.
JDBC-Treiberklassenname	Name der JDBC-Treiberklasse. Die folgende Liste enthält den Treiberklassennamen, den Sie für den entsprechenden Datenbanktyp eingeben können: <ul style="list-style-type: none"> - JDBC-Treiberklassenname für die Azure SQL-Datenbank: <code>com.microsoft.sqlserver.jdbc.SQLServerDriver</code> - JDBC-Treiberklassenname für Aurora PostgreSQL: <code>org.postgresql.Driver</code> - JDBC-Treiberklassenname für die SAP HANA-Datenbank: <code>com.sap.db.jdbc.Driver</code> Weitere Informationen über die mit bestimmten Datenbanken zu verwendenden Treiberklassen finden Sie in der Dokumentation des Drittanbieters.

Eigenschaft	Beschreibung
Verbindungszeichenfolge	<p>Verbindungszeichenfolge für die Verbindung zur Datenbank. Verwenden Sie die folgende Verbindungszeichenfolge:</p> <pre>jdbc:<subprotocol>:<subname></pre> <p>Die folgende Liste enthält die Beispiolverbindungszeichenfolgen, die Sie für den entsprechenden Datenbanktyp eingeben können:</p> <ul style="list-style-type: none"> - Verbindungszeichenfolge für den JDBC-Treiber der Azure SQL-Datenbank: <pre>jdbc:sqlserver://<host>:<port>;database=<database_name></pre> - Verbindungszeichenfolge für den JDBC-Treiber von Aurora PostgreSQL: <pre>jdbc:postgresql://<host>:<port>[/<database_name>]</pre> - Verbindungszeichenfolge für den SAP HANA-Datenbanktreiber: <pre>jdbc:sap://<host>:<port>/?databaseName=<Database_Name></pre> <p>Weitere Informationen über die mit bestimmten Treibern zu verwendende Verbindungszeichenfolge finden Sie in der Dokumentation des Drittanbieters.</p>
Subtyp	<p>Der Datenbanktyp, zu dem eine Verbindung hergestellt werden soll. Folgende Datenbanktypen stehen hierbei zur Auswahl bereit:</p> <ul style="list-style-type: none"> - Azure SQL-Datenbank. Stellt eine Verbindung zur Azure SQL-Datenbank her. - PostgreSQL Stellt eine Verbindung zur Aurora PostgreSQL-Datenbank her. - SAP HANA-Datenbank. Stellt eine Verbindung zur SAP HANA-Datenbank her. - Andere Verbindet sich mit jeder Datenbank, die den JDBC-Treiber Typ 4 unterstützt.
Unterstützte Kennungen für gemischte Groß-/Kleinschreibung	<p>Aktivieren Sie diese Eigenschaft, wenn die Datenbank IDs für gemischte Groß-/Kleinschreibung verwendet. Bei aktivierter Eigenschaft schließt der Datenintegrationsdienst alle IDs innerhalb des Zeichens ein, das für die Eigenschaft SQL-Kennungszeichen ausgewählt wurde.</p> <p>Beispiel: Die Aurora PostgreSQL-Datenbank unterstützt gemischte Groß-/Kleinschreibung. Sie müssen diese Eigenschaft aktivieren, um eine Verbindung zur Aurora PostgreSQL-Datenbank herzustellen.</p> <p>Wenn die Eigenschaft SQL-Kennungszeichen auf „Kein“ festgelegt ist, wird die Eigenschaft Unterstützte IDs für gemischte Groß-/Kleinschreibung deaktiviert.</p>
SQL-Kennungszeichen	<p>Art des Zeichens, das von der Datenbank verwendet wird, um Delimiter-IDs in SQL-Abfragen einzuschließen. Die verfügbaren Zeichen richten sich nach dem Datenbanktyp.</p> <p>Wählen Sie (Keine) aus, wenn die Datenbank reguläre IDs verwendet. Wenn der Datenintegrationsdienst SQL-Abfragen erzeugt, schließt der Dienst IDs nicht in Delimiter-Zeichen ein.</p> <p>Wählen Sie ein Zeichen aus, wenn die Datenbank Delimiter-IDs verwendet. Wenn der Datenintegrationsdienst SQL-Abfragen erzeugt, schließt der Dienst Delimiter-IDs in dieses Zeichen ein.</p> <p>Hinweis: Wählen Sie für SQL-Kennungszeichen die Option Kein aus, wenn Sie den SAP HANA-Datenbank-Untertyp angeben.</p>

Eigenschaften der JD Edwards EnterpriseOne-Verbindung

Verwenden Sie eine JD Edwards EnterpriseOne-Verbindung, um eine Verbindung zu einem JD Edwards EnterpriseOne-Objekt herzustellen.

In der folgenden Tabelle werden die Eigenschaften der JD Edwards EnterpriseOne-Verbindung beschrieben:

Eigenschaft	Beschreibung
Name	Der Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die maximale Länge beträgt 128 Zeichen. Das Leer- und die folgenden Sonderzeichen sind möglich: ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
ID	Die Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Die Informatica-Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Der Verbindungstyp. Wählen Sie JD Edwards EnterpriseOne aus.
Hostname	Hostname des JD Edwards EnterpriseOne-Servers.
Unternehmensport	Portnummer des JD Edwards EnterpriseOne-Servers. Standardwert ist 6016.
Benutzername	Der Benutzername der JD Edwards EnterpriseOne-Datenbank.
Passwort	Das Passwort für den Benutzer der JD Edwards EnterpriseOne-Datenbank.
Umgebung	Name der JD Edwards EnterpriseOne-Umgebung, zu der Sie eine Verbindung herstellen möchten.
Rolle	Rolle des JD Edwards EnterpriseOne-Benutzers. Standardwert ist *ALL.
Benutzername	Der Benutzername der JD Edwards EnterpriseOne-Datenbank.
Passwort	Passwort für den Datenbankbenutzer.

Eigenschaft	Beschreibung
Name der Treiberklasse	<p>Die folgende Liste enthält den Treiberklassennamen, den Sie für den entsprechenden Datenbanktyp eingeben können:</p> <ul style="list-style-type: none"> - DataDirect-JDBC-Treiberklassenname für Oracle: <code>com.informatica.jdbc.oracle.OracleDriver</code> - DataDirect-JDBC-Treiberklassenname für IBM DB2: <code>com.informatica.jdbc.db2.DB2Driver</code> - DataDirect-JDBC-Treiberklassenname für Microsoft SQL Server: <code>com.informatica.jdbc.sqlserver.SQLServerDriver</code> <p>Weitere Informationen zu den mit bestimmten Datenbanken zu verwendenden Treiberklassen finden Sie in der Dokumentation des Herstellers.</p>
Verbindungszeichenfolge	<p>Die Verbindungszeichenfolge für die Verbindung zur Datenbank. Verwenden Sie die folgende Verbindungszeichenfolge:</p> <p>Die JDBC-Verbindungszeichenfolge verwendet die folgende Syntax:</p> <ul style="list-style-type: none"> - Für Oracle: <code>jdbc:informatica:oracle://<host name>:<port>,ServiceName=<db service name></code> - Für DB2: <code>jdbc:informatica:db2://<host name>:<port>;databaseName=<db name></code> - Für Microsoft SQL: <code>jdbc:informatica:sqlserver://<host name>:<port>;databaseName=<db name></code>

Kafka-Verbindungseigenschaften

Bei der Kafka-Verbindung handelt es sich um eine Messaging-Verbindung. Verwenden Sie die Kafka-Verbindung, um auf einen Apache Kafka-Broker als Quelle oder Ziel zuzugreifen. Sie können eine Kafka-Verbindung im Developer Tool oder durch infacmd erstellen und verwalten.

Wenn Sie eine Kafka-Verbindung konfigurieren, konfigurieren Sie die folgenden Eigenschaften:

- Die Liste der Kafka-Broker, von denen die Verbindung liest oder in die sie schreibt.
- Die Anzahl der Sekunden, die der Integrationsdienst versucht, eine erneute Verbindung zu der Datenbank herzustellen, wenn die Verbindung fehlschlägt.
- Die Version des Kafka-Messaging-Brokers. Konfigurieren Sie die Kafka Messaging Broker-Version auf Apache 0.10.1.1 und höher.

Allgemeine Eigenschaften

In der folgenden Tabelle werden die allgemeinen Verbindungseigenschaften für die Kafka-Verbindung beschrieben:

Eigenschaft	Beschreibung
Name	Der Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung ändern. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * () - + = { [] \ : ; " ' < , > . ? /
ID	Die Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Die Beschreibung der Verbindung. Geben Sie eine Zeichenfolge ein, mit der Sie die Verbindung angeben können. Die Beschreibung darf nicht mehr als 4.000 Zeichen enthalten.
Speicherort	Die Domäne, in der Sie die Verbindung erstellen möchten. Wählen Sie den Domänennamen aus.
Typ	Der Verbindungstyp. Wählen Sie Messaging/Kafka.

Eigenschaften des Kafka-Brokers

In der folgenden Tabelle werden die Kafka-Broker-Eigenschaften für die Kafka-Verbindung beschrieben:

Eigenschaft	Beschreibung
Liste der Kafka-Broker	Durch Kommas getrennte Liste der Kafka-Broker, die die Konfiguration des Kafka-Messaging-Brokers beibehalten. Verwenden Sie das folgende Format, um einen Kafka-Broker anzugeben: <IP-Adresse>:<Port>
Timeout der Wiederholungen	Anzahl der Sekunden, nach denen der Integrationsdienst versucht, erneut eine Verbindung zum Kafka-Broker herzustellen, um Daten zu lesen oder zu schreiben. Ist die Quelle oder das Ziel für den angegebenen Zeitraum nicht verfügbar, wird die Zuordnungsausführung zur Vermeidung von Datenverlusten angehalten.

Eigenschaft	Beschreibung
Kafka-Broker-Version	Konfigurieren Sie die Kafka Messaging Broker-Version auf Apache 0.10.1.1 und höher.
Zusätzliche Verbindungseigenschaften	<p>Optional. Durch Kommas getrennte Liste der Verbindungseigenschaften, um eine Verbindung zum Kafka-Broker herzustellen.</p> <p>Sie können beispielsweise folgende Syntax verwenden:</p> <pre>request.timeout.ms=<value>,session.timeout.ms=<value>, fetch.max.wait.ms=<value>,heartbeat.interval.ms=<value>, security.protocol=SASL_PLAINTEXT,sasl.kerberos. service.name=<kerberos_name>,sasl.mechanism=GSSAPI, sasl.jaas.config=com.sun.security.auth.module. Krb5Login Modulrequired useKeyTab=true doNotPrompt=true storeKey=true client=true keyTab="<Keytab Location>" principal="<principal>"</pre> <p>Um die Zeit für den Verbindungsaufbau mit dem Kafka-Broker zu reduzieren, stellen Sie sicher, dass Sie die folgenden Eigenschaften festgelegt haben:</p> <ul style="list-style-type: none"> - request.timeout.ms - session.timeout.ms - fetch.max.wait.ms - heartbeat.interval.ms <p>Um eine sichere Verbindung zum Kafka-Broker herzustellen, stellen Sie sicher, dass Sie einen der folgenden Werte für die Eigenschaft security.protocol festlegen:</p> <ul style="list-style-type: none"> - SASL_SSL - SSL <p>Der Standardwert der Eigenschaft security.protocol ist SASL_PLAINTEXT.</p> <p>Technische Vorschau: Die zusätzlichen Verbindungseigenschaften stehen für die technische Vorschau zur Verfügung. Funktionen für die technische Vorschau sind noch nicht produktionsreif und werden daher zwar unterstützt, aber nicht garantiert. Informatica empfiehlt, dass Sie sie nur in Nicht-Produktionsumgebungen verwenden. Weitere Informationen über die Verbindungseigenschaften finden Sie unter https://kafka.apache.org/documentation/.</p>

SSL-Eigenschaften

In der folgenden Tabelle werden die SSL-Eigenschaften für die Kafka-Verbindung beschrieben:

Eigenschaft	Beschreibung
SSL-Modus	<p>Erforderlich. SSL-Modus, der den für die Verbindung zu verwendenden Verschlüsselungstyp angibt.</p> <p>Sie können einen Modus aus den folgenden SSL-Modi auswählen:</p> <ul style="list-style-type: none"> - Deaktiviert - Unidirektional - Bidirektional
SSL-TrustStore-Dateipfad	<p>Erforderlich, wenn der SSL-Modus Unidirektional ausgewählt ist.</p> <p>Absoluter Pfad und Dateiname der SSL-Truststore-Datei, die Zertifikate des vertrauenswürdigen SSL-Servers enthält.</p>

Eigenschaft	Beschreibung
SSL-Truststore-Passwort	Erforderlich, wenn der SSL-Modus Unidirektional ausgewählt ist. Passwort für den SSL-Truststore.
SSL-KeyStore-Dateipfad	Erforderlich, wenn der SSL-Modus Bidirektional ausgewählt ist. Absoluter Pfad und Dateiname der SSL-Schlüsselspeicherdatei, die private Schlüssel und Zertifikate für den SSL-Server enthält.
SSL-Schlüsselspeicherpasswort	Erforderlich, wenn der SSL-Modus Bidirektional ausgewählt ist. Passwort für den SSL-Schlüsselspeicher.

Erstellen einer Kafka-Verbindung mit infacmd

Sie können das infacmd-Befehlszeilenprogramm verwenden, um eine Kafka-Verbindung zu erstellen.

Führen Sie den folgenden Befehl aus, um eine Kafka-Verbindung unter UNIX zu erstellen:

```
sh infacmd.sh createConnection -dn <domain name> -un <domain user> -pd <domain password> -cn
<connection name> -cid <connection id> -ct Kafka -o
kfkBrkList=<host1:port1>,<host2:port2>,<host3:port3> kafkabrokerVersion=<version>
additionalConnectionProperties=<additional properties>
```

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

Kudu-Verbindungseigenschaften

Verwenden Sie eine Kudu-Verbindung, um auf Kudu zuzugreifen.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

Sie können eine Kudu-Verbindung im Administrator Tool oder im Developer Tool erstellen und verwalten. In der folgenden Tabelle werden die Kudu-Verbindungseigenschaften beschrieben:

Eigenschaft	Beschreibung
Name	Der Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung ändern. Der Name darf maximal 128 Zeichen umfassen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * () - + = { [] \ : ; " ' < , > . ? /
ID	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 4.000 Zeichen enthalten.

Eigenschaft	Beschreibung
Speicherort	Die Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Der Verbindungstyp. Wählen Sie „Kudu“ aus.

In der folgenden Tabelle werden die Eigenschaften für den Metadatenzugriff beschrieben:

Eigenschaft	Beschreibung
Kudu-Master-URLs	Die URLs der Kudu-Mastertabellen.
Kudu-Bibliotheksversion	Die Versionsnummer der Kudu-Bibliothek.
Cluster-Konfiguration	Der Hadoop-Cluster, den Sie für die Verbindung verwenden.

Eigenschaften der LDAP-Verbindung

Verwenden Sie eine LDAP-Verbindung, um eine Verbindung zu einem LDAP-Objekt herzustellen.

In der folgenden Tabelle werden die Eigenschaften einer LDAP-Verbindung beschrieben:

Eigenschaft	Beschreibung
Name	Der Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die maximale Länge beträgt 128 Zeichen. Das Leer- und die folgenden Sonderzeichen sind möglich: ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
ID	Die Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Die Informatica-Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Der Verbindungstyp. Wählen Sie LDAP aus.
Hostname	Hostname des LDAP-Verzeichnisseservers. Standardwert ist „localhost“.
Port	Portnummer des LDAP-Verzeichnisseservers. Standardwert ist 389.
Anonyme Verbindung	Stellt eine anonyme Verbindung zum LDAP-Verzeichnisservers her. Wählen Sie „Anonyme Verbindung“ aus, um als anonymer Benutzer ohne Authentifizierung auf einen Verzeichnisservers zuzugreifen. Hinweis: Sie können keine anonyme Verbindung mit Active Directory herstellen.

Eigenschaft	Beschreibung
Benutzername	Der LDAP-Benutzername für die Verbindung mit dem LDAP-Verzeichnisserver.
Passwort	Das Passwort für die Verbindung mit dem LDAP-Verzeichnisserver.
Sichere Verbindung	Richtet über das TLS-Protokoll eine sichere Verbindung zum LDAP-Verzeichnisserver ein.
TrustStore-Dateiname	Der Dateiname des Truststores, der das TLS-Zertifikat für die Einrichtung einer sicheren Verbindung zum LDAP-Verzeichnisserver enthält. Standardwert ist <code>infa_truststore.jks</code> . Erforderlich, wenn Sie „Sichere Verbindung“ auswählen. Bitten Sie den LDAP-Administrator um den Namen und das Passwort der Truststore-Datei.
TrustStore-Passwort	Das Passwort für die Truststore-Datei, die das SSL-Zertifikat enthält.
Name der Schlüsselspeicherdatei	Der Dateiname des Schlüsselspeichers, der die Schlüssel und Zertifikate enthält, die zum Einrichten sicherer Kommunikation mit dem LDAP-Verzeichnisserver benötigt werden. Erforderlich, wenn Sie „Sichere Verbindung“ auswählen. Bitten Sie den LDAP-Administrator um den Namen und das Passwort der Schlüsselspeicherdatei.
Schlüsselspeicherpasswort	Das Passwort für die Schlüsselspeicherdatei, das für sichere Kommunikation erforderlich ist.

Eigenschaften der Microsoft Azure Blob Storage-Verbindung

Verwenden Sie für den Zugriff auf Microsoft Azure Blob Storage eine Microsoft Azure SQL Blob Storage-Verbindung.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

Sie können eine Microsoft Azure Blob Storage-Verbindung im Administrator Tool oder im Developer Tool erstellen und verwalten. In der folgenden Tabelle werden die Eigenschaften der Microsoft Azure Blob Storage-Verbindung beschrieben:

Eigenschaft	Beschreibung
Name	Name der Microsoft Azure Blob Storage-Verbindung.
ID	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Beschreibung der Verbindung.

Eigenschaft	Beschreibung
Speicherort	Die Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Typ der Verbindung. Wählen Sie „Azure Blob Storage“ aus.

Die Registerkarte **Verbindungsdetails** enthält die Verbindungsattribute der Microsoft Azure Blob Storage-Verbindung. In der folgenden Tabelle werden die Verbindungsattribute beschrieben:

Eigenschaft	Beschreibung
Kontoname	Name des Microsoft Azure Storage-Kontos.
Autorisierungstyp	Autorisierungstyp. Sie können einen der folgenden Autorisierungsmechanismen auswählen: <ul style="list-style-type: none"> - Gemeinsame Schlüsselautorisierung - Gemeinsame Zugriffssignaturen
Kontoschlüssel	Microsoft Azure Storage-Zugriffsschlüssel. Gilt, wenn Sie die gemeinsame Schlüsselautorisierung auswählen.
SAS-Token	SAS-URI mit SAS-Token, das Sie im Microsoft Azure-Portal für Ihr Konto erstellt haben. Gilt, wenn Sie den Autorisierungstyp „Gemeinsame Zugriffssignaturen“ ausgewählt haben. Hinweis: Sie müssen einen gültigen SAS-URI mit einem gültigen SAS-Token bereitstellen.
Containername	Der Root-Container oder die Unterordner mit dem absoluten Pfad. Hinweis: Geben Sie zum Importieren komplexer Dateien nur den Root-Container an.
Endpunktsuffix	Typ der Microsoft Azure-Endpunkte. Sie können einen der folgenden Endpunkte auswählen: <ul style="list-style-type: none"> - <code>core.windows.net</code>: Standard - <code>core.usgovcloudapi.net</code>: Zum Auswählen der Microsoft Azure-Endpunkte (US-Regierung) - <code>core.chinacloudapi.cn</code>: Nicht anwendbar

Microsoft Azure Cosmos DB SQL API-Verbindungseigenschaften

Mit einer Microsoft Azure Cosmos DB-Verbindung können Sie eine Verbindung zur Cosmos DB-Datenbank herstellen. Wenn Sie eine Microsoft Azure Cosmos DB-Verbindung erstellen, geben Sie Informationen für die Metadaten und den Datenzugriff ein.

In der folgenden Tabelle werden die Eigenschaften der Microsoft Azure Cosmos DB-Verbindung beschrieben:

Eigenschaft	Beschreibung
Name	Name der Cosmos DB-Verbindung.
ID	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Das Projekt oder der Ordner im Modellrepository, in dem Sie die Cosmos DB-Verbindung speichern möchten.
Typ	Wählen Sie die Microsoft Azure Cosmos DB SQL API aus.
URI der Cosmos-Datenbank	Die URI des Microsoft Azure Cosmos DB-Kontos.
Schlüssel	Der Primär- und Sekundärschlüssel, mit dem Sie vollständigen administrativen Zugriff auf die Ressourcen innerhalb des Microsoft Azure Cosmos DB-Kontos erhalten.
Datenbank	Name der Datenbank, die die Sammlungen enthält, aus denen Sie JSON-Dokumente lesen oder in die Sie JSON-Dokumente schreiben möchten.

Hinweis: Sie finden die Cosmos DB-URI- und -Schlüsselwerte in den **Keys**-Einstellungen auf dem Azure-Portal. Weitere Details erfahren Sie von Ihrem Azure-Administrator.

Eigenschaften der Microsoft Azure Data Lake Storage Gen1-Verbindung

Verwenden Sie eine Microsoft Azure Data Lake Storage Gen1-Verbindung, um auf Microsoft Azure Data Lake Storage Gen1 zuzugreifen.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

Sie können eine Microsoft Azure Data Lake Storage Gen1-Verbindung im Administrator Tool oder im Developer Tool erstellen und verwalten. In der folgenden Tabelle werden die Eigenschaften der Microsoft Azure Data Lake Storage Gen1-Verbindung beschrieben:

Eigenschaft	Beschreibung
Name	Der Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung ändern. Der Name darf maximal 128 Zeichen umfassen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * () - + = { [] \ : ; " ' < , > . ? /
ID	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 4.000 Zeichen enthalten.
Speicherort	Die Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Der Verbindungstyp. Wählen Sie „Microsoft Azure Data Lake Storage Gen1“ aus.

In der folgenden Tabelle werden die Eigenschaften für den Metadatenzugriff beschrieben:

Eigenschaft	Beschreibung
ADLS-Kontoname	Der Name des Microsoft Azure Data Lake Storage Gen1-Kontos.
Client-ID	Die ID der Anwendung, in der die OAuth-Authentifizierung in Active Directory abgeschlossen werden soll.
Geheimer Clientschlüssel	Der geheime Schlüssel des Clients, mit dem die OAuth-Authentifizierung in Active Directory abgeschlossen werden soll.
Verzeichnis	Das Microsoft Azure Data Lake Storage Gen1-Verzeichnis, das Sie zum Lesen oder Schreiben von Daten verwenden. Der Standardeinstellung ist das Root-Verzeichnis.
AuthEndpoint	Der Endpunkt des OAuth 2.0-Tokens, von dem aus der Zugriffscode basierend auf der Client-ID generiert und der geheime Client-Schlüssel fertiggestellt wird.

Weitere Informationen zum Erstellen einer Client-ID, eines Clientschlüssel und eines Authentifizierungsendpunkts erhalten Sie beim Azure-Administrator oder in der Dokumentation zu Microsoft Azure Data Lake Storage Gen1.

Eigenschaften der Microsoft Azure Data Lake Storage Gen2-Verbindung

Verwenden Sie eine Microsoft Azure Data Lake Storage Gen2-Verbindung, um auf Microsoft Azure Data Lake Storage Gen2 zuzugreifen.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

Sie können eine Microsoft Azure Data Lake Storage Gen2-Verbindung im Administrator Tool oder im Developer Tool erstellen und verwalten. In der folgenden Tabelle werden die Eigenschaften der Microsoft Azure Data Lake Storage Gen2-Verbindung beschrieben:

Eigenschaft	Beschreibung
Name	Der Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung ändern. Der Name darf maximal 128 Zeichen umfassen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * () - + = { [] \ : ; " ' < , > . ? /
ID	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 4.000 Zeichen enthalten.
Speicherort	Die Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Der Verbindungstyp. Wählen Sie „Microsoft Azure Data Lake Storage Gen2“ aus.

In der folgenden Tabelle werden die Eigenschaften für den Metadatenzugriff beschrieben:

Eigenschaft	Beschreibung
Kontoname	Der Konto- oder Dienstname in Microsoft Azure Data Lake Storage Gen2.
Authentifizierungstyp	Authentifizierungstyp für den Zugriff auf das Microsoft Azure Data Lake Storage Gen2-Konto. Wählen Sie eine der folgenden Optionen aus: <ul style="list-style-type: none">- Dienstprinzipal-Authentifizierung. Wählen Sie diese Option aus, um die Client-ID, den geheimen Clientschlüssel und die Mandanten-ID zum Herstellen einer Verbindung mit Microsoft Azure Data Lake Storage Gen2 zu verwenden.- Authentifizierung mit gemeinsam verwendetem Schlüssel. Wählen Sie diese Option aus, um den Kontoschlüssel zum Herstellen einer Verbindung mit Microsoft Azure Data Lake Storage Gen2 zu verwenden. Hinweis: Sie können die Authentifizierung mit gemeinsam verwendetem Schlüssel nicht in einem Streaming-Mapping verwenden.
Client-ID	Gilt für die Dienstprinzipal-Authentifizierung. Die ID der Anwendung zum Abschließen der OAuth-Authentifizierung in Azure Active Directory (AD).

Eigenschaft	Beschreibung
Geheimer Clientschlüssel	Gilt für die Dienstprinzipal-Authentifizierung. Der geheime Clientschlüssel zum Abschließen der OAuth-Authentifizierung im Azure Active Directory.
Mandanten-ID	Gilt für die Dienstprinzipal-Authentifizierung. Die Verzeichnis-ID für das Azure Active Directory.
Kontoschlüssel	Gilt für die Authentifizierung mit gemeinsam verwendetem Schlüssel. Der Kontoschlüssel für das Microsoft Azure Data Lake Storage Gen2-Konto.
Name des Dateisystems	Der Name eines vorhandenen Dateisystems in Microsoft Azure Data Lake Storage Gen2.
Verzeichnispfad	Der Pfad eines vorhandenen Verzeichnisses ohne den Namen des Dateisystems. Ein Standardverzeichnis ist nicht vorhanden. Sie können eine der folgenden Syntaxen auswählen: <ul style="list-style-type: none"> - / für Root-Verzeichnis. - /dir1 - dir1/dir2
Adls Gen2-Endpunkt	Typ von Microsoft Azure-Endpunkten. Sie können einen der folgenden Endpunkte auswählen: <ul style="list-style-type: none"> - core.windows.net: Standard - core.usgovcloudapi.net: Zur Auswahl der Azure Government-Endpunkte

Weitere Informationen zum Erstellen einer Client-ID, eines geheimen Clientschlüssels, einer Mandanten-ID und eines Dateisystemnamens erhalten Sie beim Azure-Administrator oder in der Dokumentation zu Microsoft Azure Data Lake Storage Gen2.

Eigenschaften der Microsoft Azure SQL Data Warehouse-Verbindung

Verwenden Sie für den Zugriff auf ein Microsoft Azure SQL Data Warehouse eine Microsoft Azure SQL Data Warehouse-Verbindung.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

Sie können eine Microsoft Azure SQL Data Warehouse-Verbindung im Administrator Tool oder im Developer Tool erstellen und verwalten. In der folgenden Tabelle werden die Eigenschaften der Microsoft Azure SQL Data Warehouse-Verbindung beschrieben:

Eigenschaft	Beschreibung
Name	Der Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung ändern. Der Name darf maximal 128 Zeichen umfassen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * () - + = { [] \ : ; " ' < , > . ? /
ID	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 4.000 Zeichen enthalten.
Speicherort	Die Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Der Verbindungstyp. Wählen Sie „Azure SQL Data Warehouse“ aus.

In der folgenden Tabelle werden die Eigenschaften für den Metadatenzugriff beschrieben:

Eigenschaft	Beschreibung
Azure DW-JDBC-URL	JDBC-Verbindungszeichenfolge von Microsoft Azure Data Warehouse. Sie können beispielsweise folgende Verbindungszeichenfolge eingeben: jdbc:sqlserver:// <Server>.database.windows.net:1433;database=<Datenbank> Der Administrator kann die URL vom Microsoft Azure-Portal herunterladen.
Azure DW-JDBC-Benutzername	Benutzername für die Verbindung zum Microsoft Azure SQL Data Warehouse-Konto. Sie müssen über die Berechtigung zum Lesen, Schreiben und Kürzen von Daten in Microsoft Azure SQL Data Warehouse verfügen.
Azure DW-JDBC-Passwort	Passwort für die Verbindung zum Microsoft Azure SQL Data Warehouse-Konto.
Azure DW-Schemaname	Name des Schemas in Microsoft Azure SQL Data Warehouse.
Azure-Speichertyp	Der Typ des Azure-Speichers zum Bereitstellen der Dateien. Sie können einen der folgenden Speichertypen auswählen: - Azure Blob. Standard. Zur Verwendung von Microsoft Azure Blob Storage zum Bereitstellen der Dateien. - ADLS Gen2. Zur Verwendung von Microsoft Azure Data Lake Storage Gen2 als Speicher zum Bereitstellen der Dateien.
Azure Blob-Kontoname	Name des Microsoft Azure Storage-Kontos zum Bereitstellen der Dateien.
Schlüssel des Azure Blob-Kontos	Der Schlüssel zur Authentifizierung des Zugriffs auf das Konto des Blob-Speichers.
Name des ADLS Gen2-Speicherkontos	Name des Microsoft Azure Data Lake Storage Gen2-Kontos zum Bereitstellen der Dateien.

Eigenschaft	Beschreibung
Schlüssel des ADLS Gen2-Kontos	Microsoft Azure Data Lake Storage Gen2-Zugriffsschlüssel zum Bereitstellen der Dateien.
Blob-Endpunkt	<p>Typ von Microsoft Azure-Endpunkten.</p> <p>Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> - <code>core.windows.net</code>: Standard - <code>core.usgovcloudapi.net</code>: Wählen Sie diese Option aus, um auf die Microsoft Azure Data Warehouse-Endpunkte der US-Regierung zuzugreifen. - <code>core.chinacloudapi.cn</code>: Wählen Sie diese Option aus, um auf einen Microsoft Azure Data Warehouse-Endpunkt in der Region China zuzugreifen. <p>Sie können die Microsoft Azure-Endpunkte (US-Regierung) konfigurieren, wenn ein Mapping in der nativen Umgebung und auf der Spark-Engine ausgeführt wird.</p>
VNet-Regel	Aktivieren Sie diese Option, um eine Verbindung zu einem Microsoft Azure SQL Data Warehouse-Endpunkt herzustellen, der sich in einem virtuellen Netzwerk (VNet) befindet.

Hinweis: Stellen Sie sicher, dass die Eigenschaft **Externe Datenquelle** leer gelassen wird. Obwohl diese Option in der Benutzeroberfläche sichtbar ist, ist sie nicht mit PowerExchange für Microsoft Azure Data Warehouse kompatibel. .

MS SQL Server-Verbindungseigenschaften

Verwenden Sie eine Microsoft SQL Server-Verbindung für den Zugriff auf Microsoft SQL Server. Eine Microsoft SQL Server-Verbindung ist eine Verbindung zu einer relationalen Microsoft SQL Server-Datenbank. Sie können eine Microsoft SQL Server-Verbindung im Administrator Tool oder im Developer Tool erstellen und verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die MS SQL Server-Verbindungseigenschaften beschrieben:

Eigenschaft	Beschreibung
Datenbanktyp	Der Datenbanktyp.
Name	<p>Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten:</p> <p>~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /</p>
ID	<p>Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.</p>
Beschreibung	Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.

Eigenschaft	Beschreibung
Vertrauenswürdige Verbindung verwenden	Ermöglicht dem Anwendungsdienst, Windows-Authentifizierung für den Zugriff auf die Datenbank zu verwenden. Der Benutzername, der den Anwendungsdienst startet, muss ein gültiger Windows-Benutzer mit Zugriff auf die Datenbank sein. Diese Option ist standardmäßig deaktiviert. Hinweis: Windows- und NTLM-Authentifizierung sind nicht für eine Microsoft SQL Server 2017-Version zertifiziert, die unter Linux gehostet wird.
Benutzername	Der Benutzername der Datenbank. Erforderlich, wenn der Microsoft SQL Server NTLMv1- oder NTLMv2-Authentifizierung verwendet.
Passwort	Das Passwort für den Benutzernamen der Datenbank. Erforderlich, wenn der Microsoft SQL Server NTLMv1- oder NTLMv2-Authentifizierung verwendet.
Pass-Through-Sicherheit aktiviert	Aktiviert Pass-Through-Sicherheit für die Verbindung. Wenn Sie Pass-Through-Sicherheit für eine Verbindung aktivieren, verwendet die Domäne nicht die im Verbindungsobjekt definierten Anmeldeinformationen, sondern den Benutzernamen und das Passwort des Clients, um sich an der entsprechenden Datenbank anzumelden.
Eigenschaften für den Metadaten-Zugriff: Verbindungszeichenfolge	<p>Verbindungszeichenfolge für den Zugriff auf Metadaten in der Datenbank. Verwenden Sie die folgende Verbindungszeichenfolge:</p> <pre>jdbc:informatica:sqlserver://<host name>:<port>;DatabaseName=<database name></pre> <p>Beziehen Sie zum Testen der Verbindung mit NTLM-Authentifizierung die folgenden Parameter in die Verbindungszeichenfolge ein:</p> <ul style="list-style-type: none"> - AuthenticationMethod. Die zu verwendende Version der NTLM-Authentifizierung. <p>Hinweis: UNIX unterstützt NTLMv1 und NTLMv2, jedoch nicht NTLM.</p> <ul style="list-style-type: none"> - Domäne. Die Domäne, zu der der SQL Server gehört. <p>Die folgenden Beispiel zeigt die Verbindungszeichenfolge für einen SQL Server, der NTLMv2-Authentifizierung in einer NT-Domäne namens Informatica.com verwendet:</p> <pre>jdbc:informatica:sqlserver://host01:1433;DatabaseName=SQL1;AuthenticationMethod=ntlm2java;Domain=Informatica.com</pre> <p>Wenn Sie eine Verbindung über NTLM-Authentifizierung herstellen, können Sie in den MS SQL Server-Verbindungseigenschaften die Option Verwenden Sie trusted Verbindung aktivieren. Wenn Sie eine Verbindung über NTLMv1- oder NTLMv2-Authentifizierung herstellen, müssen Sie den Benutzernamen und das Kennwort in den Verbindungseigenschaften angeben.</p>

Eigenschaft	Beschreibung
AdvancedJDBCSecurityOptions	<p>Datenbankparameter für Metadata-Zugriff auf eine sichere Datenbank. Informatica behandelt den Wert des AdvancedJDBCSecurityOptions-Felds als vertrauliche Daten und speichert die Parameterzeichenfolge als Verschlüsselung.</p> <p>Um eine Verbindung zu einer sicheren Datenbank herzustellen, beziehen Sie die folgenden Parameter mit ein:</p> <ul style="list-style-type: none"> - EncryptionMethod. 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 vom Datenbankserver gesendet wird. Wenn dieser Parameter auf "True" gesetzt wird, validiert Informatica das vom Datenbankserver gesendete Zertifikat. Wenn Sie den HostNameInCertificate-Parameter angeben, validiert Informatica ebenfalls den Hostnamen im Zertifikat. Wenn dieser Parameter auf "False" festgelegt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat nicht. Informatica ignoriert alle Truststore-Informationen, die Sie angeben. - HostNameInCertificate. Optional. Hostname des Computers, auf dem die sichere Datenbank gehostet wird. Wenn Sie einen Hostnamen angeben, validiert Informatica den Hostnamen in der Verbindungszeichenfolge mit dem Hostnamen im SSL-Zertifikat. - cryptoProtocolVersion. Optional. Wenn Sie TLS für die Microsoft SQL Server-Instanz aktivieren, legen Sie den Parameter cryptoProtocolVersion wie folgt fest: cryptoProtocolVersion=TLSv<version number>. Beispiel: cryptoProtocolVersion=TLSv1.2 Hinweis: Die Versionsnummer muss mit der TLS-Version übereinstimmen, die für den Server konfiguriert wurde. - TrustStore. Erforderlich. Pfad und Dateiname der Truststore-Datei. Hinweis: Wenn Sie SSL oder TLS konfigurieren und nur den Dateinamen angeben, müssen Sie die Truststore-Datei in das folgende Verzeichnis kopieren, um die Verbindung zu testen: <Informatica server installation directory>/tomcat/bin - TrustStorePassword Erforderlich. Passwort der Truststore-Datei für die sichere Datenbank. <p>Nicht anwendbar auf ODBC. Hinweis: Informatica hängt die sichere JDBC-Parameter an die Verbindungszeichenfolge an. Wenn Sie die sicheren JDBC-Parameter direkt in der Verbindungszeichenfolge einschließen, geben Sie keinen Parameter in das Feld AdvancedJDBCSecurityOptions ein.</p>
Datenzugriffseigenschaften: Providertyp	<p>Der Verbindungsprovider, den Sie für eine Verbindung zur Microsoft SQL-Serverdatenbank nutzen möchten.</p> <p>Sie können die folgenden Providertypen auswählen:</p> <ul style="list-style-type: none"> - ODBC - OLDEB (veraltet) <p>Standardwert ist ODBC.</p> <p>Hinweis: Obwohl der Providertyp OLEDB auf der Benutzeroberfläche der Microsoft SQL Server-Verbindung als veraltet angezeigt wird, unterstützt Informatica diesen Providertyp. Weitere Informationen zur Unterstützung des Providertyps OLEDB finden Sie in folgendem Artikel der Wissensdatenbank KB 522895.</p>

Eigenschaft	Beschreibung
DSN verwenden	<p>Ermöglicht dem Datenintegrationsdienst die Verwendung des Datenquellennamens (DSN – Data Source Name) für die Verbindung. Wenn Sie die Option „DSN verwenden“ auswählen, ruft der Datenintegrationsdienst die Namen der Datenbank und des Servers aus dem DSN ab.</p> <p>Wenn Sie die Option „DSN verwenden“ nicht auswählen, müssen Sie die Namen der Datenbank und des Servers angeben.</p>
Verbindungsstring	<p>Verwenden Sie den folgenden Verbindungsstring, wenn Sie den DSN-Modus aktivieren möchten:</p> <pre><server name>@<database name></pre> <p>Wenn Sie den DSN-Modus aktivieren, verwenden Sie die folgenden Verbindungsstrings:</p> <pre><DSN Name></pre>
Codepage	Die Codepage, die zum Lesen aus einer Quelldatenbank oder zum Schreiben in eine Zieldatenbank oder Zieldatei verwendet wird.
Domänenname	Der Name der Domäne.
Paketgröße	Die zum Übertragen der Daten verwendete Paketgröße. Dient zur Optimierung der nativen Treiber für Microsoft SQL Server.
Eigentümername	<p>Der Name des Schemaeigentümers.</p> <p>Hinweis: Wenn Sie ein Tabellen-DDL über ein dynamisches Mapping erzeugen oder über die Option DDL generieren und ausführen, enthalten die DDL-Metadaten nicht den Schemanamen und die Eigenschaften des Eigentümernamens.</p>
Schemaname	<p>Der Name des Schemas in der Datenbank. Sie müssen den Schemanamen für das Profiling-Warehouse angeben, wenn der Schemaname anders lautet als der Benutzername für die Datenbank. Sie müssen den Schemanamen für die Datenobjekt-Cache-Datenbank angeben, wenn der Schemaname nicht mit dem Datenbank-Benutzernamen übereinstimmt und Sie benutzerverwaltete Cache-Tabellen konfigurieren.</p> <p>Hinweis: Wenn Sie ein Tabellen-DDL über ein dynamisches Mapping erzeugen oder über die Option DDL generieren und ausführen, enthalten die DDL-Metadaten nicht den Schemanamen und die Eigenschaften des Eigentümernamens.</p>
Umgebungs-SQL	SQL-Befehle zum Einrichten der Datenbankumgebung beim Herstellen einer Verbindung zur Datenbank. Der Datenintegrationsdienst führt die Verbindungsumgebungs-SQL bei jeder Verbindung mit der Datenbank aus.
Transaktions-SQL	SQL-Befehle zum Einrichten der Datenbankumgebung beim Herstellen einer Verbindung zur Datenbank. Der Datenintegrationsdienst führt die Verbindungsumgebungs-SQL zu Beginn jeder Transaktion aus.
Wiederholungsperiode	Diese Eigenschaft ist für die zukünftige Verwendung reserviert.

Eigenschaft	Beschreibung
SQL-ID-Zeichen	<p>Art des Zeichens, das von der Datenbank verwendet wird, um Delimiter-IDs in SQL-Abfragen einzuschließen. Die verfügbaren Zeichen richten sich nach dem Datenbanktyp.</p> <p>Wählen Sie (Keine) aus, wenn die Datenbank reguläre IDs verwendet. Wenn der Datenintegrationsdienst SQL-Abfragen erzeugt, schließt der Dienst IDs nicht in Delimiter-Zeichen ein.</p> <p>Wählen Sie ein Zeichen aus, wenn die Datenbank Delimiter-IDs verwendet. Wenn der Datenintegrationsdienst SQL-Abfragen erzeugt, schließt der Dienst Delimiter-IDs in dieses Zeichen ein.</p>
Unterstützte IDs für gemischte Groß-/Kleinschreibung	<p>Aktivieren Sie diese Eigenschaft, wenn die Datenbank IDs für gemischte Groß-/Kleinschreibung verwendet. Bei aktivierter Eigenschaft schließt der Datenintegrationsdienst alle IDs innerhalb des Zeichens ein, das für die Eigenschaft SQL-Kennungszeichen ausgewählt wurde.</p> <p>Wenn die Eigenschaft SQL-Kennungszeichen auf „Kein“ festgelegt ist, wird die Eigenschaft Unterstützte IDs für gemischte Groß-/Kleinschreibung deaktiviert.</p>
ODBC-Provider	<p>ODBC. Der Datenbanktyp, zu dem ODBC eine Verbindung herstellt. Geben Sie zur Pushdown-Optimierung den Datenbanktyp an, damit der Datenintegrationsdienst die native Datenbank-SQL generieren kann.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> - Andere - Sybase - Microsoft_SQL_Server <p>Standardwert ist „Andere“.</p>

Eigenschaften von Netezza-Verbindungen

Verwenden Sie eine Netezza-Verbindung für den Zugriff auf eine Netezza-Datenbank. Die Netezza-Verbindung ist eine Datenbank-Verbindung. Sie können eine Netezza-Verbindung im Administrator Tool oder im Developer Tool verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Eigenschaften von Netezza-Verbindungseigenschaften erläutert:

Eigenschaft	Beschreibung
Name	<p>Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten:</p> <p>~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /</p>
ID	<p>Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.</p>

Eigenschaft	Beschreibung
Beschreibung	Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Die Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Verbindungstyp. Wählen Sie Netezza aus.
Benutzername	Benutzername mit den entsprechenden Berechtigungen für den Zugriff auf die Netezza-Datenbank.
Passwort	Passwort für den Datenbankbenutzernamen.
JDBC-URL	JDBC-URL, die vom Developer Tool beim Herstellen einer Verbindung zur Netezza-Datenbank verwendet werden muss. Verwenden Sie das folgende Format: <code>jdbc:netezza://<Hostname>:<Port>/<Datenbankname></code>
Verbindungszeichenfolge	Name der ODBC-Datenquelle, die Sie zum Herstellen einer Verbindung zur Netezza-Datenbank verwenden möchten.
Timeout	Zeit in Sekunden, die das Developer Tool auf eine Antwort von der Netezza-Datenbank wartet, ehe es die Verbindung schließt.

Eigenschaften von OData-Verbindungen

Verwenden Sie eine OData-Verbindung für den Zugriff auf eine OData-URL. Die OData-Verbindung ist eine Web-Verbindung. Sie können eine OData-Verbindung im Administrator Tool oder im Developer Tool erstellen und verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Eigenschaften von OData-Verbindungseigenschaften erläutert:

Eigenschaft	Beschreibung
Name	Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: <code>~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /</code>
ID	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 4.000 Zeichen enthalten.

Eigenschaft	Beschreibung
Speicherort	Die Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Verbindungstyp. Wählen Sie OData aus.
Benutzername	Optional. Benutzername mit den entsprechenden Leseberechtigungen für die OData-Ressource.
Passwort	Optional. Passwort für den Benutzernamen der OData-URL.
URL	Root-URL des OData-Diensts, die die Daten bereitstellt, die Sie lesen möchten.
Sicherheitstyp	Optional. Sicherheitsprotokoll, das das Developer Tool verwenden muss, um eine sichere Verbindung mit dem OData-Server herzustellen. Wählen Sie einen der folgenden Werte aus: <ul style="list-style-type: none"> - Keine - SSL - TLS Standardwert ist „Keine“.
TrustStore-Dateiname	Erforderlich, wenn Sie einen Sicherheitstyp auswählen Name der Truststore-Datei, die das öffentliche Zertifikat für den OData-Server enthält. Standardwert ist <code>infa_truststore.jks</code> .
Passwort	Erforderlich, wenn Sie einen Sicherheitstyp auswählen Passwort für die Truststore-Datei, die das öffentliche Zertifikat für den OData-Server enthält.
KeyStore-Dateiname	Erforderlich, wenn Sie einen Sicherheitstyp auswählen Name der Schlüsselspeicherdatei, die den privaten Schlüssel für den OData-Server enthält. Standardwert ist <code>infa_truststore.jks</code> .
Passwort	Erforderlich, wenn Sie einen Sicherheitstyp auswählen Passwort für die Schlüsselspeicherdatei, die den privaten Schlüssel für den OData-Server enthält.

ODBC-Verbindungseigenschaften

Verwenden Sie eine ODBC-Verbindung für den Zugriff auf ODBC-Daten. Eine ODBC-Verbindung ist eine relationale Datenbankverbindung. Sie können eine ODBC-Verbindung im Administrator tool, Developer tool oder Analyst Tool erstellen und verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Eigenschaften von ODBC-Verbindungen erläutert:

Eigenschaft	Beschreibung
Datenbanktyp	Der Datenbanktyp.
Name	Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
ID	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Benutzername	Der Benutzername der Datenbank.
Passwort	Das Passwort für den Benutzernamen der Datenbank.
Pass-Through-Sicherheit aktiviert	Aktiviert Pass-Through-Sicherheit für die Verbindung. Wenn Sie Pass-Through-Sicherheit für eine Verbindung aktivieren, verwendet die Domäne nicht die im Verbindungsobjekt definierten Anmeldeinformationen, sondern den Benutzernamen und das Passwort des Clients, um sich an der entsprechenden Datenbank anzumelden.
Eigenschaften für den Datenzugriff: Verbindungszeichenfolge	ODBC-Verbindungs-URL für den Zugriff auf Metadaten in der Datenbank. <Name der Datenquelle>
Codepage	Die Codepage, die zum Lesen aus einer Quelldatenbank oder zum Schreiben in eine Zieldatenbank oder Zieldatei verwendet wird.
Umgebungs-SQL	SQL-Befehle zum Einrichten der Datenbankumgebung beim Herstellen einer Verbindung zur Datenbank. Der Datenintegrationsdienst führt die Verbindungsumgebungs-SQL bei jeder Verbindung mit der Datenbank aus.
Transaktions-SQL	SQL-Befehle zum Einrichten der Datenbankumgebung beim Herstellen einer Verbindung zur Datenbank. Der Datenintegrationsdienst führt die Verbindungsumgebungs-SQL zu Beginn jeder Transaktion aus.
Wiederholungsperiode	Diese Eigenschaft ist für die zukünftige Verwendung reserviert.
SQL-Kennungszeichen	Art des Zeichens, das von der Datenbank verwendet wird, um Delimiter-IDs in SQL-Abfragen einzuschließen. Die verfügbaren Zeichen richten sich nach dem Datenbanktyp. Wählen Sie (Keine) aus, wenn die Datenbank reguläre IDs verwendet. Wenn der Datenintegrationsdienst SQL-Abfragen erzeugt, schließt der Dienst IDs nicht in Delimiter-Zeichen ein. Wählen Sie ein Zeichen aus, wenn die Datenbank Delimiter-IDs verwendet. Wenn der Datenintegrationsdienst SQL-Abfragen erzeugt, schließt der Dienst Delimiter-IDs in dieses Zeichen ein.

Eigenschaft	Beschreibung
Unterstützte Kennungen für gemischte Groß-/Kleinschreibung	Aktivieren Sie diese Eigenschaft, wenn die Datenbank IDs für gemischte Groß-/Kleinschreibung verwendet. Bei aktivierter Eigenschaft schließt der Datenintegrationsdienst alle IDs innerhalb des Zeichens ein, das für die Eigenschaft SQL-Kennungszeichen ausgewählt wurde. Wenn die Eigenschaft SQL-Kennungszeichen auf „Kein“ festgelegt ist, wird die Eigenschaft Unterstützte IDs für gemischte Groß-/Kleinschreibung deaktiviert.
ODBC-Provider	Der Datenbanktyp, zu dem ODBC eine Verbindung herstellt. Geben Sie zur Pushdown-Optimierung den Datenbanktyp an, damit der Datenintegrationsdienst die native Datenbank-SQL generieren kann. Mögliche Werte: <ul style="list-style-type: none"> - Andere - Sybase - Microsoft_SQL_Server - Snowflake Standardwert ist „Andere“.

Hinweis: Verwenden Sie eine ODBC-Verbindung, um eine Verbindung zu Microsoft SQL Server herzustellen, wenn der Datenintegrationsdienst unter UNIX oder Linux ausgeführt wird. Verwenden Sie eine native Verbindung zu Microsoft SQL Server, wenn der Datenintegrationsdienst unter Windows ausgeführt wird.

Eigenschaften für Oracle-Verbindungen

Verwenden Sie eine Oracle-Verbindung, um eine Verbindung zu einer Oracle-Datenbank herzustellen. Die Oracle-Verbindung ist eine relationale Verbindung. Sie können eine Oracle-Verbindung im Administrator Tool, Developer Tool oder Analyst Tool erstellen und verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Eigenschaften von Oracle-Verbindungen erläutert:

Eigenschaft	Beschreibung
Datenbanktyp	Der Datenbanktyp.
Name	Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
ID	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Benutzername	Der Benutzername der Datenbank.

Eigenschaft	Beschreibung
Passwort	Das Passwort für den Benutzernamen der Datenbank.
Pass-Through-Sicherheit aktiviert	Aktiviert Pass-Through-Sicherheit für die Verbindung. Wenn Sie Pass-Through-Sicherheit für eine Verbindung aktivieren, verwendet die Domäne nicht die im Verbindungsobjekt definierten Anmeldeinformationen, sondern den Benutzernamen und das Passwort des Clients, um sich an der entsprechenden Datenbank anzumelden.
Eigenschaften für den Metadaten-Zugriff: Verbindungszeichenfolge	<p>Verbindungszeichenfolge für den Zugriff auf Metadaten in der Datenbank. Verwenden Sie die folgende Verbindungszeichenfolge:</p> <pre>jdbc:informatica:oracle://<host_name>:<port>;SID=<database name></pre> <p>Verwenden Sie die folgende Verbindungszeichenfolge, um über Oracle Connection Manager eine Verbindung zu einer Oracle-Datenbank herzustellen:</p> <pre>jdbc:informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS server name>;</pre>

Eigenschaft	Beschreibung
AdvancedJDBCSecurityOptions	<p>Datenbankparameter für Metadata-Zugriff auf eine sichere Datenbank. Informatica behandelt den Wert des AdvancedJDBCSecurityOptions-Felds als vertrauliche Daten und speichert die Parameterzeichenfolge als Verschlüsselung.</p> <p>Um eine Verbindung zu einer sicheren Datenbank herzustellen, beziehen Sie die folgenden Parameter mit ein:</p> <ul style="list-style-type: none"> - EncryptionMethod. Erforderlich. Gibt an, ob Daten bei der Netzwerkübertragung verschlüsselt werden. Dieser Parameter muss auf SSL festgelegt werden. - ValidateServerCertificate. Optional. Gibt an, ob Informatica das Zertifikat validiert, das vom Datenbankserver gesendet wird. Wenn dieser Parameter auf TRUE festgelegt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat. Wenn Sie den HostNameInCertificate-Parameter angeben, validiert Informatica ebenfalls den Hostnamen im Zertifikat. Wenn dieser Parameter auf "false" festgelegt ist, validiert Informatica das vom Datenbankserver gesendete Zertifikat nicht. Informatica ignoriert alle Truststore-Informationen, die Sie angeben. - HostNameInCertificate. Optional. Hostname des Computers, auf dem die sichere Datenbank gehostet wird. Wenn Sie einen Hostnamen angeben, validiert Informatica den Hostnamen in der Verbindungszeichenfolge mit dem Hostnamen im SSL-Zertifikat. - cryptoProtocolVersion. Optional. Wenn Sie TLS für die Oracle-Instanz aktivieren, legen Sie den Parameter cryptoProtocolVersion wie folgt fest: cryptoProtocolVersion=TLSv<version number>. Beispiel: cryptoProtocolVersion=TLSv1.2 Hinweis: Die Versionsnummer muss mit der TLS-Version übereinstimmen, die für den Server konfiguriert wurde. - TrustStore. Erforderlich. Pfad und Dateiname der Truststore-Datei. Hinweis: Wenn Sie SSL oder TLS konfigurieren und nur den Dateinamen angeben, müssen Sie die Truststore-Datei in das folgende Verzeichnis kopieren, um die Verbindung zu testen: <Informatica server installation directory>/tomcat/bin - TrustStorePassword. Erforderlich. Passwort der Truststore-Datei für die sichere Datenbank. - KeyStore. Erforderlich. Pfad und Dateiname der Schlüsselspeicherdatei. - KeyStorePassword. Erforderlich. Passwort der Schlüsselspeicherdatei für die sichere Datenbank. Hinweis: Informatica hängt die sichere JDBC-Parameter an die Verbindungszeichenfolge an. Wenn Sie die sicheren JDBC-Parameter direkt in der Verbindungszeichenfolge einschließen, geben Sie keinen Parameter in das Feld AdvancedJDBCSecurityOptions ein.
Eigenschaften für den Datenzugriff: Verbindungszeichenfolge	<p>Verwenden Sie die folgende Verbindungszeichenfolge:</p> <pre><database name>.world</pre>
Codepage	Die Codepage, die zum Lesen aus einer Quelldatenbank oder zum Schreiben in eine Zieldatenbank oder Zieldatei verwendet wird.
Umgebungs-SQL	SQL-Befehle zum Einrichten der Datenbankumgebung beim Herstellen einer Verbindung zur Datenbank. Der Datenintegrationsdienst führt die Verbindungsumgebungs-SQL bei jeder Verbindung mit der Datenbank aus.

Eigenschaft	Beschreibung
Transaktions-SQL	SQL-Befehle zum Einrichten der Datenbankumgebung beim Herstellen einer Verbindung zur Datenbank. Der Datenintegrationsdienst führt die Verbindungsumgebungs-SQL zu Beginn jeder Transaktion aus.
Wiederholungszeitraum	Diese Eigenschaft ist für die zukünftige Verwendung reserviert.
Parallelmodus aktivieren	Ermöglicht Parallelverarbeitung beim Laden von Daten in eine Tabelle im Bulk-Modus. Diese Option ist standardmäßig deaktiviert.
SQL-Bezeichnerzeichen	<p>Art des Zeichens, das von der Datenbank verwendet wird, um Delimiter-IDs in SQL-Abfragen einzuschließen. Die verfügbaren Zeichen richten sich nach dem Datenbanktyp.</p> <p>Wählen Sie (Keine) aus, wenn die Datenbank reguläre IDs verwendet. Wenn der Datenintegrationsdienst SQL-Abfragen erzeugt, schließt der Dienst IDs nicht in Delimiter-Zeichen ein.</p> <p>Wählen Sie ein Zeichen aus, wenn die Datenbank Delimiter-IDs verwendet. Wenn der Datenintegrationsdienst SQL-Abfragen erzeugt, schließt der Dienst Delimiter-IDs in dieses Zeichen ein.</p>
Bezeichner mit gemischter Groß-/Kleinschreibung unterstützen	<p>Aktivieren Sie diese Eigenschaft, wenn die Datenbank IDs für gemischte Groß-/Kleinschreibung verwendet. Bei aktivierter Eigenschaft schließt der Datenintegrationsdienst alle IDs innerhalb des Zeichens ein, das für die Eigenschaft SQL-Kennungszeichen ausgewählt wurde.</p> <p>Wenn die Eigenschaft SQL-Kennungszeichen auf „Kein“ festgelegt ist, wird die Eigenschaft Unterstützte IDs für gemischte Groß-/Kleinschreibung deaktiviert.</p>

Salesforce-Verbindungseigenschaften

Verwenden Sie eine Salesforce-Verbindung zum Herstellen einer Verbindung zu einem Salesforce-Objekt. Der Salesforce-Verbindung ist ein Anwendungsverbindungstyp. Sie können eine Salesforce-Verbindung im Administrator-Tool oder im Developer-Tool verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Eigenschaften von Salesforce-Verbindungen erläutert:

Eigenschaft	Beschreibung
Name	<p>Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Die maximale Länge beträgt 128 Zeichen. Das Leer- und die folgenden Sonderzeichen sind möglich:</p> <p>~ ` ! \$ % ^ & * () - + = { [] } \ : ; ' ' < , > . ? /</p>
ID	<p>Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.</p>

Eigenschaft	Beschreibung
Beschreibung	Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Die Informatica-Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Der Verbindungstyp. Sie können den Verbindungstypen „Standard“ oder „OAuth“ auswählen.
Benutzername	Anwendbar für den Verbindungstyp „Standard“. Salesforce-Benutzername.
Benutzerpasswort	<p>Anwendbar für den Verbindungstyp „Standard“. Passwort für den Salesforce-Benutzernamen</p> <p>Für den Zugriff auf Salesforce von außerhalb des vertrauenswürdigen Netzwerks Ihres Unternehmens müssen Sie einen Sicherheitstoken an Ihr Passwort anhängen, um sich bei der API oder einem Desktop-Client anzumelden. Um Ihren Sicherheitstoken zu erhalten oder zurückzusetzen, melden Sie sich bei Salesforce an und klicken auf Setup (Einrichten) > My Personal Information (Meine persönlichen Daten) > Reset My Security Token (Meinen Sicherheitstoken zurücksetzen).</p> <p>Beim Passwort wird zwischen Groß- und Kleinschreibung unterschieden.</p>
Dienst-URL	<p>URL des Salesforce-Diensts, auf den Sie zugreifen möchten</p> <p>Beispiel:</p> <p><code>https://login.salesforce.com/services/Soap/u/<version></code></p> <p>In einer Test- oder Entwicklungsumgebung möchten Sie möglicherweise auf die Salesforce-Sandbox-Testumgebung zugreifen. Weitere Informationen zur Salesforce-Sandbox finden Sie in der Salesforce-Dokumentation.</p>
Aktualisierungs-Token	Anwendbar für den Verbindungstyp „OAuth“. Aktualisierungs-Token von Salesforce.
Verbraucherschlüssel	Anwendbar für den Verbindungstyp „OAuth“. Der von Salesforce bereitgestellte Verbraucherschlüssel, der zum Erzeugen des Aktualisierungstokens benötigt wird. Weitere Informationen zum Erzeugen des Verbraucherschlüssels finden Sie in der Salesforce-Dokumentation.
Verbrauchergeheimwort	Anwendbar für den Verbindungstyp „OAuth“. Das von Salesforce bereitgestellte Verbrauchergeheimwort, das zum Erzeugen des Aktualisierungstokens benötigt wird. Weitere Informationen zum Erzeugen des Verbrauchergeheimworts finden Sie in der Salesforce-Dokumentation.

Eigenschaften der Salesforce Marketing Cloud-Verbindung

Verwenden Sie eine Salesforce Marketing Cloud-Verbindung, um eine Verbindung zu einem Salesforce Marketing Cloud-Objekt herzustellen. Sie können eine Salesforce Marketing Cloud-Verbindung im Administrator Tool oder im Developer Tool erstellen und verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Salesforce Marketing Cloud-Verbindungseigenschaften beschrieben:

Verbindungseigenschaft	Beschreibung
Name	Name der Salesforce Marketing Cloud-Verbindung.
ID	Der Datenintegrationsdienst verwendet die ID zur Angabe der Verbindung.
Beschreibung	Optional. Die Beschreibung der Verbindung.
Speicherort	Die Informatica-Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Verbindungstyp. Wählen Sie „Salesforce Marketing Cloud“ aus.
URL der Salesforce Marketing Cloud	<p>Die URL, die der Datenintegrationsdienst zum Herstellen einer Verbindung zu Salesforce Marketing Cloud-WSDL verwendet.</p> <p>Folgende URL ist ein Beispiel für OAuth 1.0 URL: https://webservice.s7.exacttarget.com/etframework.wSDL</p> <p>Folgende URL ist ein Beispiel für OAuth 2.0 URL: <a href="https://<SUBDOMÄNE>.soap.marketingcloudapis.com/etframework.wSDL">https://<SUBDOMÄNE>.soap.marketingcloudapis.com/etframework.wSDL</p> <p>Wichtig: Salesforce wird die OAuth 1.0-APIs bis zum 30. September 2022 verwerfen. Informatica empfiehlt Ihnen, neue und vorhandene Pakete auf OAuth 2.0 zu aktualisieren.</p>
Benutzername	Benutzername des Salesforce Marketing Cloud-Kontos.
Passwort	Passwort für das Salesforce Marketing Cloud-Konto.
Client-ID	Für die Client-ID von Salesforce Marketing Cloud ist das Generieren eines gültigen Zugriffstokens erforderlich.
Geheimer Clientschlüssel	Für den geheimen Schlüssel des Clients von Salesforce Marketing Cloud ist das Generieren eines gültigen Zugriffstokens erforderlich.
Protokollierung aktivieren	Wenn Sie die Protokollierung aktivieren, können Sie das Sitzungsprotokoll für die Aufgaben sehen.
UTC-Offset	Der Sicherheitsagent verwendet die UTC-Offset-Verbindungseigenschaft, um Daten in der UTC-Offset-Zeitzone von der Salesforce Marketing Cloud zu lesen und in sie zu schreiben.
Batch-Größe	<p>Anzahl der Zeilen, die der Sicherheitsagent in einem Batch in das Ziel schreibt.</p> <p>Wenn Sie Daten einfügen oder aktualisieren und den Kontaktschlüssel angeben, werden die der angegebenen Kontakt-ID zugeordneten Daten in einem Batch in der Salesforce Marketing Cloud eingefügt oder aktualisiert. Geben Sie bei einem Upsert der Daten nach Salesforce Marketing Cloud keinen Kontaktschlüssel an.</p>
Mehrere BU aktivieren	Wählen Sie diese Option aus, wenn Ihr Salesforce Marketing Cloud-Konto mehrere Geschäftsbereiche enthält. Sie können die Salesforce Marketing Cloud-Verbindung verwenden, um auf Daten in allen Geschäftsbereichen zuzugreifen.

SAP-Verbindungseigenschaften

Verwenden Sie eine SAP-Verbindung, um auf eine SAP-Tabelle oder ein SAP BW-Objekt zuzugreifen. Bei der SAP-Verbindung handelt es sich um die Verbindung einer Unternehmensanwendung. Sie können eine SAP-Verbindung im Administrator-Tool oder im Developer-Tool verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Eigenschaften von SAP-Verbindungen erläutert:

Eigenschaft	Beschreibung
Benutzername	Erforderlich. Benutzername für das SAP-Quellsystem, auf das Sie zugreifen möchten.
Passwort	Erforderlich. Passwort für den Benutzernamen.
Verbindungstyp	<p>Erforderlich. Typ der Verbindung, die erstellt werden soll.</p> <p>Wählen Sie einen der folgenden Werte aus:</p> <ul style="list-style-type: none">- Anwendung. Erstellen Sie eine Anwendungsverbindung, wenn Sie eine Verbindung zu einem bestimmten SAP-Anwendungsserver herstellen möchten.- Lastausgleich. Erstellen Sie eine Lastausgleichsverbindung, wenn Sie SAP-Lastausgleich verwenden möchten. <p>Standardwert ist „Anwendung“.</p> <p>Je nach ausgewähltem Verbindungstyp werden die entsprechenden Felder der Verbindungseigenschaften im Dialogfeld Verbindungsdetails aktiviert. Das Developer Tool stellt die Felder der Verbindungseigenschaften, die auf einen bestimmten Verbindungstyp nicht anwendbar sind, abgeblendet dar.</p>
Hostname	<p>Erforderlich, wenn Sie eine SAP-Anwendungsverbindung erstellen.</p> <p>Hostname oder IP-Adresse des SAP-Servers, zu dem eine Verbindung hergestellt werden soll.</p>
Systemnummer	<p>Erforderlich, wenn Sie eine SAP-Anwendungsverbindung erstellen.</p> <p>SAP-Systemnummer.</p>
Name des Nachrichtenhosts	<p>Erforderlich, wenn Sie eine SAP-Lastausgleichsverbindung erstellen.</p> <p>Hostname des SAP-Nachrichtenservers.</p>
R3-Name/SysID	<p>Erforderlich, wenn Sie eine SAP-Lastausgleichsverbindung erstellen.</p> <p>Name des SAP-Systems.</p>
Gruppe	<p>Erforderlich, wenn Sie eine SAP-Lastausgleichsverbindung erstellen.</p> <p>Gruppenname des SAP-Anwendungsservers.</p>
Client	Erforderlich. SAP-Clientnummer.
Sprache	<p>Optional. Für Zuordnungen und Arbeitsabläufe zu verwendende Sprache.</p> <p>Muss mit der Codepage des Developer Tools kompatibel sein.</p> <p>Wenn Sie diese Option leer lassen, verwendet das Developer Tool die Standardsprache des SAP-Systems.</p>

Eigenschaft	Beschreibung
Verfolgen	<p>Optional. Verwenden Sie diese Option zum Verfolgen der vom SAP-System durchgeführten JCo-Aufrufe. SAP speichert die Informationen über die JCo-Aufrufe in einer Ablaufverfolgungsdatei.</p> <p>Geben Sie einen der folgenden Werte an:</p> <ul style="list-style-type: none"> - 0. Aus - 1. Vollständig <p>Standardwert ist 0.</p> <p>Über die folgenden Verzeichnisse können Sie auf die Ablaufverfolgungsdateien zugreifen:</p> <ul style="list-style-type: none"> - Verzeichnis <Informatica-Installationsverzeichnis>/tomcat/bin auf dem Computer, auf dem die Informatica-Dienste installiert sind - Verzeichnis <Informatica-Installationsverzeichnis>/clients/DeveloperClient auf dem Computer, auf dem das Developer Tool installiert ist
Zusätzliche Parameter	<p>Optional. Geben Sie einen beliebigen anderen Verbindungsparameter ein, den Sie verwenden möchten.</p> <p>Verwenden Sie das folgende Format:</p> <pre><parameter name>=<value></pre>
Staging-Verzeichnis	Pfad im SAP-System, in dem die Staging-Datei erstellt wird.
Quellverzeichnis	Pfad, der die Quelldatei enthält. Der Datenintegrationsdienst muss auf den Pfad zugreifen können.
FTP verwenden	Ermöglicht FTP-Zugriff auf SAP.
FTP-Benutzer	<p>Erforderlich bei Verwendung von FTP.</p> <p>Benutzername zum Herstellen einer Verbindung zum FTP-Server.</p>
FTP-Passwort	<p>Erforderlich bei Verwendung von FTP.</p> <p>Passwort für den FTP-Benutzer.</p>
FTP-Host	<p>Erforderlich bei Verwendung von FTP.</p> <p>Hostname oder IP-Adresse des FTP-Servers.</p> <p>Optional können Sie eine Portnummer von 1 bis einschließlich 65535 angeben. Standardwert für FTP ist 21.</p> <p>Verwenden Sie eine der folgenden Syntaxen zur Angabe des Hostnamens:</p> <ul style="list-style-type: none"> - hostname:port_number - IP address:port_number <p>Wenn Sie eine Portnummer angeben, aktivieren Sie diese Portnummer für FTP auf dem Host.</p> <p>Wenn Sie SFTP aktivieren, geben Sie einen Hostnamen oder eine Portnummer für einen SFTP-Server an. Standardwert für SFTP ist 22.</p>
Wiederholungszeitraum	<p>Zeitraum in Sekunden, während dem der Datenintegrationsdienst nach Abbruch der Verbindung versucht, eine erneute Verbindung zum FTP-Host herzustellen.</p> <p>Wenn der Datenintegrationsdienst im Wiederholungszeitraum keine erneute Verbindung zum FTP-Host herstellen kann, schlägt die Zuordnung oder der Arbeitsablauf fehl.</p> <p>Standardwert ist 0. Mit einem Wert von 0 wird ein unendlicher Wiederholungszeitraum angegeben.</p>
SFTP verwenden	Ermöglicht SFTP-Zugriff auf SAP.

Eigenschaft	Beschreibung
Name der öffentlichen Schlüsseldatei	Erforderlich, wenn Sie SFTP aktivieren und der SFTP-Server Authentifizierung mit öffentlichen Schlüsseln verwendet. Pfad und Name der öffentlichen Schlüsseldatei.
Name der privaten Schlüsseldatei	Erforderlich, wenn Sie SFTP aktivieren und der SFTP-Server Authentifizierung mit öffentlichen Schlüsseln verwendet. Pfad und Name der privaten Schlüsseldatei.
Passwort für privaten Schlüsseldateinamen	Erforderlich, wenn Sie SFTP aktivieren und der SFTP-Server Authentifizierung mit öffentlichen Schlüsseln verwendet und der private Schlüssel verschlüsselt ist. Passwort zum Entschlüsseln der privaten Schlüsseldatei.
Portbereich	HTTP-Portbereich, der vom Datenintegrationsdienst verwendet werden muss, um Daten im Streaming-Modus vom SAP-Server zu lesen. Geben Sie die minimale und maximale Portnummer mit einem Bindestrich als Trennzeichen ein. Die minimale und maximale Portnummern kann zwischen 10000 und 65535 liegen. Sie können den Portbereich auch nach Maßgabe Ihres Unternehmens eingeben. Standardwert ist 10000-65535.
HTTPS verwenden	Wählen Sie diese Option, um HTTPS-Streaming beim Lesen von Daten aus SAP-Tabellen zu aktivieren. Standardmäßig ist das Kontrollkästchen HTTPS verwenden nicht aktiviert. Weitere Informationen zum Konfigurieren von HTTPS für Tabellenlesezuordnungen im Streaming-Modus finden Sie im Artikel „HTTPS Configuration for Table Reader Mappings in Streaming Mode for PowerExchange for SAP NetWeaver“ im Portal für Informatica-Dokumentationen.
Pfad der Schlüsselspeicherdatei	Erforderlich bei Verwendung von HTTPS. Pfad zur Schlüsselspeicherdatei, die die privaten oder öffentlichen Schlüsselpaare und die zugeordneten Zertifikate enthält.
Passwort des Schlüsselspeichers	Erforderlich bei Verwendung von HTTPS. Passwort für die Schlüsselspeicherdatei
Passwort des privaten Schlüssels	Erforderlich bei Verwendung von HTTPS. Passwort zum Entschlüsseln der privaten Schlüsseldatei.

Eigenschaften sequenzieller Verbindungen

Verwenden Sie eine sequenzielle Verbindung für den Zugriff auf eine sequenzielle Datenquelle. Sie erstellen eine sequenzielle Verbindung im Developer Tool. Sie können eine sequenzielle Verbindung im Administrator Tool oder im Developer Tool verwalten.

Eine sequenzielle Datenquelle ist eine Datenquelle, auf die mit PowerExchange über ein Daten-Mapping zugegriffen werden kann, die mittels einer SEQ-Zugriffsmethode definiert wurde. Der Datenintegrationsdienst stellt über PowerExchange eine Verbindung mit der Datenquelle her.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Eigenschaften von sequenziellen Verbindungen erläutert:

Option	Beschreibung
Speicherort	Knotenname für den Speicherort des PowerExchange-Listenerdiensts, der eine Verbindung zum sequenziellen Datensatz herstellt. Der Knotenname ist im ersten Parameter der NODE-Anweisung in der PowerExchange-Konfigurationsdatei „dbmover.cfg“ definiert.
Benutzername	Ein Benutzername, der für den Zugriff auf den sequenziellen Datensatz autorisiert ist.
Passwort	<p>Passwort für den angegebenen Benutzernamen oder eine gültige PowerExchange-Passphrase.</p> <p>Eine PowerExchange-Passphrase kann 9 bis 128 Zeichen lang sein und die folgenden Zeichen enthalten:</p> <ul style="list-style-type: none"> - Groß- und Kleinbuchstaben - Die Zahlen 0 bis 9 - Leerzeichen - Die folgenden Sonderzeichen: ' - ; # \ , . / ! % & * () _ + { } : @ < > ? <p>Hinweis: Das erste Zeichen ist ein Apostroph.</p> <p>Passphrasen dürfen keine einfachen Anführungszeichen ('), doppelten Anführungszeichen (") oder Währungssymbole enthalten.</p> <p>Stellen Sie vor der Verwendung von Passphrasen sicher, dass der PowerExchange-Listenerdienst im DBMOVER-Mitglied mit der Sicherheitseinstellung SECURITY=(1,N) oder höher ausgeführt wird. Weitere Informationen finden Sie unter „SECURITY-Anweisung“ im <i>PowerExchange-Referenzhandbuch</i>.</p> <p>Die zulässigen Zeichen beim Beenden von IBM IRRPHREX haben keine Auswirkungen auf die zulässigen Zeichen in PowerExchange-Passphrasen.</p> <p>Hinweis: Eine gültige RACF-Passphrase kann bis zu 100 Zeichen enthalten. PowerExchange schneidet Passphrases mit mehr als 100 Zeichen ab, wenn diese zur Validierung an RACF übergeben werden.</p>
Codepage	Erforderlich. Name der Codepage für das Lesen aus oder Schreiben in den sequenziellen Datensatz. Normalerweise ist dieser Wert ein ISO-Codepage-Name, z. B. ISO-8859-6.
Pass-Through-Sicherheit aktiviert	Aktiviert Pass-Through-Sicherheit für die Verbindung.
Verschlüsselungstyp	<p>Optional. Der Verschlüsselungstyp, den der Datenintegrationsdienst verwendet. Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> - Keine - AES <p>Standardwert ist „Keine“.</p> <p>Hinweis: Informatica empfiehlt die Verwendung von SSL-Authentifizierung (Secure Sockets Layer) statt der Konfiguration der Verbindungseigenschaften Verschlüsselungstyp und Ebene. SSL-Authentifizierung bietet striktere Sicherheit und wird von verschiedenen Informatica-Produkten verwendet.</p> <p>Weitere Informationen zum Implementieren von SSL-Authentifizierung in einem PowerExchange-Netzwerk finden Sie im <i>PowerExchange-Referenzhandbuch</i>.</p>
[Encryption]-Ebene	<p>Bei Verwendung von AES für Verschlüsselungstyp wählen Sie eine der folgenden Optionen aus, um die vom Datenintegrationsdienst verwendete Verschlüsselungsebene anzugeben:</p> <ul style="list-style-type: none"> - 1. Verwenden Sie einen 128-Bit-Verschlüsselungsschlüssel. - 2. Verwenden Sie einen 192-Bit-Verschlüsselungsschlüssel. - 3. Verwenden Sie einen 256-Bit-Verschlüsselungsschlüssel. <p>Wenn Sie als Verschlüsselungstyp nicht AES auswählen, wird diese Option ignoriert. Standard ist 1.</p>

Option	Beschreibung
Pacing-Größe	Optional. Menge der Daten, die das Quellsystem an den PowerExchange-Listenerdienst übergeben kann. Legen Sie die Pacing-Größe fest, wenn eine externe Anwendung, eine Datenbank oder der Knoten mit dem Datenintegrationsdienst einen Engpass darstellt. Verwenden Sie niedrigere Werte für schnellere Leistung. Der Mindest- und Standardwert ist 0. Der Wert 0 bietet die beste Leistung.
Als Zeilen interpretieren	Wählen Sie diese Option optional aus, um die Pacing-Größe als eine Anzahl von Zeilen auszudrücken. Löschen Sie diese Option, um die Pacing-Größe in Kilobyte anzugeben. Diese Option ist standardmäßig nicht ausgewählt und die Pacing-Größe wird in Kilobyte angegeben.
Komprimierung	Optional. Wählen Sie diese Option zum Aktivieren der Quelldatenkomprimierung aus. Durch die Komprimierung von Daten können Sie die Menge der Daten verringern, die Informatica-Anwendungen über das Netzwerk senden. Standardmäßig ist diese Option nicht ausgewählt und die Komprimierung ist deaktiviert.
Offload-Verarbeitung	Optional. Steuert, ob für die Verarbeitung von Stapeldaten vom Quellcomputer zum Datenintegrationsdienst-Computer Offload-Verarbeitung verwendet werden soll. Wählen Sie eine der folgenden Optionen aus: <ul style="list-style-type: none"> - AUTO. Der Datenintegrationsdienst bestimmt, ob Offload-Verarbeitung verwendet werden soll. - Ja. Offload-Verarbeitung wird verwendet. - Nein. Offload-Verarbeitung wird nicht verwendet. Der Standardwert ist AUTO.
Worker-Threads	Optional. Anzahl der vom Datenintegrationsdienst verwendeten Threads, um Stapeldaten bei aktivierter Offload-Verarbeitung zu verarbeiten. Um eine optimale Leistung zu erzielen, sollte dieser Wert die Anzahl der verfügbaren Prozessoren auf dem Rechner des Datenintegrationsdienstes nicht überschreiten. Gültige Werte sind 1 bis 64. Der Standardwert ist 0, der Multithreading deaktiviert.
Array-Größe	Optional: Die Anzahl der Datensätze im Speicher-Array für die Worker-Threads. Diese Option kann verwendet werden, wenn Sie die Option Worker-Threads auf einen Wert größer als 0 festlegen. Gültige Werte sind 25 bis 5000. Standardwert ist 25.
Schreibmodus	Optional. Modus, in dem der Datenintegrationsdienst Daten zum PowerExchange-Listenerdienst sendet. Wählen Sie einen der folgenden Schreibmodi aus: <ul style="list-style-type: none"> - CONFIRMWRITEON. Sendet Daten an den PowerExchange-Listenerdienst und wartet auf eine Antwort, bevor weitere Daten gesendet werden. Wählen Sie diese Option aus, wenn die Fehlerbehebung Priorität hat. Diese Option kann sich jedoch negativ auf die Leistung auswirken. - CONFIRMWRITEOFF. Sendet Daten an den PowerExchange-Listenerdienst, ohne auf eine Antwort zu warten. Verwenden Sie diese Option, wenn Sie die Zieltabelle im Fall eines Fehlers erneut laden können. - ASYNCHRONOUSWITHFAULTTOLERANCE. Sendet Daten an den PowerExchange-Listenerdienst, ohne auf eine Antwort zu warten. Diese Option aktiviert außerdem die Fehlererkennung. Diese Option kombiniert die Geschwindigkeit von CONFIRMWRITEOFF und die Datenintegrität von CONFIRMWRITEON. Der Standardwert ist CONFIRMWRITEON.

Snowflake-Verbindungseigenschaften

Wenn Sie eine Snowflake-Verbindung einrichten, müssen Sie die Verbindungseigenschaften konfigurieren.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Snowflake-Verbindungseigenschaften beschrieben:

Eigenschaft	Beschreibung
Name	Der Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung ändern. Der Name darf maximal 128 Zeichen umfassen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * () - + = { [] \ : ; " ' < , > . ? /
ID	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Die ID darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Optional. Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 4.000 Zeichen enthalten.
Speicherort	Die Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Der Verbindungstyp. Wählen Sie Snowflake aus.
Snowflake-Authentifizierungstyp	Geben Sie an, ob eine Verbindung zu Snowflake mit der Standardauthentifizierung oder der Schlüsselpaar-Authentifizierung hergestellt werden soll. Bei der Standardauthentifizierung werden der Benutzername und das Kennwort des Snowflake-Kontos verwendet. Bei der Schlüsselpaar-Authentifizierung werden die Datei mit dem privaten Schlüssel und das Passwort für die Datei mit dem privaten Schlüssel zusammen mit dem Benutzernamen Ihres Snowflake-Kontos verwendet.
Benutzername	Der Benutzername zum Herstellen einer Verbindung zum Snowflake-Konto.
Passwort	Erforderlich für Standardauthentifizierung. Das Passwort zum Herstellen einer Verbindung zum Snowflake-Konto.
Konto	Der Name des Snowflake-Kontos.
Privater Schlüssel	Erforderlich für die Schlüsselpaar-Authentifizierung. Vollständig qualifizierter Pfad zur Datei mit dem privaten Schlüssel, den der Datenintegrationsdienst für den Zugriff auf Snowflake verwendet.
Passwort des privaten Schlüssels	Erforderlich für die Schlüsselpaar-Authentifizierung. Passwort für die Datei des privaten Schlüssels.
Warehouse	Der Name des Snowflake-Warehouses.

Eigenschaft	Beschreibung
Rolle	Die dem Benutzer zugewiesene Snowflake-Rolle.
Zusätzliche JDBC-URL-Parameter	<p>Geben Sie einen oder mehrere JDBC-Verbindungsparameter in folgendem Format ein:</p> <pre><param1>=<value>&<param2>=<value>&<param3>=<value>...</pre> <p>Beispiel:</p> <pre>user=jon&warehouse=mywh&db=mydb&schema=public</pre> <p>Um über die Okta SSO-Authentifizierung auf Snowflake zuzugreifen, geben Sie das webbasierte IdP-implementierende SAML 2.0-Protokoll in folgendem Format ein:</p> <pre>authenticator=https://<Your_Okta_Account_Name>.okta.com</pre> <p>Hinweis: Microsoft ADFS wird nicht unterstützt.</p> <p>Weitere Informationen über das Konfigurieren der Okta-Authentifizierung finden Sie auf der folgenden Website:</p> <p>https://docs.snowflake.net/manuals/user-guide/admin-security-fed-auth-configure-snowflake.html#configuring-snowflake-to-use-federated-authentication</p>

Verbindungseigenschaften des parallelen Teradata-Transporters

Verwenden Sie eine Teradata-PT-Verbindung, um auf Teradata-Tabellen zuzugreifen. Die Teradata-PT-Verbindung ist ein Datenbank-Verbindungstyp. Sie können eine Teradata-PT-Verbindung im Administrator Tool oder im Developer Tool erstellen und verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Eigenschaften von Teradata-PT-Verbindungen erläutert:

Eigenschaft	Beschreibung
Name	<p>Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten:</p> <pre>~ ` ! \$ % ^ & * () - + = { [] \ : ; " ' < , > . ? /</pre>
ID	<p>Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.</p>
Beschreibung	Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Die Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Verbindungstyp. Wählen Sie „Teradata PT“.

Eigenschaft	Beschreibung
Benutzername	Benutzername der Teradata-Datenbank mit der entsprechenden Lese- und Schreibberechtigung für den Zugriff auf die Datenbank.
Passwort	Passwort für den Benutzernamen der Teradata-Datenbank.
Treibername	Name des Teradata-JDBC-Treibers.
Verbindungszeichenfolge	Verbindungszeichenfolge für den Zugriff auf Metadaten in der Datenbank. Verwenden Sie die folgende Verbindungszeichenfolge: <code>jdbc:teradata://<hostname>/database=<database name>, tmode=ANSI, charset=UTF8</code>

Die folgende Tabelle beschreibt die Eigenschaften für den Datenzugriff:

Eigenschaft	Beschreibung
TDPID	Name oder IP-Adresse des Teradata-Datenbankcomputers.
Datenbankname	Teradata-Datenbankname. Wenn Sie keinen Datenbanknamen eingeben, verwendet die Teradata-PT-API den Standardanmeldungsnamen der Datenbank.
Daten-Codepage	Codepage, die mit der Datenbank verbunden ist. Beim Ausführen einer Zuordnung, die Daten auf ein Teradata-Ziel schreibt, muss die Codepage der Teradata-PT-Verbindung mit der Codepage des Teradata-Ziels übereinstimmen. Standardwert ist UTF-8.
Beharrlichkeit	Anzahl der Stunden, in denen die Teradata-PT-API weiterhin versucht, sich anzumelden, wenn die maximale Anzahl von Operationen in der Teradata-Datenbank ausgeführt wird. Muss ein positiver, ganzzahliger Wert sein, der nicht Null ist. Standardwert ist 4.
Maximalanzahl Sitzungen	Maximale Anzahl der Sitzungen, die die Teradata-PT-API mit der Teradata-Datenbank herstellt. Muss ein positiver, ganzzahliger Wert sein, der nicht Null ist. Standardwert ist 4.
Min. Sitzungen	Mindestanzahl von Teradata-PT-API-Sitzungen, die erforderlich ist, damit der Teradata-PT-API-Job fortfährt. Muss ein positiver, ganzzahliger Wert zwischen 1 und dem Wert für Maximalanzahl Sitzungen sein. Standardwert ist 1.
Ruhezustand	Anzahl der Minuten, in denen die Teradata-PT-API anhält, bevor sie wieder versucht, sich anzumelden, wenn die maximale Anzahl von Operationen in der Teradata-Datenbank ausgeführt wird. Muss ein positiver, ganzzahliger Wert sein, der nicht Null ist. Standardwert ist 6.
Metadaten-JDBC-URL für TDCH verwenden	Gibt an, dass der Teradata-Connector für Hadoop (TDCH) die JDBC-URL verwenden muss, die im Verbindungsstring unter den Metadaten-Zugriffseigenschaften angegeben ist. Standardwert ist Ausgewählt. Löschen Sie diese Option, um eine andere JDBC-URL einzugeben, die TDCH beim Ausführen des Mappings verwenden muss.

Eigenschaft	Beschreibung
TDCH-JDBC-URL	<p>Geben Sie die JDBC-URL ein, die TDCH beim Ausführen eines Teradata-Mappings verwenden muss. Verwenden Sie das folgende Format:</p> <pre>jdbc:teradata://<hostname>/database=<database name>, tmode=ANSI, charset=UTF8</pre> <p>Dieses Feld ist nur verfügbar, wenn Sie die Option Metadaten-JDBC-URL für TDCH verwenden deaktivieren.</p>
Datenverschlüsselung	<p>Aktiviert vollständige Sicherheitsverschlüsselung von SQL-Abfragen, Antworten und Daten unter Windows.</p> <p>Standardwert ist „Deaktiviert“.</p>
Zusätzliche Sqoop-Argumente	<p>Diese Eigenschaft ist anwendbar, wenn Sie einen Hortonworks- oder Cloudera-Cluster verwenden und auf der Blaze- oder Spark-Engine über Sqoop eine Teradata-Zuordnung ausführen.</p> <p>Geben Sie die Argumente ein, die von Sqoop zum Verarbeiten der Daten verwendet werden müssen. Geben Sie beispielsweise <code>--method split.by.amp</code> ein. Trennen Sie mehrere Argumente durch ein Leerzeichen.</p> <p>Eine Liste der Argumente, die Sie angeben können, finden Sie in der Dokumentation zu Hortonworks for Teradata Connector und Cloudera Connector Powered by Teradata.</p> <p>Hinweis: Wenn Sie Hortonworks for Teradata Connector verwenden, ist das Argument „<code>--split-by</code>“ erforderlich, wenn Sie im Lesevorgang zwei oder mehr Quelltabellen hinzufügen. Wenn Sie Cloudera Connector Powered by Teradata verwenden, ist das Argument „<code>--split-by</code>“ in der Quellverbindung erforderlich, wenn für die Quelltable kein Primärschlüssel definiert ist.</p>
Authentifizierungstyp	<p>Methode zur Authentifizierung des Benutzers.</p> <p>Wählen Sie einen der folgenden Authentifizierungstypen aus:</p> <ul style="list-style-type: none"> - Nativ. Authentifiziert den Benutzernamen und das Kennwort für die in der Verbindung angegebene Teradata-Datenbank. - LDAP. Authentifiziert Benutzeranmeldeinformationen für den externen LDAP-Verzeichnisdienst. <p>Standardwert ist „Nativ“.</p>

Tableau-Verbindungseigenschaften

Verwenden Sie eine Tableau-Verbindung, um eine Verbindung mit Tableau herzustellen. Wenn Sie eine Tableau-Verbindung erstellen, geben Sie Informationen für den Zugriff auf Tableau ein.

In der folgenden Tabelle werden die Tableau-Verbindungseigenschaften beschrieben:

Eigenschaft	Beschreibung
Name	Name der Tableau-Verbindung.
ID	<p>Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.</p>

Eigenschaft	Beschreibung
Beschreibung	Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Die Informatica-Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Typ der Verbindung. Wählen Sie „Tableau“.

In der folgenden Tabelle werden die Eigenschaften zum Herstellen einer Verbindung mit Tableau beschrieben:

Verbindungseigenschaft	Beschreibung
Tableau-Produkt	Der Name des Tableau-Produkts, zu dem Sie eine Verbindung herstellen möchten. Zum Veröffentlichen der TDE- oder TWBX-Datei können Sie eines der folgenden Tableau-Produkte auswählen: <ul style="list-style-type: none"> - Tableau Desktop. Erstellt eine TDE-Datei auf dem Computer des Datenintegrationsdiensts. Sie können dann die TDE-Datei manuell in Tableau Desktop importieren. - Tableau Server. Veröffentlicht die generierte TDE- oder TWBX-Datei auf Tableau Server. - Tableau Online. Veröffentlicht die generierte TDE- oder TWBX-Datei auf Tableau Online.
URL der Verbindung	URL von Tableau Server oder Tableau Online, unter der Sie die TDE- oder TWBX-Datei veröffentlichen möchten. Die URL hat folgendes Format: <code>http://<Hostname von Tableau Server oder Tableau Online>:<port></code>
Benutzername	Benutzername des Tableau Server- oder Tableau Online-Kontos.
Passwort	Passwort für das Tableau Server- oder Tableau Online-Konto.
Inhalts-URL	Der Name der Website auf Tableau Server oder Tableau Online, auf der Sie die TDE- oder TWBX-Datei veröffentlichen möchten. Wenden Sie sich an den Tableau-Administrator, um den Namen der Website bereitzustellen.

Tableau V3-Verbindungseigenschaften

Wenn Sie eine Tableau V3-Verbindung einrichten, müssen Sie die Verbindungseigenschaften konfigurieren.

In der folgenden Tabelle werden die Tableau V3-Verbindungseigenschaften beschrieben:

Eigenschaft	Beschreibung
Name	Name der Tableau V3-Verbindung.
ID	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.

Eigenschaft	Beschreibung
Beschreibung	Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Die Informatica-Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Typ der Verbindung. Wählen Sie Tableau V3 aus.

In der folgenden Tabelle werden die Eigenschaften zum Herstellen einer Verbindung mit Tableau beschrieben:

Verbindungseigenschaft	Beschreibung
Tableau-Produkt	<p>Der Name des Tableau-Produkts, zu dem Sie eine Verbindung herstellen möchten. Sie können eines der folgenden Tableau-Produkte auswählen, um die .hyper- oder TWBX-Datei zu veröffentlichen:</p> <p>Tableau Desktop</p> <p>Erstellen Sie eine .hyper-Datei auf dem Datenintegrationsdienst-Computer. Anschließend können Sie die .hyper-Datei manuell in den Tableau Desktop importieren.</p> <p>Tableau Server</p> <p>Veröffentlicht die generierte .hyper- oder TWBX-Datei auf dem Tableau Server.</p> <p>Tableau Online</p> <p>Veröffentlicht die generierte .hyper- oder TWBX-Datei auf Tableau Online.</p>
URL der Verbindung	<p>Die URL für Tableau Server bzw. Tableau Online, wo die .hyper- oder TWBX-Datei veröffentlicht werden soll.</p> <p>Geben Sie die URL in folgendem Format ein: <code>http://<Hostname von Tableau Server oder Tableau Online>:<port></code></p>
Benutzername	Der Benutzername des Tableau Server- oder Tableau Online-Kontos.
Passwort	Das Passwort des Kontos für Tableau Server bzw. Tableau Online.
Site-ID	<p>Die ID der Site auf Tableau Server bzw. Tableau Online, wo Sie die TWBX-Datei veröffentlichen möchten.</p> <p>Hinweis: Setzen Sie sich mit dem Tableau-Administrator in Verbindung, um die Site-ID zu erhalten.</p>
Dateipfad für Schema	<p>Der Pfad zu einer .hyper-Beispieldatei, von wo aus der Datenintegrationsdienst die Tableau-Metadaten importiert.</p> <p>Geben Sie eine der folgenden Optionen für den Schemadateipfad ein:</p> <ul style="list-style-type: none"> - Absoluter Pfad zur .hyper-Datei. - Verzeichnispfad für die .hyper-Dateien. - Leerer Verzeichnispfad. <p>Der Pfad, den Sie für die Schemadatei angeben, wird zum Standardpfad für die .hyper-Zieldatei. Wenn Sie keinen Dateipfad angeben, verwendet der Datenintegrationsdienst für die .hyper-Zieldatei den folgenden Standard-Dateipfad:</p> <p><code><Installationsverzeichnis für den Datenintegrationsdienst>/apps/Data_Integration_Server/<Neueste Version>/bin/rtdm</code></p>

Streaming-Verbindungseigenschaften für Twitter

Verwenden Sie eine Twitter-Streaming-Verbindung, um auf Nahezu-Echtzeitdaten von der Twitter-Website zuzugreifen. Die Twitter-Streaming-Verbindung ist eine Verbindung zu der Streaming-API des sozialen Medienunternehmens. Sie können eine Twitter-Streaming-Verbindung im Administrator-Tool oder im Developer-Tool erstellen und verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

Die folgende Tabelle beschreibt die Eigenschaften für eine Twitter-Streaming-Verbindung:

Eigenschaft	Beschreibung
Name	Name der Verbindung. Der Name unterliegt nicht der Groß-/Kleinschreibung und muss innerhalb der Domäne eindeutig sein. Der Name darf nicht mehr als 128 Zeichen und weder Leerzeichen noch die folgenden Sonderzeichen enthalten: ~ ` ! \$ % ^ & * () - + = { [] \ : ; " ' < , > . ? /
ID	Zeichenfolge, die der Datenintegrationsdienst zum Erkennen der Verbindung verwendet. Bei der ID wird die Groß- und Kleinschreibung nicht beachtet. Sie darf maximal 255 Zeichen umfassen und muss in der Domäne eindeutig sein. Sie können diese Eigenschaft nach dem Erstellen der Verbindung nicht mehr ändern. Als Standardwert dient der Verbindungsname.
Beschreibung	Die Beschreibung der Verbindung. Die Beschreibung darf nicht mehr als 765 Zeichen enthalten.
Speicherort	Die Domäne, in der Sie die Verbindung erstellen möchten.
Typ	Der Verbindungstyp. Wählen Sie Twitter-Streaming aus.

Die folgende Tabelle beschreibt die Eigenschaften für den Hose-Typ und die offene Authentifizierung (OAuth):

Eigenschaft	Beschreibung
Hose-Typ	Streaming-API-Methoden. Sie können eine der folgenden Methoden angeben: <ul style="list-style-type: none">- Filter. Die Twitter <code>statuses/filter</code>-Methode gibt öffentliche Statusangaben zurück, die mit den Suchkriterien übereinstimmen.- Beispiel. Die Twitter <code>statuses/sample</code>-Methode gibt eine zufällige Stichprobe aus allen öffentlichen Statusangaben zurück.
Verbraucherschlüssel	Der Verbraucherschlüssel, den Sie beim Erstellen der Anwendung in Twitter erhalten. Twitter verwendet die Schlüssel zur Identifizierung der Anwendung.
Verbrauchergeheimwort	Das Verbrauchergeheimwort, das Sie beim Erstellen einer Twitter-Anwendung erhalten. Twitter verwendet das Geheimwort für das Eigentum am Verbraucherschlüssel.
Haben Sie OAuth-Details?	Zeigt an, ob Sie OAuth konfigurieren möchten. Wählen Sie einen der folgenden Werte aus: <ul style="list-style-type: none">- Ja. Zeigt an, dass Sie über den Zugriffstoken und das Geheimwort verfügen.- Nein. Startet das OAuth-Dienstprogramm.
Zugriffstoken	Zugriffstoken, den das OAuth-Dienstprogramm zurückgibt. Twitter verwendet diesen Token anstelle der Benutzeranmeldedaten für den Zugriff auf geschützte Ressourcen.
Zugriffsgeheimwort	Zugriffsgeheimwort, das das OAuth-Dienstprogramm zurückgibt. Das Geheimwort legt das Eigentum eines Token fest.

VSAM-Verbindungseigenschaften

Verwenden Sie eine VSAM-Verbindung für den Zugriff auf VSAM-Datentabellen. Die VSAM-Verbindung ist ein Einfachdatei-Verbindungstyp. Sie erstellen eine VSAM-Verbindung im Developer-Tool. Sie können eine VSAM-Verbindung im Administrator-Tool oder im Developer-Tool verwalten.

Hinweis: Die Reihenfolge der Verbindungseigenschaften kann je nach Tool, in dem Sie diese anzeigen, variieren.

In der folgenden Tabelle werden die Eigenschaften von VSAM-Verbindungen erläutert:

Option	Beschreibung
Speicherort	Knotenname für den Speicherort des PowerExchange-Listenerdiensts, der eine Verbindung zum VSAM-Dataset herstellt. Der Knotenname ist im ersten Parameter der NODE-Anweisung in der PowerExchange-Konfigurationsdatei „dbmover.cfg“ definiert.
Benutzername	Ein Benutzername, der zum Herstellen einer Verbindung zum VSAM-Dataset autorisiert ist.
Passwort	<p>Passwort für den angegebenen Benutzer oder eine gültige PowerExchange-Passphrase. Eine PowerExchange-Passphrase kann 9 bis 128 Zeichen lang sein und die folgenden Zeichen enthalten:</p> <ul style="list-style-type: none">- Groß- und Kleinbuchstaben- Die Zahlen 0 bis 9- Leerzeichen- Die folgenden Sonderzeichen: ' - ; # \ , . / ! % & * () _ + { } : @ < > ? <p>Hinweis: Das erste Zeichen ist ein Apostroph.</p> <p>Passphrasen dürfen keine einfachen Anführungszeichen ('), doppelten Anführungszeichen (") oder Währungssymbole enthalten.</p> <p>Stellen Sie vor der Verwendung von Passphrasen sicher, dass der PowerExchange-Listenerdienst im DBMOVER-Mitglied mit der Sicherheitseinstellung SECURITY=(1,N) oder höher ausgeführt wird. Weitere Informationen finden Sie unter „SECURITY-Anweisung“ im <i>PowerExchange-Referenzhandbuch</i>.</p> <p>Die zulässigen Zeichen beim Beenden von IBM IRRPHREX haben keine Auswirkungen auf die zulässigen Zeichen in PowerExchange-Passphrasen.</p> <p>Hinweis: Eine gültige RACF-Passphrase kann bis zu 100 Zeichen enthalten. PowerExchange schneidet Passphrases mit mehr als 100 Zeichen ab, wenn diese zur Validierung an RACF übergeben werden.</p>
Codepage	Erforderlich. Name der Codepage für das Lesen aus oder Schreiben in das VSAM-Dataset. Normalerweise ist dieser Wert ein ISO-Codepage-Name, z. B. ISO-8859-6.
Pass-Through-Sicherheit aktiviert	Aktiviert Pass-Through-Sicherheit für die Verbindung.

Option	Beschreibung
Verschlüsselungstyp	<p>Optional. Der Verschlüsselungstyp, den der Datenintegrationsdienst verwendet. Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> - Keine - AES <p>Standardwert ist „Keine“.</p> <p>Hinweis: Informatica empfiehlt die Verwendung von SSL-Authentifizierung (Secure Sockets Layer) statt der Konfiguration der Verbindungseigenschaften Verschlüsselungstyp und Ebene. SSL-Authentifizierung bietet striktere Sicherheit und wird von verschiedenen Informatica-Produkten verwendet.</p> <p>Weitere Informationen zum Implementieren von SSL-Authentifizierung in einem PowerExchange-Netzwerk finden Sie im <i>PowerExchange-Referenzhandbuch</i>.</p>
[Encryption]-Ebene	<p>Bei Verwendung von AES für Verschlüsselungstyp wählen Sie eine der folgenden Optionen aus, um die vom Datenintegrationsdienst verwendete Verschlüsselungsebene anzugeben:</p> <ul style="list-style-type: none"> - 1. Verwenden Sie einen 128-Bit-Verschlüsselungsschlüssel. - 2. Verwenden Sie einen 192-Bit-Verschlüsselungsschlüssel. - 3. Verwenden Sie einen 256-Bit-Verschlüsselungsschlüssel. <p>Wenn Sie als Verschlüsselungstyp nicht AES auswählen, wird diese Option ignoriert. Standard ist 1.</p>
Pacing-Größe	<p>Optional. Menge der Daten, die das Quellsystem an den PowerExchange-Listenerdienst übergeben kann. Legen Sie die Pacing-Größe fest, wenn eine externe Anwendung, eine Datenbank oder der Knoten mit dem Datenintegrationsdienst einen Engpass darstellt. Verwenden Sie niedrigere Werte für schnellere Leistung.</p> <p>Der Mindest- und Standardwert ist 0. Der Wert 0 bietet die beste Leistung.</p>
Als Zeilen interpretieren	<p>Optional. Wählen Sie diese Option, um die Pacing-Größe als Anzahl von Zeilen anzugeben. Löschen Sie diese Option, um die Pacing-Größe in Kilobyte anzugeben. Diese Option ist standardmäßig nicht ausgewählt und die Pacing-Größe wird in Kilobyte angegeben.</p>
Komprimierung	<p>Optional. Wählen Sie diese Option zum Aktivieren der Quelldatenkomprimierung aus. Durch die Komprimierung von Daten können Sie die Menge der Daten verringern, die Informatica-Anwendungen über das Netzwerk senden. Standardmäßig ist diese Option nicht ausgewählt und die Komprimierung ist deaktiviert.</p>
Offload-Verarbeitung	<p>Optional. Steuert, ob für die Verarbeitung von Stapeldaten vom Quellcomputer zum Datenintegrationsdienst-Computer Offload-Verarbeitung verwendet werden soll. Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> - AUTO. Der Datenintegrationsdienst bestimmt, ob Offload-Verarbeitung verwendet werden soll. - Ja. Offload-Verarbeitung wird verwendet. - Nein. Offload-Verarbeitung wird nicht verwendet. <p>Der Standardwert ist AUTO.</p>
Worker-Threads	<p>Optional. Anzahl der vom Datenintegrationsdienst verwendeten Threads, um Stapeldaten bei aktivierter Offload-Verarbeitung zu verarbeiten. Um eine optimale Leistung zu erzielen, sollte dieser Wert die Anzahl der verfügbaren Prozessoren auf dem Rechner des Datenintegrationsdienstes nicht überschreiten. Gültige Werte sind 1 bis 64. Der Standardwert ist 0, der Multithreading deaktiviert.</p>

Option	Beschreibung
Array-Größe	Optional. Die Anzahl der Datensätze im Speicher-Array für die Worker-Threads. Diese Option kann verwendet werden, wenn Sie die Option Worker-Threads auf einen Wert größer als 0 festlegen. Gültige Werte sind 25 bis 5000. Standardwert ist 25.
Schreibmodus	<p>Optional. Modus, in dem der Datenintegrationsdienst Daten an den PowerExchange-Listenerdienst sendet. Wählen Sie einen der folgenden Schreibmodi aus:</p> <ul style="list-style-type: none"> - CONFIRMWRITEON. Sendet Daten an den PowerExchange-Listenerdienst und wartet auf eine Antwort, bevor weitere Daten gesendet werden. Wählen Sie diese Option aus, wenn die Fehlerbehebung Priorität hat. Diese Option kann sich jedoch negativ auf die Leistung auswirken. - CONFIRMWRITEOFF. Sendet Daten an den PowerExchange-Listenerdienst, ohne auf eine Antwort zu warten. Verwenden Sie diese Option, wenn Sie die Zieltabelle im Fall eines Fehlers erneut laden können. - ASYNCHRONOUSWITHFAULTTOLERANCE. Sendet Daten an den PowerExchange-Listenerdienst, ohne auf eine Antwort zu warten. Diese Option aktiviert außerdem die Fehlererkennung. Diese Option kombiniert die Geschwindigkeit von CONFIRMWRITEOFF und die Datenintegrität von CONFIRMWRITEON. <p>Der Standardwert ist CONFIRMWRITEON.</p>

Verbindungseigenschaften von Webdiensten

Verwenden Sie eine Web-Dienst-Verbindung, um eine Web-Dienst-Verbraucher-Umwandlung mit einem Web-Dienst zu verbinden.

Die folgende Tabelle beschreibt die konfigurierbaren Eigenschaften von Web-Diensten:

Eigenschaft	Beschreibung
Benutzername	<p>Benutzername, der mit dem Web-Dienst verbunden werden soll. Geben Sie einen Benutzernamen ein, wenn Sie die HTTP-Authentifizierung oder die WS-Security aktiviert haben.</p> <p>Wenn die Web-Dienst-Verbraucher-Umwandlung WS-Security-Ports enthält, erhält die Umwandlung einen dynamischen Benutzernamen durch einen Eingangsport. Der Datenintegrationsdienst überschreibt den Benutzernamen, der in der Verbindung definiert ist.</p>
Passwort	<p>Passwort für den Benutzernamen. Geben Sie ein Passwort ein, wenn Sie die HTTP-Authentifizierung oder die WS-Security aktiviert haben.</p> <p>Wenn die Web-Dienst-Verbraucher-Umwandlung WS-Security-Ports enthält, erhält die Umwandlung ein dynamisches Passwort durch einen Eingangsport. Der Datenintegrationsdienst überschreibt das Passwort, das in der Verbindung definiert ist.</p>
Endpunkt-URL	<p>URL für den Web-Dienst, auf den zugegriffen werden soll. Der Datenintegrationsdienst überschreibt die URL, die in der WSDL-Datei definiert ist.</p> <p>Wenn die Web-Dienst-Verbraucher-Umwandlung einen Endpunkt-URL-Port enthält, erhält die Umwandlung die URL durch einen Eingangsport. Der Datenintegrationsdienst überschreibt die URL, die in der Verbindung definiert ist.</p>
Timeout	Dauer in Sekunden, die der Datenintegrationsdienst auf eine Antwort vom Webdienst-Provider wartet, ehe die Verbindung geschlossen wird. Geben Sie einen Timeout-Wert zwischen 1 und 10.000 Sekunden an.

Eigenschaft	Beschreibung
HTTP-Authentifizierungstyp	<p>Art der Benutzer-Authentifizierung via HTTP. Wählen Sie einen der folgenden Werte aus:</p> <ul style="list-style-type: none"> - Keine. Keine Authentifizierung. - Automatisch. Der Datenintegrationsdienst wählt den Authentifizierungstyp, den der Webdienst-Provider verwendet. - Basis Sie müssen der Domäne des Webdienst-Providers einen Benutzernamen und ein Passwort bereitstellen. Der Datenintegrationsdienst sendet den Benutzernamen und das Passwort zur Authentifizierung an den Webdienst-Provider. - zusammengefasst Sie müssen der Domäne des Webdienst-Providers einen Benutzernamen und ein Passwort bereitstellen. Der Datenintegrationsdienst generiert eine verschlüsselte Meldungszusammenfassung aus dem Benutzernamen und dem Passwort und sendet diese an den Webdienst-Provider. Der Provider generiert einen temporären Wert für den Benutzernamen und das Passwort und speichert diesen in seinem Active Directory auf dem Domänen-Controller. Er vergleicht den Wert mit der Meldungszusammenfassung. Wenn beide übereinstimmen, authentifiziert Sie der Webdienst-Provider. - NTLM Sie müssen einen Domänennamen, einen Servernamen oder einen Standardbenutzernamen und ein Passwort bereitstellen. Der Webdienst-Provider authentifiziert Sie anhand der Domäne, mit der Sie verbunden sind. Er erhält den Benutzernamen und das Passwort vom Windows Domain Controller und vergleicht sie mit dem Benutzernamen und Passwort, das Sie bereitgestellt haben. Wenn beide übereinstimmen, authentifiziert Sie der Webdienst-Provider. Bei der NTLM-Authentifizierung werden keine verschlüsselten Passwörter im Active Directory des Domain Controllers gespeichert.
WS-Security-Typ	<p>Art der WS-Security, die Sie verwenden möchten. Wählen Sie einen der folgenden Werte aus:</p> <ul style="list-style-type: none"> - Keine. Der Datenintegrationsdienst fügt keinen Web-Dienst Sicherheits-Header an die generierte SOAP-Anfrage an. - PasswordText. Der Datenintegrationsdienst fügt einen Web-Dienst Sicherheits-Header an die generierte SOAP-Anfrage an. Das Passwort wird in reinem Textformat gespeichert. - PasswordDigest. Der Datenintegrationsdienst fügt einen Web-Dienst Sicherheits-Header an die generierte SOAP-Anfrage an. Das Passwort wird in zusammengefasster Form gespeichert, was einen effektiven Schutz gegen Antwortangriffe auf das Netzwerk bietet. Der Datenintegrationsdienst kombiniert das Passwort mit einem Einmalschlüssel und einem Zeitstempel. Der Datenintegrationsdienst weist dem Passwort einen SHA-Hashwert zu, codiert es in base64-Codierung und verwendet das verschlüsselte Passwort im SOAP-Header.
Trust-Zertifikatsdatei	<p>Die Datei enthält ein Bundle aus vertrauenswürdigen Zertifikaten, die der Datenintegrationsdienst verwendet, wenn er das SSL-Zertifikat des Web-Dienstes authentifiziert. Geben Sie den Dateinamen und den kompletten Verzeichnispfad ein.</p> <p>Voreinstellung ist <Informatica-Installationsverzeichnis>/services/shared/bin/ca-bundle.crt.</p>
Dateiname des Clientzertifikats	<p>Clientzertifikat, das der Web-Dienst verwendet, um einen Client zu authentifizieren. Geben Sie die Clientzertifikatsdatei an, wenn der Web-Dienst den Datenintegrationsdienst authentifizieren muss.</p>
Passwort des Clientzertifikats	<p>Passwort des Clientzertifikats Geben Sie das Passwort des Clientzertifikats an, wenn der Web-Dienst den Datenintegrationsdienst authentifizieren muss.</p>
Clientzertifikat - Typ	<p>Format der Clientzertifikatsdatei. Wählen Sie einen der folgenden Werte aus:</p> <ul style="list-style-type: none"> - PEM. Dateien mit der Dateiendung .pem. - DER. Dateien mit der Dateiendung .cer oder .der <p>Geben Sie den Clientzertifikatstyp an, wenn der Webdienst den Datenintegrationsdienst authentifizieren muss.</p>

Eigenschaft	Beschreibung
Dateiname des privaten Schlüssels	Der private Schlüssel für das Clientzertifikat. Geben Sie den Dateinamen des privaten Schlüssels an, wenn der Web-Dienst den Datenintegrationsdienst authentifizieren muss.
Passwort des privaten Schlüssels	Passwort für den privaten Schlüssel des Clientzertifikats. Geben Sie das Passwort des privaten Schlüssels an, wenn der Web-Dienst den Datenintegrationsdienst authentifizieren muss.
Privater Schlüssel - Typ	Typ des privaten Schlüssels. Der unterstützte Typ ist PEM.

Bezeichnereigenschaften in Datenbankverbindungen

Bei der Erstellung der meisten relationalen Datenbankverbindungen müssen Sie die Eigenschaften der Datenbankbezeichner konfigurieren. Die Bezeichnereigenschaften legen fest, ob der Datenintegrationsdienst die Bezeichner mit Trennzeichen umschließt, wenn der Dienst SQL-Abfragen für den Zugriff auf die Datenbank generiert.

Ein Datenbankbezeichner ist ein Datenbankobjektname. Tabellen, Ansichten, Spalten, Indizes, Auslöser, Verfahren, Einschränkungen und Regeln können Bezeichner aufweisen. Verwenden Sie den Bezeichner, um auf das Objekt in SQL-Abfragen zu verweisen. Eine Datenbank kann reguläre Bezeichner oder begrenzte Bezeichner, die innerhalb von Trennzeichen stehen müssen, verwenden.

Reguläre Bezeichner

Reguläre Bezeichner erfüllen die Formatregeln für Bezeichner. Für reguläre Bezeichner sind keine Trennzeichen erforderlich, wenn sie in SQL-Abfragen verwendet werden.

Beispiel: Die folgende SQL-Anweisung verwendet die regulären Bezeichner *MYTABLE* und *MYCOLUMN*:

```
SELECT * FROM MYTABLE
WHERE MYCOLUMN = 10
```

Begrenzte Bezeichner

Begrenzte Bezeichner müssen zwischen Trennzeichen stehen, da sie nicht mit den Formatregeln für Bezeichner übereinstimmen.

Datenbanken können die folgenden Typen von begrenzten Bezeichnern verwenden:

Bezeichner, die reservierte Schlüsselwörter verwenden

Wenn ein Bezeichner ein reserviertes Schlüsselwort verwendet, muss der Bezeichner in einer SQL-Abfrage zwischen Trennzeichen stehen. Beispiel: Die folgende SQL-Anweisung greift auf eine Tabelle mit dem Namen *ORDER* zu:

```
SELECT * FROM "ORDER"
WHERE MYCOLUMN = 10
```

Bezeichner, die Sonderzeichen verwenden

Wenn ein Bezeichner Sonderzeichen verwendet, muss der Bezeichner in einer SQL-Abfrage zwischen Trennzeichen stehen. Beispiel: Die folgende SQL-Anweisung greift auf eine Tabelle mit dem Namen *MYTABLE\$@* zu:

```
SELECT * FROM "MYTABLE$@"
WHERE MYCOLUMN = 10
```

Bezeichner in Groß- und Kleinschreibung

Standardmäßig wird bei Bezeichnern in IBM DB2-, Microsoft SQL Server- und Oracle-Datenbanken nicht zwischen Groß- und Kleinschreibung unterschieden. Datenbankobjektnamen werden in Großbuchstaben gespeichert, jedoch kann in SQL-Anfragen, die sich darauf beziehen, Groß- und Kleinschreibung beliebig verwendet werden. Beispiel: Die folgenden SQL-Anweisungen greifen auf die Tabelle mit dem Namen *MYTABLE* zu:

```
SELECT * FROM mytable
SELECT * FROM MyTable
SELECT * FROM MYTABLE
```

Um Bezeichner zu verwenden, die Groß- und Kleinschreibung unterscheiden, muss der Bezeichner in einer SQL-Abfrage zwischen Trennzeichen stehen. Beispiel: Die folgende SQL-Anweisung greift auf eine Tabelle mit dem Namen *MyTable* zu:

```
SELECT * FROM "MyTable"
WHERE MYCOLUMN = 10
```

Bezeichnereigenschaften

Bei der Erstellung der meisten Datenbankverbindungen müssen Sie die Eigenschaften der Datenbankbezeichner konfigurieren. Die zu konfigurierenden Bezeichnereigenschaften variieren, je nachdem, ob die Datenbank reguläre Bezeichner, Bezeichner mit Schlüsselwörtern bzw. Sonderzeichen oder Bezeichner mit Unterscheidung zwischen Groß- und Kleinschreibung verwendet.

Konfigurieren Sie in einer Datenbankverbindung die folgenden Bezeichnereigenschaften:

SQL-Kennungszeichen

Art des Zeichens, das von der Datenbank verwendet wird, um Delimiter-IDs in SQL-Abfragen einzuschließen. Die verfügbaren Zeichen richten sich nach dem Datenbanktyp.

Wählen Sie (Keine) aus, wenn die Datenbank reguläre IDs verwendet. Wenn der Datenintegrationsdienst SQL-Abfragen erzeugt, schließt der Dienst IDs nicht in Delimiter-Zeichen ein.

Wählen Sie ein Zeichen aus, wenn die Datenbank Delimiter-IDs verwendet. Wenn der Datenintegrationsdienst SQL-Abfragen erzeugt, schließt der Dienst Delimiter-IDs in dieses Zeichen ein.

Unterstützte IDs für gemischte Groß-/Kleinschreibung

Aktivieren Sie diese Eigenschaft, wenn die Datenbank IDs für gemischte Groß-/Kleinschreibung verwendet. Bei aktivierter Eigenschaft schließt der Datenintegrationsdienst alle IDs innerhalb des Zeichens ein, das für die Eigenschaft **SQL-Kennungszeichen** ausgewählt wurde.

In den Informatica-Client-Tools müssen Sie mit der korrekten Groß-/Kleinschreibung auf diese IDs verweisen. Wenn Sie beispielsweise die Datenbankverbindung erstellen, müssen Sie den Namen des Datenbankbenutzers mit korrekter Groß-/Kleinschreibung eingeben.

Wenn die Eigenschaft **SQL-Kennungszeichen** auf „Kein“ festgelegt ist, wird die Eigenschaft **Unterstützte IDs für gemischte Groß-/Kleinschreibung** deaktiviert.

Beispiel: Die Datenbank verwendet reguläre Bezeichner

In diesem Beispiel verwendet die Datenbank reguläre Bezeichner. Keiner der Bezeichner enthält ein reserviertes Schlüsselwort oder ein Sonderzeichen. Die Datenbank verwendet Bezeichner, die nicht zwischen Groß- und Kleinschreibung unterscheiden.

Legen Sie in der Datenbankverbindung die Eigenschaft **SQL-Kennungszeichen** auf (Keine) fest. Wenn die Eigenschaft **SQL-Kennungszeichen** auf „Keine“ festgelegt ist, wird die Eigenschaft **Bezeichner mit gemischter Groß-/Kleinschreibung unterstützen** deaktiviert.

Wenn der Datenintegrationsdienst SQL-Abfragen erzeugt, werden die Bezeichner nicht von Trennzeichen eingeschlossen.

Beispiel: Die Datenbank verwendet in Bezeichnern Schlüsselwörter oder Sonderzeichen

In diesem Beispiel verwendet die Datenbank in einigen Bezeichnern Schlüsselwörter oder Sonderzeichen. Die Datenbank verwendet Bezeichner, die nicht zwischen Groß- und Kleinschreibung unterscheiden.

Konfigurieren Sie die Bezeichnereigenschaften in der Datenbankverbindung wie folgt:

1. Legen Sie für die Eigenschaft **SQL-Kennungszeichen** das Zeichen fest, das die Datenbank für begrenzte Bezeichner verwenden soll.

In diesem Beispiel wird die Eigenschaft auf `"` (Anführungszeichen) festgelegt.

2. Löschen Sie die Eigenschaft **Bezeichner mit gemischter Groß-/Kleinschreibung unterstützen**.

Wenn der Datenintegrationsdienst SQL-Abfragen generiert, platziert der Dienst das ausgewählte Zeichen vor und hinter Bezeichnern, die reservierte Schlüsselwörter oder Sonderzeichen verwenden. Beispiel: Der Datenintegrationsdienst generiert die folgende Abfrage:

```
SELECT * FROM "MYTABLE$" /* identifier with special characters enclosed within delimited
character */
WHERE MYCOLUMN = 10 /* regular identifier not enclosed within delimited character */
```

Beispiel: Die Datenbank verwendet Bezeichner in Groß- und Kleinschreibung

In diesem Beispiel verwendet die Datenbank Bezeichner, die zwischen Groß- und Kleinschreibung unterscheiden. Die Datenbank kann in einigen Bezeichnern Sonderzeichen oder Schlüsselwörter verwenden.

Konfigurieren Sie die Bezeichnereigenschaften in der Datenbankverbindung wie folgt:

1. Legen Sie für die Eigenschaft **SQL-Kennungszeichen** das Zeichen fest, das die Datenbank für begrenzte Bezeichner verwenden soll.

In diesem Beispiel wird die Eigenschaft auf `"` (Anführungszeichen) festgelegt.

2. Wählen Sie die Eigenschaft **Bezeichner mit gemischter Groß-/Kleinschreibung unterstützen** aus.

Wenn der Datenintegrationsdienst SQL-Abfragen generiert, platziert der Dienst das ausgewählte Zeichen vor und hinter jedem Bezeichner. Beispiel: Der Datenintegrationsdienst generiert die folgende Abfrage:

```
SELECT * FROM "MyTable" /* case-sensitive identifier enclosed within delimited
character */
WHERE "MYCOLUMN" = 10 /* regular identifier enclosed within delimited character */
```

KAPITEL 10

Pläne

Dieses Kapitel umfasst die folgenden Themen:

- [Zeitpläne - Übersicht, 236](#)
- [Erstellen und Bearbeiten von Zeitplänen, 236](#)
- [Anhalten und Fortsetzen eines Zeitplans, 239](#)
- [Entfernen von Jobs aus einem Zeitplan, 240](#)
- [Löschen eines Zeitplans, 240](#)

Zeitpläne - Übersicht

Sie können einen Zeitplan erstellen, um die Ausführung von bereitgestellten Zuordnungen und Arbeitsabläufen anzugeben. Sie können ebenfalls das Datum und die Uhrzeit für die Ausführung von Profilen und Scorecards planen.

Beim Erstellen eines Zeitplans konfigurieren Sie, wann er ausgeführt wird. Sie können dem Zeitplan während dessen Erstellung Jobs hinzufügen oder den Zeitplan speichern und diesem später Jobs hinzufügen.

Sie können zum Beispiel einen Zeitplan zur Automatisierung von Routineaufgaben oder zum Verwalten der Ressourcennutzung in der Domäne definieren. Beispielsweise können Sie umfangreiche Zuordnungen so planen, dass diese zu unterschiedlichen Zeiten ausgeführt werden. Dadurch verhindern Sie eine mögliche Überlastung der Knoten. Sie können den Zeitplan auch anhalten, damit bestimmte Jobs nicht in den Ferien oder während der Domänenwartung ausgeführt werden.

Erstellen und Bearbeiten von Zeitplänen

Bevor Sie einen Job planen, erstellen Sie einen Zeitplan, in dem Sie definieren, wann der Job ausgeführt wird. Jobs können einmalig oder in einem bestimmten Intervall ausgeführt werden. Sie können Jobs beim Erstellen des Zeitplans planen oder diesem zu einem späteren Zeitpunkt Jobs hinzufügen.

Wenn Sie das Datum und die Uhrzeit für die Ausführung des Zeitplans konfigurieren, können Sie eine Zeitzone auswählen. Wenn Sie eine Startzeit für einen Zeitplan eingeben, handelt es sich bei der Zeitzone standardmäßig um die Zeitzone Ihres Clientcomputers. Wenn der Datenintegrationsdienst auf einem Clientcomputer in einer Zeitzone ausgeführt wird, die sich von der Zeitzone des Clients unterscheidet, müssen Sie sicherstellen, dass der Job zu einer angegebenen Zeit für diese Zeitzone ausgeführt wird. Sie können die Zeitzone beim Definieren des Zeitplans auswählen.

Sie können bereitgestellte Zuordnungen und Arbeitsabläufe planen. Dazu zählen Zuordnungen und Arbeitsabläufe für Profile und Scorecards. Optional können Sie eine Parameterdatei oder einen Parametersatz für den Job konfigurieren. Konfigurieren Sie eine Parameterdatei oder einen Parametersatz, wenn Sie das bereitgestellte Mapping bzw. den Arbeitsablauf mit unterschiedlichen Einstellungen ausführen möchten. Wenn der Scheduler-Dienst auf mehreren Knoten ausgeführt wird, müssen Sie die Parameterdatei in einem Verzeichnis speichern, auf das alle Knoten zugreifen können. Konfigurieren Sie das Verzeichnis in den Speichereigenschaften für den Scheduler-Dienst.

Optional können Sie die Eigenschaft **Ausführen als Benutzer** für den Job konfigurieren. Sie können die Eigenschaft konfigurieren, wenn Sie ein Objekt planen müssen, für das Sie über keine Berechtigung verfügen. Wenn Sie die Eigenschaft **Ausführen als Benutzer** konfigurieren, führen Sie den Job als Benutzer in der Domäne aus, der über die Berechtigung für das Objekt verfügt.

Nach dem Erstellen eines Zeitplans können Sie diesen bearbeiten. Wenn Sie einen Zeitplan bearbeiten, können Sie die Wiederholungsoptionen ändern, Jobs planen oder die Jobparameter ändern.

Erstellen eines Zeitplans

Erstellen Sie einen Zeitplan zur Ausführung von bereitgestellten Zuordnungen, bereitgestellten Arbeitsabläufen, Profilen oder Scorecards zu einem angegebenen Zeitpunkt.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie auf die Ansicht **Pläne**.
3. Klicken Sie auf **Aktionen > Zeitplan erstellen**.
Das Dialogfeld **Eigenschaften** wird angezeigt.
4. Geben Sie einen Namen und eine optionale Beschreibung für den Zeitplan ein.
5. Wählen Sie im Abschnitt **Wiederholung** die Option Einmal ausführen aus, um den Zeitplan einmalig auszuführen, oder wählen Sie Wiederholungszeitplan aus, um den Zeitplan in einem Intervall auszuführen.
6. Wenn Sie einen Wiederholungszeitplan erstellen, geben Sie an, ob der Job in einem Intervall – Täglich, Wöchentlich oder Monatlich – ausgeführt werden soll.

In der folgenden Tabelle werden die Wiederholungsoptionen beschrieben, die Sie konfigurieren können:

Option	Beschreibung
Täglich - Ausführen alle	Ausführung des Jobs alle n Tage
Täglich - Ausführen nach jeweils	Ausführung des Jobs alle n Minuten bzw. Stunden
Wöchentlich	Ausführung des Jobs an einem oder mehreren Wochentagen
Monatlich - Ausführen alle n Tage	Ausführung des Jobs an einem Tag des Monats
Monatlich - Ausführen alle	Ausführung des Jobs an einem Tag alle n Wochen des Monats
Monatlich - Jeden letzten Tag des Monats ausführen	Ausführung des Jobs am letzten Tag des Monats

7. Konfigurieren Sie im Abschnitt **Start** ein Startdatum und einen Anfangszeitpunkt für den Zeitplan.
8. Wählen Sie die Zeitzone für den Zeitplan aus der Liste aus.

Die Standardzeitzone entspricht der Zeitzone des Clientcomputers.

9. Wenn Sie einen Wiederholungsplan erstellen, können Sie optional ein Enddatum und eine Endzeit konfigurieren.

Sie können festlegen, dass die Wiederholung an einem bestimmten Datum oder nach n Ausführungen beendet wird.

Die folgende Abbildung zeigt den Scheduler-Assistenten:

Properties - Step 1 of 3

General

Name *

Description

Recurrence

☐ Run once

☒ Recurring Schedule

☒ Daily ☐ Run every days

☐ Weekly ☒ Run after every Minutes

☐ Monthly

Start

Time Zone

Start Date

Start Time HH:MM

End

☐ No End Date

☐ End Date

End Time HH:MM

☒ End After : Runs

10. Klicken Sie auf **Weiter**.
- Das Dialogfeld **Anwendungen** wird angezeigt.
11. Erweitern Sie einen Datenintegrationsdienst und wählen Sie im Zeitplan die auszuführenden Jobs aus.
12. Laden Sie optional eine Parameterdatei hoch, um Parameter für das Mapping oder den Arbeitsablauf zu definieren.
- Wählen Sie ein Mapping oder einen Arbeitsablauf aus.
Der Abschnitt **Anwendungseigenschaften** wird angezeigt.
 - Klicken Sie auf **Hochladen**.
Das Dialogfeld **Parameterdatei hochladen** wird angezeigt.
 - Klicken Sie auf **Dateien auswählen**.
 - Suchen Sie nach einer Datei und klicken Sie dann auf **Öffnen**.
 - Klicken Sie auf **OK**.
13. Wählen Sie optional einen Parametersatz aus.

14. Konfigurieren Sie optional die Eigenschaft **Ausführen als Benutzer**, um den Job als ein anderer Benutzer auszuführen.
 - a. Klicken Sie auf **Ändern**.
Das Dialogfeld **Ausführen als** wird angezeigt.
 - b. Erweitern Sie die Benutzerliste.
 - c. Wählen Sie einen Benutzer aus.
 - d. Geben Sie das Passwort für den Benutzer ein.
 - e. Klicken Sie auf **OK**.
15. Klicken Sie auf **Weiter**.
Das Fenster **Überprüfung** wird angezeigt. Es enthält eine Liste der Zeitplaneigenschaften.
16. Klicken Sie auf **Fertig stellen**, um den Zeitplan zu erstellen.
Der Zeitplan wird in der Liste der Zeitpläne im Navigator angezeigt.

Bearbeiten eines Zeitplans

Sie können einen Zeitplan im Administrator Tool bearbeiten. Sie können einen Zeitplan bearbeiten, um Wiederholungsoptionen zu ändern, Jobs zu planen oder Jobs mit anderen Parametern auszuführen.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie auf die Ansicht **Pläne**.
Im Domänen-Navigator werden die Zeitpläne in der Domäne aufgelistet.
3. Wählen Sie im Domänen-Navigator einen Zeitplan aus.
Im Inhaltsbereich werden die Zeitplaneigenschaften angezeigt.
4. Klicken Sie zum Bearbeiten des Zeitplans auf **Aktionen > Zeitplan bearbeiten**.

Anhalten und Fortsetzen eines Zeitplans

Sie können einen Zeitplan im Administrator Tool anhalten und fortsetzen. Es empfiehlt sich beispielsweise, einen Zeitplan anzuhalten, wenn Sie Wartungsarbeiten am Scheduler-Dienst ausführen.

Wenn Sie einen Zeitplan anhalten, werden die ausgeführten Jobs im Zeitplan gestoppt, bis Sie den Zeitplan fortsetzen.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie auf die Ansicht **Pläne**.
In der Ansicht **Alle Zeitpläne** werden die Zeitpläne in der Domäne aufgelistet.
3. Wählen Sie einen Zeitplan aus. Verwenden Sie die **Strg-Taste** und die **Umschalttaste**, um mehrere Zeitpläne auszuwählen.
4. Klicken Sie zum Anhalten des Zeitplans auf **Anhalten**.
Die Meldung **Anhalten bestätigen** wird angezeigt.
5. Klicken Sie auf **OK**.
Die Meldung **Zeitplanstatus ändern** wird angezeigt.

6. Klicken Sie auf **OK**.
Der Zeitplanstatus wird in „Angehalten“ geändert.
7. Zum Fortsetzen des Zeitplans wählen Sie diesen aus und klicken dann auf **Fortsetzen**.
Die Meldung **Fortsetzen bestätigen** wird angezeigt.
8. Klicken Sie auf **OK**.
Die Meldung **Zeitplanstatus ändern** wird angezeigt.
9. Klicken Sie auf **OK**.
Der Zeitplanstatus wird in „Geplant“ geändert.

Entfernen von Jobs aus einem Zeitplan

Sie können einen bereitgestellten Zuordnungs-, Profil-, Scorecard- oder Arbeitsablauf-Job aus einem Zeitplan entfernen.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie auf die Ansicht **Pläne**.
3. Klicken Sie auf die Ansicht **Geplante Aufträge**.
Im Inhaltsbereich wird eine Liste der geplanten Jobs angezeigt.
4. Wählen Sie den Job aus, den Sie aus einem Zeitplan entfernen möchten.
5. Klicken Sie auf **Aktionen > Zeitplanzuordnung löschen**.
Die Meldung **Job-Entfernung bestätigen** wird angezeigt.
6. Klicken Sie auf **OK**.
Der Job wird aus dem Zeitplan und der Ansicht **Geplante Aufträge** entfernt.

Löschen eines Zeitplans

Sie können einen Zeitplan im Administrator Tool löschen.

Wenn Sie einen Zeitplan löschen, werden alle ausgeführten Jobs zu Ende ausgeführt und alle künftigen Ausführungen abgebrochen. Wenn die Ausführung der Jobs nicht gestoppt werden soll, fügen Sie sie vor dem Löschen des Zeitplans einem anderen Zeitplan hinzu.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten**.
2. Klicken Sie auf die Ansicht **Pläne**.
In der Ansicht **Alle Zeitpläne** werden alle Zeitpläne in der Domäne aufgelistet.
3. Wählen Sie in der Ansicht **Alle Zeitpläne** einen Zeitplan aus. Verwenden Sie die **Strg-Taste** und die **Umschalttaste**, um mehrere Zeitpläne auszuwählen.
4. Klicken Sie auf **Aktionen > Zeitplan löschen**.
Das Dialogfeld **Löschen bestätigen** wird geöffnet.
5. Klicken Sie auf **OK**, um den Zeitplan zu löschen.

KAPITEL 11

Exportieren und Importieren von Domänenobjekten

Dieses Kapitel umfasst die folgenden Themen:

- [Export und Import von Domänenobjekten - Übersicht , 241](#)
- [Exportprozess, 242](#)
- [Domänenobjekte anzeigen, 242](#)
- [Importprozess, 244](#)

Export und Import von Domänenobjekten - Übersicht

Mit Hilfe der Befehlszeile können Sie Objekte zwischen unterschiedlichen Domänen derselben Version migrieren.

Beispielsweise können Domänenobjekte aus der Entwicklungsumgebung in eine Test- oder Produktionsumgebung migriert werden.

Verwenden Sie zum Exportieren und Importieren von Domänenobjekten die folgenden infacmd isp Befehle:

ExportDomainObjects

Exportiert native Benutzer, native Gruppen, Rollen und Verbindungen in eine XML-Datei.

ImportDomainObjects

Importiert native Benutzer, native Gruppen, Rollen und Verbindungen in eine Informatica-Domäne.

Mit einer infacmd-Kontrolldatei können Sie beim Exportieren und Importieren die Objekte filtern.

Mit dem Befehl `infacmd xrf generateReadableViewXML` können Sie außerdem eine lesbare XML-Datei aus einer Exportdatei generieren. Prüfen Sie die lesbare XML-Datei, um herauszufinden, ob die importierten Objekte gefiltert werden müssen.

Exportprozess

Sie können die Befehlszeile zum Exportieren von Domänenobjekten aus einer Domäne verwenden.

Führen Sie die folgenden Schritte durch, wenn Sie ein Domänenobjekt exportieren möchten:

1. Bestimmen Sie, welche Domänenobjekte exportiert werden sollen.
2. Wenn Sie nicht alle Domänenobjekte exportieren möchten, erstellen Sie eine Export-Steuerdatei, um die zu exportierenden Objekte herauszufiltern.
3. Führen Sie den Befehl `infacmd isp exportDomainObjects` aus, um die Domänenobjekte zu exportieren.

Der Befehl exportiert die Domänenobjekte in eine Exportdatei. Sie können diese Datei zum Importieren in eine andere Domäne nutzen.

Regeln und Richtlinien für das Exportieren von Domänenobjekten

Lesen Sie die folgenden Regeln und Richtlinien, bevor Sie Domänenobjekte exportieren:

- Wenn Sie einen Benutzer exportieren, wird standardmäßig nicht das Passwort des Benutzers exportiert. Wenn Sie das Passwort nicht exportieren, muss der Administrator das Passwort für den Benutzer zurücksetzen, nachdem der Benutzer in die Domäne importiert wurde. Wenn Sie jedoch den Befehl `infacmd isp exportDomainObjects` ausführen, können Sie wählen, eine verschlüsselte Version des Passworts zu exportieren.
- Wenn Sie einen Benutzer exportieren, werden die zugehörigen Gruppen des Benutzers nicht exportiert. Weisen Sie gegebenenfalls den Benutzer der Gruppe zu, nachdem Sie den Benutzer und die Gruppe importieren haben.
- Wenn Sie eine Gruppe exportieren, werden alle Untergruppen und Benutzer in der Gruppe exportiert.
- Sie können den Administrator-Benutzer, die Administrator-Rolle, die Gruppe "Jeder" und LDAP-Benutzer oder -Gruppen nicht exportieren. Um LDAP-Benutzer und -Gruppen in einer Informatica-Domäne zu ersetzen, exportieren Sie die LDAP-Benutzer und -Gruppen direkt aus dem LDAP-Verzeichnisdienst.
- Um native Benutzer und Gruppen aus Domänen der verschiedenen Versionen zu exportieren, verwenden Sie den Befehl `infacmd isp exportUsersAndGroups`.
- Wenn Sie eine Verbindung exportieren, wird standardmäßig nicht das Verbindungspasswort exportiert. Wenn Sie das Passwort nicht exportieren, muss der Administrator das Passwort für die Verbindung zurücksetzen, nachdem die Verbindung in die Domäne importiert wurde. Wenn Sie jedoch den Befehl `infacmd isp exportDomainObjects` ausführen, können Sie wählen, eine verschlüsselte Version des Passworts zu exportieren.

Domänenobjekte anzeigen

Sie können die Namen und Eigenschaften von Domänenobjekten in der exportierten XML-Datei anzeigen lassen.

Führen Sie den Befehl `infacmd xrf generateReadableViewXML` aus, um aus der Exportdatei eine lesbare XML-Datei zu erstellen.

Der nachfolgende Abschnitt stellt eine lesbare XML-Datei dar:

```
<global:View xmlns:global="http://global" xmlns:connection="http://connection"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="
  http://connection connection.xsd http://global globalSchemaDomain.xsd http://global
```

```

globalSchema.xsd">
<NativeUser isAdmin="false" name="admin" securityDomain="Native" viewId="0">
  <UserInfo email="" fullName="admin" phone="" viewId="1"/>
</NativeUser>
<User isAdmin="false" name="User1" securityDomain="Native" viewId="15">
  <UserInfo email="" fullName="NewUSer" phone="" viewId="16"/>
</User>
<Group name="TestGroup1" securityDomain="Native" viewId="182">
  <UserRef name="User1" securityDomain="Native" viewId="183"/>
  <UserRef name="User6" securityDomain="Native" viewId="188"/>
</Group>
<Role customRole="false" name="Administrator" viewId="242">
  <Description viewId="243">Provides all privilege and permission access to an
Informatica service.</Description>
  <ServicePrivilegeDefinition name="PwxListenerService" viewId="244">
    <Privilege category="" isEnabled="true" name="close" viewId="245"/>
    <Privilege category="" isEnabled="true" name="closeforce" viewId="246"/>
    <Privilege category="" isEnabled="false" name="Management Commands" viewId="249"/>
    <Privilege category="" isEnabled="false" name="Informational Commands"
viewId="250"/>
  </ServicePrivilegeDefinition>
</Role>
<Connection connectionString="inqa85sql25@qa90"
connectionType="SQLServerNativeConnection"
domainName="" environmentsSQL="" name="conn4" ownerName=""
schemaName="" transactionSQL="" userName="dummy" viewId="7512">
  <ConnectionPool maxIdleTime="120" minConnections="0" usePool="true" viewId="7514"/>
</Connection>
</global:View>

```

Darstellbare Domänenobjektnamen

Sie können die folgenden Namen von Domänenobjekten in einer lesbaren XML-Datei anzeigen:

Benutzer
 UserInfo
 Rolle
 ServicePrivilegeDef
 Berechtigung
 Group
 GroupRef
 UserRef
 ConnectInfo
 ConnectionPoolAttributes

Unterstützte Verbindungstypen

DB2iNativeConnection
 DB2NativeConnection
 DB2zNativeConnection
 JDBCConnection
 ODBCNativeConnection
 OracleNativeConnection
 PWXMetaConnection
 SAPConnection

Importprozess

Sie können die Befehlszeile zum Importieren von Domänenobjekten aus einer Exportdatei in eine Domäne verwenden.

Führen Sie die folgenden Schritte durch, wenn Sie Domänenobjekte importieren möchten:

1. Führen Sie den Befehl `xrf generateReadableViewXML` aus, um aus der Exportdatei eine lesbare XML-Datei zu erstellen. Sehen Sie die Domänenobjekte in der lesbaren XML-Datei durch und legen Sie fest, welche Objekte importiert werden sollen.
2. Wenn Sie nicht alle Domänenobjekte aus der Exportdatei importieren möchten, erstellen Sie eine Import-Steuerdatei, um die zu importierenden Objekte herauszufiltern.
3. Führen Sie den Befehl `infacmd isp importDomainObjects` aus, um die Domänenobjekte in die angegebene Domäne zu importieren.
4. Nach dem Importieren der Objekte, ist es eventuell erforderlich, andere Domänenobjekte wie Anwendungsdienst und Ordner zu erstellen.

Regeln und Richtlinien für den Import von Domänenobjekten

Beachten Sie die folgenden Regeln und Richtlinien, ehe Sie Domänenobjekte importieren:

- Wenn Sie eine Gruppe importieren, importieren Sie auch alle zugehörigen Untergruppen und Benutzer dieser Gruppe.
- Um native Benutzer und Gruppen von Domänen verschiedener Versionen zu importieren, verwenden Sie den Befehl `infacmd isp importUsersAndGroups`.
- Nach dem Importieren eines Benutzers oder einer Gruppe, können Sie den Benutzer oder diese Gruppe nicht mehr umbenennen.
- Rollen werden unabhängig von Benutzern oder Gruppen importiert. Weisen Sie den Benutzern und Gruppen Rollen zu, nachdem Sie die Rollen, Benutzer und Gruppen importiert haben.
- Sie können die Administrator-Gruppe, den Administrator-Benutzer, die Administrator-Rolle, die Gruppe „Jeder“ bzw. LDAP-Benutzer und -Gruppen nicht importieren.

Konfliktlösung

Ein Konflikt tritt immer dann auf, wenn Sie versuchen, ein Objekt mit einem Namen zu importieren, der bereits für ein Objekt in der Zieldomäne vergeben wurde. Durch Konfigurieren der Konfliktlösung können Sie bestimmen, wie bei Konflikten während des Imports verfahren werden soll.

Eine Konfliktlösungsstrategie bestimmen Sie entweder über die Befehlszeile oder die Kontrolldatei beim Importieren der Objekte. Wenn Sie die Konfliktlösung über die Befehlszeile und die Kontrolldatei vorgeben, hat die Kontrolldatei Priorität. Tritt ein Konflikt auf, ohne dass Sie eine Konfliktlösungsstrategie festgelegt haben, schlägt der Import fehl.

Sie können eine der folgenden Konfliktlösungsstrategien konfigurieren:

Erneut verwenden

Wiederverwendung des Objekts in der Target-Domäne

Umbenennen

Umbenennen des Quellobjekts Entweder Sie geben einen Namen in der Kontrolldatei an, oder der Name wird generiert. Ein generierter Name hat am Ende eine angehängte Nummer.

Ersetzen

Das Target-Objekt wird durch das Quellobjekt ersetzt.

Zusammenführen

Führt Quell- und Target-Objekte zu einer Gruppe zusammen. Wenn Sie zum Beispiel Gruppen desselben Namens zusammenführen, werden die Benutzer und Untergruppen beider Gruppen in der Gruppe im Target-Objekt zusammengeführt.

Sie können die Konfliktlösungsstrategie bei einem Zusammenführungskonflikt nicht über die Befehlszeile definieren. Verwenden Sie eine Steuerungsdatei zum Definieren der Lösungsstrategie bei Zusammenführungskonflikten. Sie müssen den Abschnitt des Gruppenobjektyps mit Zusammenführung als Konfliktlösungsrichtlinie mit erneuter Verwendung, Austausch oder Umbenennen für alle in Konflikt stehenden Benutzer in der Steuerungsdatei einbeziehen.

Geben Sie zum Beispiel die Lösungsstrategie bei Zusammenführungskonflikten für die folgenden Gruppen an:

- Gruppe A mit Benutzern a1, a2, b1, b2 in der Quelldomäne
- Gruppe A mit Benutzern a1, a2, a3, b1, b2 in der Zieldomäne

Sie erhalten die folgenden Ergebnisse in der Gruppe nach dem Zusammenführen in der Zieldomäne:

- a1, a2, b1, b2, wenn Sie sich zur Wiederverwendung oder zum Ersatz entscheiden
- a1, a2, a3, b1, b2, wenn Sie sich zum Umbenennen entscheiden

KAPITEL 12

Lizenzverwaltung

Dieses Kapitel umfasst die folgenden Themen:

- [Lizenzverwaltung - Übersicht, 246](#)
- [Arten von Lizenzschlüsseln, 248](#)
- [Ein Lizenzobjekt erstellen, 249](#)
- [Eine Lizenz einem Dienst zuweisen, 250](#)
- [Entfernen eine Lizenz von einem Anwendungsdienst, 251](#)
- [Aktualisieren einer Lizenz, 251](#)
- [Entfernen einer Lizenz, 252](#)
- [Lizenzeigenschaften, 252](#)

Lizenzverwaltung - Übersicht

Der Dienstmanager auf dem Master-Gateway-Knoten verwaltet die Informatica-Lizenzen.

Mit einer Lizenz können Sie die folgenden Aufgaben ausführen:

- Ausführen von Anwendungsdiensten wie der Analyst-Dienst, Datenintegrationsdienst und PowerCenter-Repository-Dienst.
- Verwenden von Add-On-Optionen wie Partitionierung für PowerCenter, Gitter und hohe Verfügbarkeit.
- Zugriff auf bestimmte Typen von Verbindungen wie Oracle, Teradata, Microsoft SQL Server und IBM MQ Series.
- Verwenden von Metadaten Exchange-Optionen wie Metadaten Exchange für Cognos und Metadaten Exchange für Rational Rose.

Beim Installieren von Informatica erstellt das Installationsprogramm basierend auf dem von Ihnen für die Installation verwendeten Lizenzschlüssel ein Lizenzobjekt in der Domäne.

Sie müssen jedem Anwendungsdienst ein Lizenzobjekt zuordnen, um den Dienst zu aktivieren. So müssen Sie zum Beispiel dem PowerCenter-Integrationsdienst eine Lizenz zuordnen, bevor Sie einen Arbeitsablauf mit dem PowerCenter-Integrationsdienst ausführen können.

Sie können weitere Lizenzobjekte in der Domäne erstellen. Basierend auf Ihren Projektanforderungen benötigen Sie möglicherweise mehrere Lizenzobjekte. Beispielsweise können Sie zwei Lizenzobjekte haben, wobei jedes Lizenzobjekt Ihnen ermöglicht, Dienste auf einem anderen Betriebssystem auszuführen. Sie können auch mehrere Lizenzobjekte verwenden, um mehrere Projekte in derselben Domäne zu verwalten. Ein Projekt benötigt eventuell Zugriff auf bestimmte Datenbanktypen, während dies für das andere Projekt nicht erforderlich ist.

Lizenzvalidierung

Beim Starten der Anwendungsprozesse werden diese vom Service Manager validiert. Der Service Manager validiert für jeden Dienstprozess die folgenden Informationen:

- Produktversion. Stellt sicher, dass Sie die richtige Version der Informatica Services ausführen.
- Plattform. Stellt sicher, dass die Informatica Services auf einem lizenzierten Betriebssystem ausgeführt werden.
- Ablaufdatum. Überprüft, dass die Lizenz nicht erloschen ist. Erlischt die Lizenz, kann kein der Lizenz zugeordneter Anwendungsdienst starten. Sie müssen den Informatica Services eine gültige Lizenz zuordnen, um sie starten zu können.
- PowerCenter-Optionen. Bestimmt die Optionen, die von den Informatica Services verwendet werden können. So prüft beispielsweise der Service Manager, ob der PowerCenter Integration Service die Sitzung mit Gitteroption nutzen kann.
- Konnektivität. Überprüft Verbindungen, die von den Informatica Services verwendet werden können. Zum Beispiel prüft der Service Manager, ob PowerCenter sich mit einer IBM DB2 Datenbank verbinden kann.
- Metadaten austausch-Optionen. Bestimmt die Metadaten austausch-Optionen, die für die Nutzung zur Verfügung stehen. Beispielsweise prüft der Service Manager, dass Sie Zugriff auf den Metadaten austausch für Business-Objekt-Designer haben.

Lizenzierungsprotokollereignisse

Der Service Manager generiert Protokollereignisse und schreibt diese in den Protokoll-Manager. Protokollereignisse werden für folgende Aktionen generiert:

- Erstellen oder Löschen einer Lizenz.
- Zuweisen eines inkrementellen Lizenzschlüssels an eine Lizenz.
- Zuweisen eines Anwendungsdienstes an eine Lizenz.
- Entfernen einer Lizenz von einem Anwendungsdienst.
- Ablauf der Lizenz.
- Der Service Manager trifft auf einen Fehler, zum Beispiel einen Validierungsfehler.

Ein Protokollereignis enthält den Benutzernamen und den Zeitpunkt des Ereignisses.

Sie müssen eine Berechtigung für die Domäne besitzen, um die Protokolle für die Lizenzierungsereignisse anzuzeigen.

Die Lizenzierungsereignisse werden in den Domänenprotokollen angezeigt.

Lizenzverwaltungstasks

Sie können die folgenden Tasks zur Lizenzverwaltung ausführen:

- Lizenz im Administrator Tool erstellen. Zur Erstellung einer Lizenz im Administrator Tool brauchen Sie einen Lizenzschlüssel.
- Zuweisung einer Lizenz zu jedem Anwendungsdienst. Weisen Sie jedem Anwendungsdienst eine Lizenz zu, um den Dienst zu aktivieren.
- Zuweisung einer Lizenz aus einem Anwendungsdienst entfernen. Sie müssen die Zuweisung der Lizenz zum Anwendungsdienst rückgängig machen, wenn Sie den Dienst einstellen oder von einer Entwicklungsumgebung in eine Produktionsumgebung migrieren möchten. Nachdem Sie die Lizenz des Dienstes aufgehoben haben, können Sie den Dienst erst wieder aktivieren, wenn Sie ihm eine neue gültige Lizenz zuweisen.

- Aktualisieren der Lizenz. Wenn Sie der vorhandenen Lizenz PowerCenter-Optionen hinzufügen möchten, müssen Sie die Lizenz aktivieren.
- Entfernen der Lizenz. Lizenzen müssen entfernt werden, wenn sie veraltet sind.
- Konfigurieren von Benutzerberechtigungen für eine Lizenz.
- Anzeigen von Lizenzdetails. Möglicherweise müssen Sie die Lizenz überprüfen, um Details wie das Ablaufdatum und die maximale Anzahl der lizenzierten CPUs festzustellen. Diese Details müssen Sie manchmal nachprüfen, damit gewährleistet ist, dass Sie die Lizenzbedingungen einhalten. Zur Feststellung der Details für jede Lizenz verwenden Sie das Administrator Tool.
- Überwachen der Lizenznutzung und der lizenzierten Optionen. Sie können die Nutzung der logischen CPUs und der PowerCenter Repository Services überwachen. Außerdem können Sie die Anzahl der für eine Lizenz erworbenen Softwareoptionen überwachen und anhand des Lizenzverwaltungsberichts feststellen, wie oft die Nutzungsgrenzen bei einer Lizenz überschritten wurden.

All diese Tasks können Sie mit dem Administrator Tool oder anhand von *infacmd isp*-Befehlen ausführen.

Arten von Lizenzschlüsseln

Informatica bietet Lizenzschlüssel in Lizenzdateien an. Der Lizenzschlüssel ist verschlüsselt. Wenn Sie aus einer Lizenzschlüsseldatei eine Lizenz erstellen, entschlüsselt der Service Manager den Lizenzschlüssel und ermöglicht den Erwerb von Optionen.

Sie erstellen eine Lizenz aus einer Lizenzschlüsseldatei. Sie weisen die Lizenzschlüssel der Lizenz zu, um zusätzliche Optionen zu aktivieren. Informatica verwendet folgende Arten von Lizenzschlüsseln:

- Originalschlüssel Informatica generiert einen Originalschlüssel auf der Basis Ihres Vertrags. Je nach Vertrag kann Informatica auch mehrere Originalschlüssel bereitstellen.
- Inkrementelle Schlüssel Informatica generiert inkrementelle Schlüssel auf der Basis der Updates einer vorhandenen Lizenz, z. B. eine erweiterte Lizenzperiode oder eine zusätzliche Option.

Hinweis: Lizenzen von Informatica ändern sich im Allgemeinen bei jeder Version. Verwenden Sie eine für die aktuelle Version gültige Lizenzschlüsseldatei, um sicherzustellen, dass Ihre Installation alle Funktionen enthält.

Originalschlüssel

Mit einem Originalschlüssel lassen sich der Vertrag, das Produkt und die lizenzierten Funktionen identifizieren. Zu den lizenzierten Funktionen gehört die Informatica-Edition, der Bereitstellungstyp, die Anzahl der autorisierten CPUs und die autorisierten Informatica-Optionen und -Konnektivität. Sie verwenden die Originalschlüssel, um Informatica zu installieren und Lizenzen für die Dienste zu erstellen. Um Informatica zu installieren, benötigen Sie einen Lizenzschlüssel. Das Installationsprogramm erstellt ein Lizenzobjekt für die Domäne im Administrator Tool. Sie können weitere Originalschlüssel dazu verwenden, zusätzliche Lizenzen in derselben Domäne zu erstellen. Für jedes Lizenzobjekt ist ein anderer Originalschlüssel erforderlich.

Inkrementelle Schlüssel

Inkrementelle Schlüssel dienen der Aktualisierung bereits existierender Lizenzen. Inkrementelle Schlüssel fügen Sie einer existierenden Lizenz hinzu, wenn Sie Optionen wie PowerCenter-Optionen, die Konnektivität und Optionen zum Metadatenaustausch hinzufügen oder entfernen möchten. Wenn zum Beispiel eine

existierende Lizenz keine hohe Verfügbarkeit gewährleistet, können Sie zur existierenden Lizenz einen inkrementellen Schlüssel mit der Hochverfügbarkeitsoption hinzufügen.

Der Service Manager aktualisiert das Ablaufdatum der Lizenz, wenn das Ablaufdatum des inkrementellen Schlüssels später als das Ablaufdatum eines Originalschlüssels liegt. Der Service Manager nutzt das späteste Ablaufdatum. Ein Lizenzobjekt kann verschiedene Ablaufdaten für Optionen in der Lizenz haben. So kann die relationale Konnektivitätsoption der IBM DB2 zum Beispiel am 12.01.2006 und die Option für Gittersitzungen am 04.01.06 erlöschen.

Der Service Manager validiert den inkrementellen Schlüssel gegen den für die Lizenzerstellung benutzten Originalschlüssel. Sind die Schlüssel nicht kompatibel, wird eine Fehlermeldung ausgegeben.

Ein Lizenzobjekt erstellen

Sie haben die Möglichkeit, ein Lizenzobjekt in einer Domäne zu erstellen und die Lizenz zu Anwendungsdiensten hinzuzufügen. Die Lizenzerstellung erfolgt im Administrator Tool mittels einer Lizenzschlüsseldatei. Die Lizenzschlüsseldatei enthält einen verschlüsselten Originalschlüssel. Den Originalschlüssel brauchen Sie für die Lizenzerstellung.

Alternativ können Sie auch mit dem Befehl `infacmd isp AddLicense` eine Lizenz zu einer Domäne hinzufügen.

Für die Lizenzerstellung gelten folgende Richtlinien:

- Verwenden Sie eine gültige Lizenzschlüsseldatei. Die Lizenzschlüsseldatei muss einen Originallizenzschlüssel enthalten. Die Lizenzschlüsseldatei darf nicht abgelaufen sein.
- Für mehrere Lizenzen können Sie nicht dieselbe Lizenzschlüsseldatei einsetzen. Jede Lizenz muss einen eindeutigen Originalschlüssel besitzen.
- Geben Sie für jede Lizenz einen eindeutigen Namen ein. Den Namen für die Lizenz müssen Sie bei der Lizenzerstellung angeben. Der Name darf unter allen Objekten in der Domäne nur einmal vorkommen.
- Legen Sie die Lizenzschlüsseldatei an einem Speicherort ab, auf den der Administrator Tool-Computer zugreifen kann. Beim Erstellen des Lizenzobjekts müssen Sie den Speicherort der Lizenzschlüsseldatei angeben.

Nachdem Sie die Lizenz erstellt haben, können Sie die Beschreibung ändern. Um die Beschreibung einer Lizenz zu ändern, wählen Sie die Lizenz im Navigator des Administrator Tools und klicken Sie auf Bearbeiten.

1. Klicken Sie im Administrator Tool auf **Aktionen > Neu > Lizenz**.

Das Fenster **Lizenz erstellen** wird aufgerufen.

2. Geben Sie folgende Optionen ein:

Option	Beschreibung
Name	Name der Lizenz. Beim Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden, und er muss in der Domäne eindeutig sein. Er darf nicht länger als 128 Zeichen sein oder mit @ beginnen. Außerdem darf er keine Leerzeichen oder die folgenden Sonderzeichen enthalten: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () []
Beschreibung	Beschreibung der Lizenz. Die Beschreibung darf nicht länger als 765 Zeichen sein.

Option	Beschreibung
Pfad	Pfad der Domäne, in der Sie die Lizenz erstellen. Schreibgeschütztes Feld. Klicken Sie optional auf Durchsuchen und wählen Sie im Fenster Ordner auswählen eine Domäne. Optional klicken Sie auf Ordner erstellen , um einen Ordner für die Domäne zu erstellen.
Lizenzdatei	Die Datei, die den Originalschlüssel enthält. Klicken Sie auf Durchsuchen , um die Datei zu suchen.

Wenn Sie versuchen, eine Lizenz mit einem inkrementellen Schlüssel zu erstellen, wird eine Meldung eingeblendet, die besagt, dass Sie erst einen inkrementellen Schlüssel angeben können, nachdem Sie einen Originalschlüssel hinzugefügt haben.

Zur Erstellung einer Lizenz ist ein Originalschlüssel erforderlich.

3. Klicken Sie auf **Erstellen**.

Eine Lizenz einem Dienst zuweisen

Sie müssen einem Anwendungsdienst eine Lizenz zuweisen, bevor Sie den Dienst aktivieren können. Wenn Sie einem Dienst eine Lizenz zuweisen, aktualisiert der Service Manager die Metadaten der Lizenz. Sie können auch den Befehl *infacmd isp AssignLicense* verwenden, um einer Lizenz einen Dienst zuzuweisen.

1. Wählen Sie die Lizenz im **Domänen-Navigator** des Administrator Tools aus.
2. Klicken Sie auf die Registerkarte **Zugewiesene Dienste**.
3. Auf der Registerkarte **Lizenz**, klicken Sie auf **Aktionen > Zugewiesene Dienste bearbeiten**.
Das Fenster **Lizenz den Diensten zuweisen oder nicht zuweisen** erscheint.
4. Wählen Sie die Dienste unter **Nicht zugewiesene Dienste** aus und klicken Sie auf Hinzufügen.
Mit Strg-Klick wählen Sie mehrere Dienste aus. Mit Umsch-Klick wählen Sie eine zusammenhängende Liste von Diensten aus. Sie können auch auf **Alle hinzufügen** klicken, um die Lizenz allen Diensten zuzuweisen.
5. Klicken Sie auf **OK**.

Regeln und Richtlinien zum Zuweisen von Lizenzen an einen Dienst

Halten Sie sich an die folgenden Regeln und Richtlinien, wenn Sie Lizenzen zuweisen:

- Sie können Lizenzen zuweisen, um Dienste zu deaktivieren.
- Wenn Sie einem Dienst eine Lizenz zuweisen möchten, der bereit seine Lizenz besitzt, müssen Sie die vorhandene Lizenz zunächst von diesem Dienst entfernen.
- Um einen Dienst mit einem Backup-Knoten zu starten, müssen Sie diesem eine Lizenz mit einer höheren Verfügbarkeit zuweisen.
- Um einen Dienst automatisch zu starten, müssen Sie diesem eine Lizenz mit einer höheren Verfügbarkeit zuweisen.

Entfernen eine Lizenz von einem Anwendungsdienst

Möglicherweise müssen Sie die Zuordnung einer Lizenz bei einem Dienst aufheben, wenn der Dienst veraltet ist oder Sie einen Dienst nicht weiter betreiben wollen. Vielleicht möchten Sie einen Dienst nicht fortsetzen, wenn Sie mit mehr CPUs arbeiten als lizenziert sind.

Sie können das Administrator Tool oder den Befehl `infacmd isp UnassignLicense` verwenden, um die Zuordnung einer Lizenz für einen Dienst aufzuheben.

Bevor Sie die Zuordnung einer Lizenz aufheben können, müssen Sie den Dienst deaktivieren. Nachdem Sie eine Lizenz von dem Dienst entfernt haben, können Sie den Dienst nicht aktivieren. Sie müssen eine gültige Lizenz zuweisen, um den Dienst wieder aktivieren zu können.

Sie müssen den Dienst deaktivieren, bevor Sie die Lizenz entfernen können. Wenn Sie versuchen, eine Lizenz von einem aktivierten Dienst zu entfernen, wird eine Meldung angezeigt, die besagt, dass der Dienst nicht entfernt werden kann, weil er ausgeführt wird.

1. Wählen Sie die Lizenz im **Domänen-Navigator** des Administrator Tools aus.
2. Klicken Sie auf die Registerkarte **Zugewiesene Dienste**.
3. Auf der Registerkarte **Lizenz** klicken Sie auf **Aktionen > Zugewiesene Dienste bearbeiten**.
Das Fenster **Diese Lizenz zu Services zuweisen oder Zuordnung aufheben** wird angezeigt.
4. Wählen Sie unter **Zugewiesener Dienst** den Dienst aus, und klicken Sie dann auf **Entfernen**. Klicken Sie optional auf **Alle entfernen**, um alle zugewiesenen Dienste aufzuheben.
5. Klicken Sie auf **OK**.

Aktualisieren einer Lizenz

Sie können die aktuelle Lizenz in der Informatica-Domäne mit einem inkrementellen Lizenzschlüssel aktualisieren. aktualisieren.

Wenn Sie einen inkrementellen Schlüssel zu einer Lizenz hinzufügen, fügt der Dienstmanager lizenzierte Optionen hinzu oder entfernt diese, und aktualisiert das Ablaufdatum der Lizenz.

Sie können auch den Befehl `infacmd isp UpdateLicense` benutzen, um einen inkrementellen Schlüssel zu einer Lizenz hinzuzufügen.

Nach dem Aktualisieren der Lizenz müssen Sie die Informatica-Dienste neu starten, damit die Änderungen wirksam werden.

Verwenden Sie die folgenden Richtlinien, um eine Lizenz zu aktualisieren:

- Überprüfen Sie, ob die Lizenzschlüsseldatei für den Computer mit dem Administrator Tool zugänglich ist. Wenn Sie das Lizenzobjekt aktualisieren, müssen Sie den Speicherort der Lizenzschlüsseldatei angeben.
- Die inkrementelle Schlüssel muss mit dem Originalschlüssel kompatibel sein. Ein Fehler wird angezeigt, wenn die Schlüssel nicht kompatibel sind.

Der Dienstmanager validiert den inkrementellen Schlüssel gegen den ursprünglichen Schlüssel entsprechend den folgenden Informationen:

- Seriennummer
- Bereitstellungsart
- Händler

- Informatica-Ausgabe
 - Informatica Version:
1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten** > Ansicht **Dienste und Knoten**.
 2. Wählen Sie im Domänen-Navigator eine **Lizenz** aus.
 3. Klicken Sie auf **Aktionen verwalten** > **Inkrementellen Schlüssel hinzufügen**.
Das Fenster **Lizenz aktualisieren** wird angezeigt.
 4. Klicken Sie auf **Dateien auswählen**, um zu einer Lizenzschlüsseldatei zu navigieren.
 5. Klicken Sie auf **OK**.
 6. Im Abschnitt **Lizenzdetails** in der Ansicht **Eigenschaften** klicken Sie auf **Bearbeiten**, um die Beschreibung der Lizenz zu bearbeiten.
 7. Klicken Sie auf **OK**.

Entfernen einer Lizenz

Sie können eine Lizenz mit dem Administrator Tool oder dem Befehl *infacmd isp RemoveLicense* aus einer Domäne entfernen.

Deaktivieren Sie vor dem Entfernen einer Lizenz alle Dienste, die der Lizenz zugewiesen sind. Wenn Sie die Dienste nicht deaktivieren, werden alle laufenden Prozesse beim Entfernen der Lizenz abgebrochen. Wenn Sie eine Lizenz zu entfernen, hebt der Service Manager die Lizenz für jeden zugewiesenen Dienst auf und entfernt die Lizenz aus der Domäne. Zur erneuten Aktivierung eines Dienstes weisen Sie ihm eine andere Lizenz zu.

Wenn Sie eine Lizenz entfernen, können Sie noch immer die Lizenznutzungs-Logs im Log Viewer für diese Lizenz anzeigen, aber Sie können keinen Lizenzbericht für diese Lizenz ausführen.

So entfernen Sie eine Lizenz aus der Domäne:

1. Wählen Sie die Lizenz im **Domänen-Navigator** des Administrator Tools aus.
2. Klicken Sie auf **Aktionen** > **Löschen**.

Lizenzeigenschaften

Sie können Lizenzdetails mithilfe des Administrator-Tools oder des *infacmd isp ShowLicense*-Befehls anzeigen.

Die Lizenzdetails basieren auf allen Lizenzschlüsseln, die der Lizenz zugewiesen wurden. Der Service Manager aktualisiert die vorhandenen Lizenzdetails, wenn Sie einen neuen inkrementellen Schlüssel zur Lizenz hinzufügen.

Sie können die Lizenzdetails überprüfen und Optionen festlegen, die verfügbar sein sollen. Darüber hinaus können Sie die Lizenzdetails und Lizenznutzungsprotokolle auch beim Überwachen der Lizenzen überprüfen.

Zum Beispiel: Sie können die Anzahl der CPUs festlegen, für die Ihr Unternehmen pro Betriebssystem lizenziert ist.

Um die Lizenzdetails anzuzeigen, wählen Sie die Lizenz im **Domänen-Navigator** aus.

Das Administrator-Tool zeigt die Lizenzeigenschaften in den folgenden Abschnitten an:

- **Lizenzdetails:** Auf der Registerkarte **Eigenschaften** werden die Lizenzdetails angezeigt. Hier erscheinen die Attribute zu den Lizenzen, wie Lizenzobjektname, Beschreibung und Ablaufdatum.
- **Unterstützte Plattformen:** Auf der Registerkarte **Eigenschaften** werden die unterstützten Plattformen angezeigt. Hier erscheinen die Betriebssysteme und die Anzahl der unterstützten CPUS pro Betriebssystem.
- **Repositories:** Auf der Registerkarte **Eigenschaften** werden die lizenzierten Repositories angezeigt. Hier erscheint die maximale Anzahl der lizenzierten Repositories.
- **Zugewiesene Dienste:** Zeigen Sie Anwendungsdienste an, die der Lizenz auf der Registerkarte **Zugewiesene Dienste** zugeordnet sind.
- **PowerCenter-Optionen:** Auf der Registerkarte **Optionen** werden die lizenzierten Repositories angezeigt. Zeigt alle lizenzierten PowerCenter-Optionen an, z. B. Sitzung auf Gitter, hohe Verfügbarkeit und Pushdown-Optimierung.
- **Verbindungen:** Auf der Registerkarte **Optionen** werden die lizenzierten Verbindungen angezeigt. Es erscheinen alle lizenzierten Verbindungen. Die Lizenz ermöglicht es Ihnen, Verbindungen wie DB2 und Oracle-Datenbankverbindungen zu nutzen.
- **Metadaten austausch-Optionen:** Zeigen Sie auf der Registerkarte **Optionen** die Metadaten austausch-Optionen an. Sie können eine Liste aller lizenzierten Metadaten austausch-Optionen anzeigen, wie z. B. Metadaten austausch für den Business-Objekte Designer.

Sie können auch den Lizenzverwaltungsbericht zur Überwachung der Lizenzen abrufen.

Lizenzdetails

Mit den Lizenzdetails können Sie Informationen auf hoher Ebene über die Lizenz abrufen. Anhand dieser Lizenzinformationen können Sie die Lizenznutzung überprüfen.

Die allgemeinen Eigenschaften für die Lizenz finden Sie im Abschnitt **Lizenzdetails** auf der Registerkarte **Eigenschaften**.

Folgende Tabelle beschreibt die allgemeinen Eigenschaften einer Lizenz.

Eigenschaft	Beschreibung
Name	Name der Lizenz.
Beschreibung	Beschreibung der Lizenz.
Speicherort	Pfad zur Lizenz im Navigator.
Edition	PowerCenter Advanced Edition
Lizenzversion	Version der Lizenz.
Herausgegeben von	Vertragshändler des Produkts.
Ausgestellt am	Datum der Lizenzvergabe an den Kunden.
Läuft ab am	Datum, an dem die Lizenz erlischt
Gültigkeitszeitraum	Gültigkeitszeitraum der Lizenz

Eigenschaft	Beschreibung
Seriennummer	Die Seriennummer der Lizenz. Die Seriennummer kennzeichnet den Kunden oder das Projekt. Bei mehreren PowerCenter-Installationen hat jedes Projekt eine separate Seriennummer. Der Original- und der inkrementelle Schlüssel einer Lizenz haben dieselbe Seriennummer.
Bereitstellungsebene	Ebene der Bereitstellung. Die Werte sind "Entwicklung" und "Produktion."

Mit den Lizenz-Ereignisprotokollen können Sie unter anderem zusammenfassende Prüfungsberichte anzeigen. Zum Anzeigen der Logs für die Lizenzereignisse benötigen Sie die Domänenberechtigung.

Unterstützte Plattformen

Sie weisen jedem Dienst eine Lizenz zu. Der Dienst kann auf jedem Betriebssystem ausgeführt werden, das die Lizenz unterstützt. Eine Produktlizenz kann mehrere Betriebssystemplattformen unterstützen.

Die unterstützten Plattformen einer Lizenz werden im Abschnitt "Unterstützte Plattformen" der Registerkarte **Eigenschaften** angezeigt.

Die folgende Tabelle beschreibt die Eigenschaften für die unterstützten Plattformen einer Lizenz:

Eigenschaft	Beschreibung
Beschreibung	Name des unterstützten Betriebssystems.
Logische CPUs	Anzahl der CPUs, die im auf dem Betriebssystem ausgeführt werden können.
Ausgestellt am	Datum, an dem die Lizenz ausgegeben wurde.
Läuft ab	Datum, an dem die Lizenz abläuft.

Repositorys

Die maximale Anzahl aktiver Repositorys für die Lizenz erscheinen im Abschnitt Repository der Registerkarte Eigenschaften.

Die folgende Tabelle beschreibt die Repository-Eigenschaften für eine Lizenz:

Eigenschaft	Beschreibung
Beschreibung	Name des Repository
Instanzen	Anzahl der Repository-Instanzen, die auf dem Betriebssystem ausgeführt werden.
Ausgestellt am	Datum, an dem die Lizenz für diese Option ausgestellt wurde.
Läuft ab	Datum, an dem die Lizenz für diese Option abläuft.

Dienstoptionen

Die Lizenz bietet Ihnen die Möglichkeit, die Optionen des Informatica-Dienstes, wie zum Beispiel die Datenbereinigung, Datenföderation und die Pushdown-Optimierung zu nutzen.

Die Optionen für die Lizenz werden im Abschnitt PowerCenter-Optionen auf der Registerkarte **Optionen** angezeigt.

Verbindungen

Die Lizenz ermöglicht es Ihnen, Verbindungen wie DB2 und Oracle-Datenbankverbindungen zu nutzen. Die Lizenz ermöglicht Ihnen auch, Verbindungen für PowerExchange-Adapter (z. B. PowerExchange for Facebook) zu verwenden.

Die Verbindungen für die Lizenz erscheinen im Abschnitt Verbindungen der Registerkarte **Optionen**.

Metadaten austausch-Optionen

Die Lizenz bietet die Möglichkeit, Optionen für den Austausch von Metadaten zu wählen, z. B. den Metadaten austausch für den Business-Objekte Designer und für Mikrostrategien.

Die Optionen für den Austausch von Metadaten für die Lizenz erscheinen im Abschnitt Metadaten austausch-Optionen auf der Registerkarte **Optionen**.

KAPITEL 13

Überwachung

Dieses Kapitel umfasst die folgenden Themen:

- [Überwachen - Übersicht, 256](#)
- [Konfigurieren der Überwachung, 257](#)
- [Optimieren der Überwachungsleistung, 260](#)
- [Übersichtsstatistik, 261](#)
- [Data Integration Services überwachen , 262](#)
- [Überwachen von Ad-hoc-Jobs, 263](#)
- [Überwachen von Anwendungen, 269](#)
- [Überwachen bereitgestellter Zuordnungsjobs, 269](#)
- [Logische Datenobjekte überwachen, 272](#)
- [SQL-Datendienste überwachen, 273](#)
- [Web-Dienste überwachen, 276](#)
- [Überwachen von Arbeitsabläufen, 278](#)
- [Jobstatus nach dem Neustart oder Failover des Anwendungsdiensts, 286](#)
- [Überwachen eines Ordners von Objekten, 287](#)

Überwachen - Übersicht

In Informatica Administrator können Sie Statistiken für Datenintegrationsdienstjobs auf der Registerkarte **Überwachen** überwachen.

Nachdem Sie das Überwachungsmodellrepository auf Domänenebene konfiguriert haben, können Sie die Überwachungsstatistik im Administrator Tool anzeigen. Auf der Registerkarte **Überwachen** werden aktuelle und historische Informationen zu mehreren Datenintegrationsdienst- und Integrationsobjekten angezeigt. In der Ansicht **Übersichtsstatistik** können Sie grafische Übersichten zum Objektstatus und zur Objektverteilung für mehrere Datenintegrationsdienste anzeigen. Zudem können Sie sich Diagramme zur Speicher- und CPU-Nutzung des Datenintegrationsdiensts für die Ausführung der Objekte ansehen. In der Ansicht **Ausführungsstatistiken** können Sie Eigenschaften, Laufzeitstatistiken und Laufzeitberichte für Integrationsobjekte anzeigen.

Sie können die folgenden Objekte überwachen:

- Ad-hoc-Jobs
- Anwendungen

- Logische Datenobjekte
- SQL-Datendienste
- Webdienste
- Arbeitsabläufe

Bei der Überwachung handelt es sich um eine Domänenfunktion, die der Dienstmanager ausführt. Der Dienstmanager speichert die Überwachungskonfiguration im Überwachungsmodellrepository. Der Dienstmanager sorgt auch für das Beibehalten, Aktualisieren, Abrufen und Veröffentlichen von Laufzeitstatistiken für Integrationsobjekte im Überwachungsmodellrepository.

Sie können auch in den folgenden Tools auf die Überwachung zugreifen:

Informatica Monitoring Tool

Das Monitoring Tool ist eine direkte Verknüpfung mit der Registerkarte **Überwachen** im Administrator Tool. Das Monitoring Tool ist nützlich, wenn Sie keinen Zugriff auf andere Funktionen des Administrator Tools benötigen. Sie müssen über mindestens eine Überwachungsberechtigung verfügen, um auf das Monitoring Tool zugreifen zu können. Sie können über die folgende URL auf das Monitoring Tool zugreifen:

```
http://<Administrator tool host><Administrator tool port>/monitoring/
```

Analyst Tool

Sie können Objekte auf der Registerkarte **Jobstatus** im Analyst Tool überwachen. Die Registerkarte **Jobstatus** zeigt den Status der Analyst Tool-Jobs, wie Profil-Jobs, Scorecard-Jobs und solcher Jobs, die Mapping-Spezifikationsergebnisse zum Ziel laden.

Developer Tool

Sie können das Monitoring Tool im Developer Tool öffnen. Wenn Sie die Überwachung im Developer Tool vornehmen, können Sie Jobs anzeigen, die Benutzer im Developer Tool ausführen. Im Monitoring Tool wird der Status von Developer Tool-Jobs wie Mapping-Jobs angezeigt.

Konfigurieren der Überwachung

Sie können den Überwachungsmodellrepository-Dienst auf Domänenebene konfigurieren. Nachdem Sie die Parameter der Überwachungskonfiguration konfiguriert haben, werden auf der Registerkarte „Überwachen“ die Statistiken und Berichte zu den Objekten in der Domäne angezeigt. Statistiken und Berichte werden auf der Registerkarte **Verwalten** in der Ansicht **Historie** und auf der Registerkarte **Überwachen** in den Ansichten **Übersichtsstatistik** und **Ausführungsstatistiken** angezeigt.

Der Überwachungsmodellrepository-Dienst speichert Statistiken und Berichte für die Jobs des Datenintegrationsdiensts. Zu den Statistiken gehören historische Informationen zu Objekten, die von mehreren Datenintegrationsdiensten ausgeführt werden. In den Berichten werden Schlüsselmetriken zu Integrationsobjekten angezeigt.

Falls Sie die Überwachung nicht konfigurieren, weisen einige Ansichten auf den Registerkarten **Verwalten** und **Überwachen** keinen Inhalt auf. Auch das Arbeitsablaufdiagramm ist leer und Benachrichtigungen werden nicht mehr angezeigt, wenn Sie die Seite aktualisieren.

Führen Sie die folgenden Aufgaben durch, um Überwachungsstatistiken und Berichte anzuzeigen:

1. Konfigurieren der Überwachungseinstellungen. Konfigurieren Sie ein Modellrepository als Überwachungsmodellrepository, um Laufzeitstatistiken für Objekte zu speichern, die von mehreren Datenintegrationsdiensten ausgeführt werden.
2. Konfigurieren der Ansichten „Berichte“ und „Statistiken“. Wählen Sie aus, welche Statistiken in den Ansichten **Statistiken** und **Berichte** angezeigt werden.

Hinweis: In einer Domäne mit Kerberos-Authentifizierung müssen die Benutzer über die Administratorrolle für den Überwachungsmodellrepository-Dienst verfügen, der Statistiken speichert. Wenn Benutzer nicht über die Administratorrolle verfügen, werden bestimmte Statistiken nicht angezeigt.

Schritt 1. Überwachungseinstellungen konfigurieren

Konfigurieren Sie Überwachungseinstellungen für die Domäne, wenn Sie historische Informationen über die Domäne anzeigen möchten. Beim Konfigurieren von Überwachungseinstellungen geben Sie ein Modellrepository als Überwachungsmodellrepository an, um Laufzeitstatistiken für Datenintegrationsdienst-Jobs zu speichern.

Erstellen Sie Überwachungsmodellrepository-Inhalte, bevor Sie die Überwachungseinstellungen konfigurieren. Wenn Sie den Inhalt nach dem Konfigurieren der Überwachungseinstellungen erstellen, müssen Sie den Überwachungsmodellrepository-Dienst nach dem Erstellen des Inhalts wiederherstellen.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten** > Ansicht **Dienste und Knoten**.
2. Wählen Sie die Domäne im Domänennavigator aus.
3. Klicken Sie im Abschnitt „Domäne“ auf die Ansicht **Überwachungskonfiguration**.
Die aktuelle Überwachungskonfiguration wird angezeigt.
4. Klicken Sie auf **Bearbeiten**, um die Überwachungskonfiguration zu ändern.
5. Bearbeiten Sie folgende Optionen:

Option	Beschreibung
Modellrepository-Dienst	Name des Modellrepositorys, in dem die historischen Informationen gespeichert werden. Das Modellrepository darf nicht in ein Versionsverwaltungssystem integriert sein.
Benutzername	Benutzername zum Zugriff auf den Modellrepository-Dienst. Wird nicht in Domänen angezeigt, in denen Kerberos-Authentifizierung verwendet wird.
Passwort	Passwort des Benutzernamens für den Zugriff auf den Modellrepository-Dienst. Wird nicht in Domänen angezeigt, in denen Kerberos-Authentifizierung verwendet wird.
Passwort ändern	Mit dieser Option können Sie das Passwort des Modellrepository-Diensts ändern.
Sicherheitsdomäne	Name der Sicherheitsdomäne, zu der der Benutzer des Modellrepositorys gehört.

Option	Beschreibung
Zusammengefasste historische Daten beibehalten	Anzahl der Tage, für die die Durchschnittsdaten im Modellrepository gespeichert werden. Falls die Bereinigung deaktiviert ist, werden die Daten unbegrenzt im Modellrepository gespeichert. Standardwert ist 180. Minimalwert ist 0. Maximalwert ist 366.
Detaillierte historische Daten beibehalten	Anzahl der Tage, für die die pro Minute ermittelten Daten im Modellrepository gespeichert werden. Falls die Bereinigung deaktiviert ist, werden die Daten unbegrenzt im Modellrepository gespeichert. Standardwert ist 14. Minimalwert ist 1. Maximalwert ist 14.
Statistik bereinigen alle	Intervall in Tagen, in dem der Modellrepository-Dienst die Daten bereinigt, die älter sind als die in den Optionen unter Aufbewahrung von historischen Daten konfigurierten Werte. Standard ist 1 Tag.
Tage bei	Uhrzeit, zu der der Modellrepository-Dienst Statistiken bereinigt. Standardwert ist 1:00 morgens.
Maximale Anzahl an sortierbaren Datensätzen	Maximale Anzahl der Datensätze, die auf der Registerkarte Überwachen sortiert werden können. Übersteigt die Anzahl der Datensätze auf der Registerkarte Überwachen diesen Wert, können Sie nur nach den Spalten Anfangszeitpunkt und Endzeitpunkt sortieren. Standardwert ist 3.000.
Maximale Verzögerung für Aktualisierungsbenachrichtigungen	Maximale Zeit in Sekunden, für die der Datenintegrationsdienst die Statistiken zwischenspeichert, bevor er sie dauerhaft im Modellrepository speichert und auf der Registerkarte Überwachen anzeigt. Falls der Datenintegrationsdienst unerwartet heruntergefahren wird, bevor er die Statistiken im Modellrepository gespeichert hat, gehen die Statistiken verloren. Standardwert ist 10.
Millisekunden im Feld „Datum/Uhrzeit“ einblenden	Auf der Registerkarte Überwachen werden bei Datums- und Zeitfeldern auch Millisekunden angezeigt.

6. Klicken Sie auf **OK**.

Wenn Sie die Einstellungen anwenden möchten, müssen Sie alle Datenintegrationsdienste neu starten.

Schritt 2. Konfigurieren der Ansichten „Berichte“ und „Statistiken“

Die Ansichten **Statistiken** und **Berichte** in der Ansicht **Ausführungsstatistiken** sind standardmäßig leer. Wenn Sie Statistiken und Berichte anzeigen möchten, müssen Sie die Berichts- und Statistikeinstellungen in der Domäne konfigurieren. Diese Einstellungen werden auf alle Datenintegrationsdienste in der Domäne angewendet.

Bevor Sie Statistiken und Berichte konfigurieren, müssen Sie auf der Registerkarte „Überwachungskonfiguration“ einen Überwachungsmodellrepository-Dienst angeben und diesen aktivieren.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Überwachen > Ausführungsstatistiken**.
2. Klicken Sie auf **Aktionen > Berichts- und Statistikeinstellungen**.
3. Klicken Sie im Dialogfeld **Berichts- und Statistikeinstellungen** auf die Registerkarte **Statistik**.
4. Konfigurieren Sie die für Statistiken zu verwendenden Zeiträume und wählen Sie die Häufigkeit aus, mit der die Statistiken aktualisiert werden sollen, die den verschiedenen Zeiträumen zugeordnet sind.

5. Wählen Sie in der Liste **Standardzeitraum** einen Standardzeitraum aus, der für alle Statistiken angezeigt werden soll.
6. Klicken Sie auf die Registerkarte **Berichte**
7. Konfigurieren Sie die für Berichte zu verwendenden Zeiträume und wählen Sie die Häufigkeit aus, mit der die Berichte aktualisiert werden sollen, die den verschiedenen Zeiträumen zugeordnet sind.
8. Wählen Sie in der Liste **Standardzeitraum** einen Standardzeitraum aus, der für alle Berichte angezeigt werden soll.
9. Klicken Sie auf **Berichte auswählen**.
10. Fügen Sie im Dialogfeld **Berichte hinzufügen** die auszuführenden Berichte zum Feld **Ausgewählte Berichte** hinzu.
11. Ordnen Sie die Berichte in der Reihenfolge, in der Sie sie auf der Registerkarte **Überwachen** anzeigen möchten.
12. Klicken Sie auf **OK**, um das Dialogfeld **Berichte auswählen** zu schließen.
13. Klicken Sie auf **OK** im Dialogfeld **Berichts- und Statistikeinstellungen**.

Optimieren der Überwachungsleistung

Bei der Überwachungskonfiguration in der Domäne konfigurieren Sie das Überwachungsmodellrepository, in dem die Überwachungsstatistik gespeichert wird. Zudem konfigurieren Sie die Häufigkeit, mit der der Überwachungsmodellrepository-Dienst die Statistiken bereinigt. Sie können die Einstellungen für die Repository-Datenbank und die Bereinigung so konfigurieren, dass der Ressourcenverbrauch minimiert und die Überwachungsleistung maximiert wird.

Zur Optimierung der Überwachungsleistung aktivieren Sie in der Überwachungskonfiguration die Option **Statistik bereinigen alle**. Wenn Sie die Bereinigung von Statistiken aktivieren, konfigurieren Sie die Häufigkeit, mit der der Überwachungsmodellrepository-Dienst die Daten bereinigt. Mit den Optionen unter **Beibehalten** in der Überwachungskonfiguration können Sie konfigurieren, wie lange detaillierte Daten und Zusammenfassungsdaten im Überwachungsmodellrepository gespeichert werden, bevor sie bereinigt werden.

Zur Gewährleistung einer optimalen Überwachungsleistung sollten Sie die folgenden Richtlinien berücksichtigen, wenn Sie die Domäne für die Überwachung konfigurieren:

- Erstellen Sie das Überwachungsmodellrepository, um Überwachungsdaten zu speichern. Geben Sie den Überwachungsmodellrepository-Dienst an, wenn Sie Überwachung in der Domäne konfigurieren.
- Konfigurieren Sie den Überwachungsmodellrepository-Dienst auf dem Computer, auf dem Sie die Domäne konfigurieren.
- Überprüfen Sie, ob die Überwachungsmodellrepository-Datenbank für die folgenden Eigenschaften optimiert ist:
 - Eigenschaft „Maximale Heap-Größe“
 - Eigenschaft „Größe des Java-Stacks“
 - Speichereinstellungen
 - Eigenschaft „Größe des Verbindungspools im Ruhezustand“
- Bereinigen Sie Überwachungsdaten außerhalb der Arbeitszeiten, um die Auswirkung auf andere Datenbankvorgänge zu begrenzen.
- Bereinigen Sie Überwachungsdaten täglich.

Übersichtsstatistik

Die Ansicht **Übersichtsstatistik** zeigt Informationen zu den Datenintegrationsdiensten und den Objekten an, die der Datenintegrationsdienst ausführt.

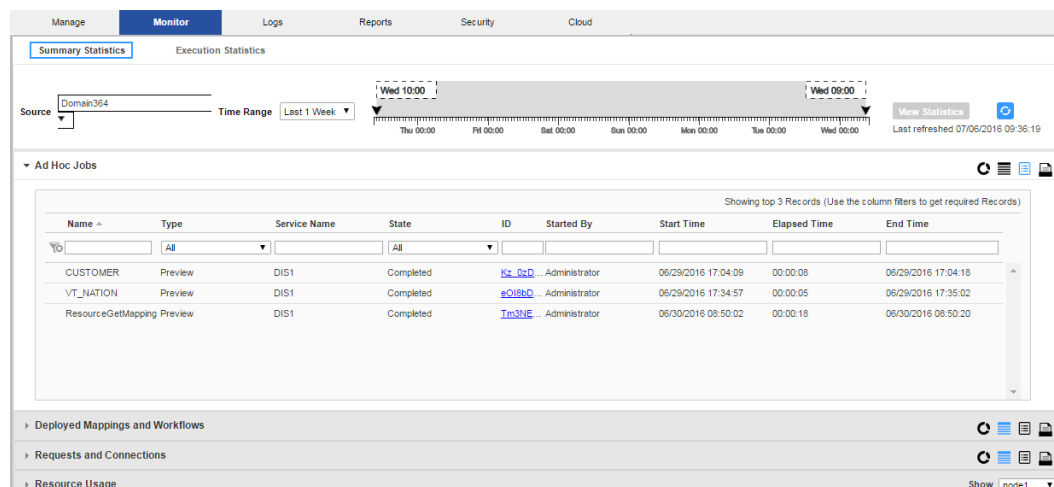
In der Ansicht **Übersichtsstatistik** können Sie Übersichten zur Objektverteilung, zum Objektstatus und zur Ressourcennutzung des Datenintegrationsdiensts für einen bestimmten Zeitraum anzeigen. Sie können Statistiken für die Domäne oder nach Datenintegrationsdienst bzw. Anwendung anzeigen.

Sie können eine Statistik zu folgenden Objekten anzeigen:

- Ad-hoc-Jobs. Jobs, die Benutzer im Developer Tool oder im Analyst Tool ausgeführt haben.
- Bereitgestellte Zuordnungen und Arbeitsabläufe. Mappings und Arbeitsabläufe, die in einer Anwendung bereitgestellt werden.
- Anfragen und Verbindungen. Bereitgestellte SQL-Datendienste und Webdienste.
- Ressourcennutzung. CPU-Nutzung und Speichernutzung der Datenintegrationsdienst-Prozesse, die in der Domäne oder auf einem Knoten in der Domäne ausgeführt werden.

Sie können beispielsweise alle Jobs in der Domäne anzeigen, bei denen in den letzten acht Stunden ein Failover stattgefunden hat. Sie können die Ressourcennutzung für diesen Zeitraum prüfen, um festzustellen, ob die Jobs aufgrund von Ressourcenproblemen auf dem Knoten fehlgeschlagen sind.

Die folgende Abbildung zeigt die Ansicht **Übersichtsstatistik** mit einer Liste der Ad-hoc-Jobs im Bereich **Details**:



Wenn Sie eine Quelle und einen Zeitbereich auswählen, steht Ihnen für die Anzeige der Daten eine der folgenden Optionen zur Verfügung:

- Grafische Verteilung. Zeigt Ring- und Liniendiagramme an, die die Objektverteilung und Ressourcennutzung für eine Zeitspanne anzeigen. Die Ringdiagramme zeigen Verteilungen von Objekten nach Status, Typ und nach Datenintegrationsdienst an, von dem sie ausgeführt werden. Mit den Liniendiagrammen können Sie die Ressourcennutzung für den Datenintegrationsdienst, der die Jobs ausgeführt hat, mit der Ressourcennutzung aller Prozesse vergleichen, die in dieser Zeitspanne auf dem Knoten ausgeführt wurden.
- Tabulare Verteilung. Anzeigen aller abgeschlossenen, laufenden, abgebrochenen, beendeten und fehlgeschlagenen Jobs.

- **Details.** Anzeigen einer Liste der Jobs, Anfragen oder Verbindungen, aus denen sich die Übersichtsstatistik zusammensetzt. Sie können auf die Job-ID klicken, um den gewünschten Job in der Ansicht „Ausführungsstatistiken“ anzuzeigen.
- **Daten exportieren.** Exportieren der Detaildaten für einen spezifischen Objekttyp in eine CSV-Datei.

In der Ansicht **Übersichtsstatistik** werden Statistiken mithilfe von Daten angezeigt, die im Überwachungsmodellrepository gespeichert sind. Sie müssen auf der Registerkarte „Überwachungskonfiguration“ ein Überwachungsmodellrepository konfigurieren, bevor Sie die **Übersichtsstatistik** anzeigen können.

Anzeigen der Übersichtsstatistik

Sie können die Übersichts- und Detailinformationen zu Ad-hoc-Jobs, bereitgestellten Zuordnungen und Arbeitsabläufen, Anfragen und Verbindungen sowie zur Ressourcennutzung für Datenintegrationsdienste in der Domäne anzeigen.

1. Klicken Sie auf die Registerkarte **Überwachen**.
2. Klicken Sie auf die Ansicht **Übersichtsstatistik**.
Die Zeitleiste wird angezeigt.
3. Wählen Sie im Feld **Quelle** die Quelle aus, für die Sie Statistiken anzeigen möchten.
4. Wählen Sie im Feld **Zeitspanne** den Zeitraum aus, für den Sie Statistiken anzeigen möchten.
5. Wählen Sie optional **Benutzerdefiniert** aus, um eine benutzerdefinierte Zeitspanne anzugeben.
6. Klicken Sie auf **Statistik anzeigen**.
Die Bereiche für die Objekte und die Ressourcennutzung werden angezeigt.
7. Erweitern Sie einen Objekttyp, um die Statistik für diesen Objekttyp anzuzeigen.
8. Wählen Sie aus, ob Sie eine grafische Verteilung, eine tabulare Verteilung oder eine Detailliste der Daten anzeigen möchten. Alternativ dazu können Sie den Export einer CSV-Datei auswählen.
9. Optional können Sie im Bereich **Ressourcennutzung** die folgenden Aktionen durchführen:

Option	Beschreibung
Anzeigen	Anzeigen aller Knoten bzw. eines Knotens.
Klick auf die Lupe	Vergrößern des Diagramms.
Ziehen	Vergrößern eines Abschnitts des Diagramms.
Zoom zurücksetzen	Anzeigen des Diagramms in der Standardgröße.

Data Integration Services überwachen

Sie können Datenintegrationsdienste auf der Registerkarte **Überwachen** in der Ansicht **Ausführungsstatistiken** überwachen.

Wenn Sie im Navigator einen Datenintegrationsdienst auswählen, werden im Inhaltsbereich die folgenden Informationen angezeigt:

- **Eigenschaftenansicht**

- Ansicht **Berichte**

Eigenschaftenansicht für einen Datenintegrationsdienst

Die Ansicht **Eigenschaften** zeigt die allgemeinen Eigenschaften und die Laufzeitstatistik für Objekte, die vom ausgewählten Datenintegrationsdienst ausgeführt wurden.

Wenn Sie einen Datenintegrationsdienst im Navigator auswählen, können Sie die allgemeinen Eigenschaften und die Laufzeit-Statistik einsehen.

Allgemeine Eigenschaften für einen Datenintegrationsdienst

Sie können die allgemeine Eigenschaften einsehen, wie z. B. Name des Dienstes, Objekttyp und eine Beschreibung. Die Eigenschaft „Beibehalten der Statistik aktiviert“ gibt an, ob der Datenintegrationsdienst persistente Statistiken im Überwachungsmodellrepository speichert. Diese Option ist aktiviert, wenn Sie die globalen Einstellungen für die Domäne konfigurieren.

Außerdem können Sie Informationen zu Objekten anzeigen, die vom Datenintegrationsdienst ausgeführt werden. Um Informationen zu einem Objekt anzuzeigen, wählen Sie das Objekt im Navigator oder Inhaltsbereich aus. Je nach Objekttyp erscheinen Details zum Objekt im Inhalts- oder Detailbereich.

Statistik für einen Datenintegrationsdienst

Sie können die Laufzeitstatistik zu Objekten anzeigen, die vom Datenintegrationsdienst ausgeführt werden. Wählen Sie den Objekttyp und den Zeitraum aus, für den die Statistik angezeigt werden soll. Sie können die Statistik über Jobs, Anwendungen Verbindungen, Anfragen und Arbeitsabläufe anzeigen. Beispielsweise können Sie die Anzahl der fehlgeschlagenen, abgebrochenen und abgeschlossenen Profiling-Jobs in den letzten vier Stunden anzeigen.

Berichtsansicht für einen Data Integration Service

In der Ansicht **Berichte** werden Berichte über die vom ausgewählten Datenintegrationsdienst ausgeführten Objekte angezeigt.

Wenn Sie im Navigator der Registerkarte **Überwachen** einen Datenintegrationsdienst auswählen, werden in der Ansicht **Berichte** Berichte über Jobs angezeigt. Zum Beispiel: Sie können den Bericht "Aktivste Benutzer von Jobs" anzeigen lassen, um jene Benutzer zu ermitteln, die die meisten Jobs innerhalb eines bestimmten Zeitraums ausführen. Klicken Sie auf einen Link in einem Bericht, um weitere Details zu den Objekten, die in dem Link enthalten sind, anzuzeigen. Zum Beispiel: Wenn Sie auf die Anzahl fehlgeschlagener, bereitgestellter Mappings klicken, sehen Sie Details zu jedem bereitgestellten Mapping, das fehlgeschlagen ist.

Überwachen von Ad-hoc-Jobs

Sie können Ad-hoc-Jobs auf der Registerkarte **Überwachen** überwachen. Bei Ad-hoc-Jobs handelt es sich um Jobs, die über das Developer Tool oder das Analyst Tool ausgeführt werden.

Ein Ad-hoc-Job ist ein Vorschau-, Scorecard-, Profil-, Mapping-, Audit- oder Referenztabelleprozess, den ein Benutzer im Developer Tool oder im Analyst Tool ausführt. Wenn ein Benutzer einen Job ausführt, führt ein Datenintegrationsdienst den Jobprozess aus. Der Job wird dann auf der Registerkarte „Überwachen“ angezeigt.

Sie können im Developer Tool bis zu fünf Jobs gleichzeitig ausführen. Alle übrigen Jobs werden in die Warteschlange gestellt und bis zu ihrer Ausführung nicht auf der Registerkarte „Überwachen“ angezeigt.

Standardmäßig können Sie Jobs überwachen, die Sie ausführen. Falls Sie die entsprechende Überwachsberechtigung haben, können Sie auch Jobs anzeigen, die andere Benutzer ausführen.

Wenn Sie im Navigator der Ansicht **Ausführungsstatistiken** auf **Ad-hoc-Jobs** klicken, wird im Inhaltsbereich eine Liste der Jobs angezeigt. Der Inhaltsbereich gruppiert zugehörige Jobs basierend auf dem Jobtyp. Sie können einen Jobtyp erweitern, um die zugehörigen Jobs darunter anzuzeigen. Wenn Sie beispielsweise einen Profiljob ausführen, wandelt der Datenintegrationsdienst den Job in ein Mapping um. Das Mapping wird unter dem Profiljob im Inhaltsbereich angezeigt.

Wenn Sie im Inhaltsbereich einen Job auswählen, können Sie Protokolle und den Kontext für den Job anzeigen bzw. den Job abbrechen. Im Detailbereich können Sie auch die Eigenschaften für den Job anzeigen. Abhängig vom Jobtyp werden im Detailbereich allgemeine Eigenschaften, Mapping-Eigenschaften oder Statistiken angezeigt.

Wenn Sie im Navigator der Ansicht „Ausführungsstatistiken“ auf Ad-hoc-Jobs klicken, wird im Inhaltsbereich eine Liste der Jobs angezeigt. Der Inhaltsbereich gruppiert zugehörige Jobs basierend auf dem Jobtyp. Sie können einen Jobtyp erweitern, um die zugehörigen Jobs darunter anzuzeigen.

In der folgenden Liste werden die Eigenschafts- und Statistiktypen beschrieben, die im Detailbereich angezeigt werden können:

Eigenschaften

Zeigt die allgemeinen Eigenschaften zum ausgewählten Job an, z. B. den Namen, den Jobtyp, den Benutzer, der den Job ausgeführt hat, sowie den Anfangszeitpunkt des Jobs. Wenn der Job in einem Gitter ausgeführt wurde, wird im Detailbereich der Knoten angezeigt, auf dem der Job ausgeführt wurde.

Mapping-Eigenschaften

Sie können Zuordnungseigenschaften anzeigen, wenn Sie einen Profil- oder Scorecard-Job im Inhaltsbereich auswählen. Diese Jobs haben ein dazugehöriges Mapping. Sie können die Mapping-Eigenschaften anzeigen, z. B. die Anfrage-ID, den Mapping-Namen und den Namen der Protokolldatei. Außerdem können Sie Durchsatz- und Ressourcennutzungsstatistiken für die zugeordneten Mappings anzeigen.

Blaze-Ausführungsplan

Sie können einen Blaze-Ausführungsplan anzeigen, wenn Sie eine Zuordnung mit der Blaze-Engine in der Hadoop-Umgebung ausführen. Im Blaze-Ausführungsplan werden das Blaze-Engine-Skript, das der Datenintegrationsdienst basierend auf der Zuordnungslogik generiert, die eindeutige ID für das Skript und die Aufgaben angezeigt, von denen das Skript abhängt.

Übersichtsstatistik

Sie können die Übersichtsstatistik bei der Auswahl eines Ad-hoc-Zuordnungs-Jobs, eines bereitgestellten Zuordnungs-Jobs oder eines Zuordnungsobjekts in einem Arbeitsablauf im Inhaltsbereich anzeigen. In der Ansicht **Übersichtsstatistik** werden Durchsatz- und Ressourcennutzungsstatistiken für die Jobausführung angezeigt.

Die folgende Abbildung zeigt die Ansicht **Übersichtsstatistik** für einen Mapping-Job:

MappingLookup							Properties	Summary Statistics	Detailed Statistics
▼ Throughput									
Source	Rows	Average Rows/Sec	Bytes	Average Bytes/Sec	First Row Accessed	Dropped Rows			
Read_CUSTOMER_DE...	4001	4001	392098	392098	09/04/2015 12:30:17	0			
Target	Rows	Average Rows/Sec	Bytes	Average Bytes/Sec	Rejected Rows				
Write_CUSTOMER_DETAILS...	4001	4001	424106	424106	0				
Write_Flat_File_Data_Object	4001	4001	16004	16004	0				
▼ Resource Usage									
Executing Node			node_715						
Average CPU Usage			0 %						
Average Memory Usage			53 MB						

Sie können die Übersichtsstatistik für die Quelle oder das Ziel auch auf der Registerkarte **Übersichtsstatistik** anzeigen, wie z. B. verarbeitete Zeilen und Byte.

Hinweis: Nur die **Anzahl der verarbeiteten Zeilen** wird in der Übersichtsstatistik für die Hive-Quelle und das Hive-Ziel angezeigt. Die restlichen Eigenschaftswerte werden als 0 oder N/V für die Hive-Quelle oder das Hive-Ziel angezeigt.

Detaillierte Statistiken

Sie können detaillierte Statistiken für einen Ad-hoc-Zuordnungs-Job, einen bereitgestellten Zuordnungs-Job oder ein Zuordnungsobjekt in einem Arbeitsablauf im Inhaltsbereich anzeigen. Es werden detaillierte Statistiken für Jobs angezeigt, die in separaten lokalen Prozessen länger als eine Minute ausgeführt werden. In der Ansicht **Detaillierte Statistiken** werden Diagramme der Durchsatz- und Ressourcennutzungsstatistiken für die Jobausführung angezeigt.

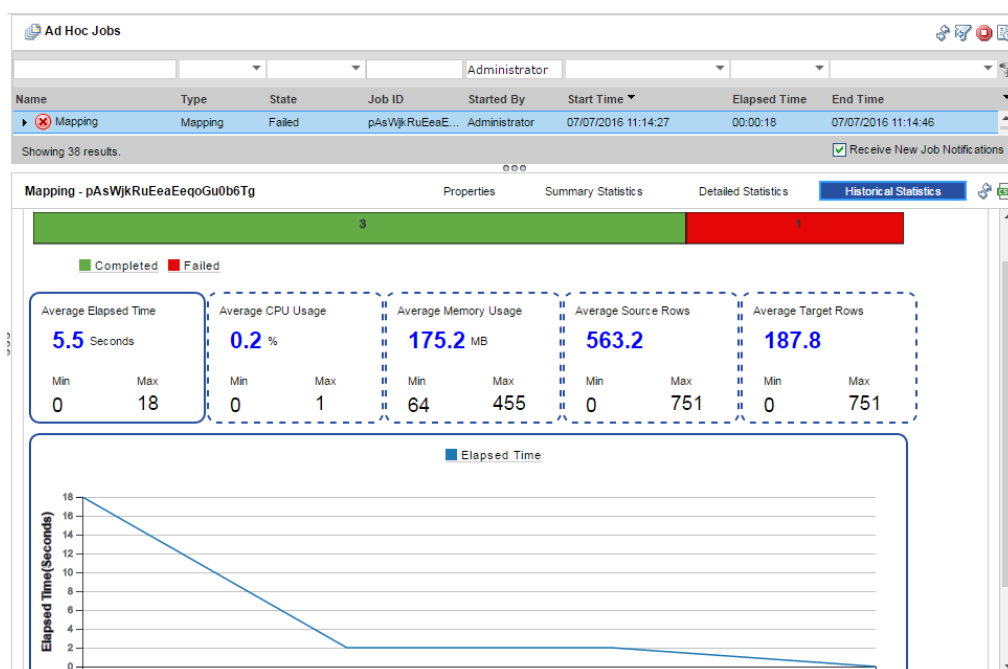
Die folgende Abbildung zeigt die Ansicht **Detaillierte Statistiken** für einen Mapping-Job in einem Arbeitsablauf:



Historische Statistik

Sie können historische Statistiken bei Auswahl eines Ad-hoc-Zuordnungs-Jobs, eines bereitgestellten Zuordnungs-Jobs oder eines Zuordnungsobjekts in einem Arbeitsablauf im Bereich **Inhalte** anzeigen. Die Ansicht **Historische Statistik** zeigt durchschnittliche Daten aus den letzten 500 Ausführungen eines bestimmten Jobs. Sie können z. B. die minimale, maximale und durchschnittliche Dauer des Zuordnungs-Jobs anzeigen. Sie können die durchschnittliche CPU-Menge anzeigen, die der Job bei Ausführung verbraucht. Sie können Durchschnittswerte für Zuordnungs-Jobs mit verschiedenen Statusangaben anzeigen, wie zum Beispiel „abgeschlossen“, „storniert“ oder „abgebrochen“. Ein Balkendiagramm zeigt die Anzahl der Jobs in jedem Status. Klicken Sie auf eine Verknüpfung unterhalb des Balkendiagramms, um die Statistik für einen bestimmten Status anzuzeigen.

Die folgende Abbildung zeigt die Ansicht **Historische Statistik** für einen Zuordnungs-Job, der drei Mal abgeschlossen wurde und ein Mal fehlgeschlagen ist:



Aggregierte Clusterprotokolle

Sie können aggregierte Clusterprotokolle für bereitgestellte Hadoop-Zuordnungen, Databricks-Zuordnungen, automatisch bereitgestellte Clusterjobs, lokale Dateien und Spark-Datenvorschaujobs basierend auf der Job-ID abrufen. Sie können eine .zip- oder tar.gz-Datei der aggregierten Clusterprotokolle für einen Job abrufen und die komprimierte aggregierte Protokolldatei in ein Zielverzeichnis schreiben. Sie können auch den `infacmd` ms-Befehl `fetchAggregatedClusterLogs` oder die REST-API verwenden, um die aggregierten Clusterprotokolle für einen Job zu erfassen.

Name	Type	State	Job ID	Started By	Start Time	Elapsed ...	End Time
▼ Mapping_f...	Mapping	Completed	D_KDU3...	Administr...	05/22/2019 15:06:23	00:01:29	05/22/2019 15:07:52
▶ MAINS...	Grid Task	Completed	D_KDU3...	Administr...	05/22/2019 15:06:23	00:01:27	05/22/2019 15:07:51
▶ Mapping_f...	Mapping	Completed	BvclHxv...	Administr...	05/22/2019 14:23:11	00:00:31	05/22/2019 14:23:42
▶ Mapping_f...	Mapping	Completed	wu9zQ3x...	Administr...	05/22/2019 14:21:17	00:00:35	05/22/2019 14:21:52
▶ Mapping_f...	Mapping	Completed	T-wXq3x...	Administr...	05/22/2019 14:18:04	00:00:48	05/22/2019 14:18:52
▶ Mapping_f...	Mapping	Canceled	BGrd-3xu...	Administr...	05/22/2019 14:15:57	00:00:01	05/22/2019 14:15:58
▶ Mapping_f...	Mapping	Completed	s7j88HxV...	Administr...	05/22/2019 11:21:54	00:03:18	05/22/2019 11:25:12

Weitere Informationen zum `infacmd` ms-Befehl `fetchAggregatedClusterLogs` finden Sie in der *Informatica 10.4.0-Befehlsreferenz*.

Anzeigen von Protokollen für einen Ad-hoc-Job

Sie können die Logs für einen Job herunterladen, um die Jobdetails zu sehen.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Überwachen**.
2. Klicken Sie auf die Ansicht für das **Ausführen von Statistiken**.
3. Erweitern Sie im Domänen-Navigator einen Datenintegrationsdienst und wählen Sie **Ad-hoc-Jobs** aus.
4. Im Inhaltsbereich wählen Sie einen Job aus.
5. Klicken Sie auf **Aktionen > Protokolle für gewähltes Objekt anzeigen**.

Es erscheint ein Dialog mit der Option zum Öffnen oder Speichern der Protokolldatei.

Abbrechen eines Ad-hoc-Jobs

Sie können einen aktuell ausgeführten Job abbrechen. Wenn ein Job zu umfangreich ist und zu viel Verarbeitungszeit benötigt, können Sie diesen wieder abbrechen.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Überwachen**.
2. Klicken Sie auf die Ansicht für das **Ausführen von Statistiken**.
3. Erweitern Sie im Domänen-Navigator einen Datenintegrationsdienst und wählen Sie **Ad-hoc-Jobs** aus.
4. Im Inhaltsbereich wählen Sie einen Job aus.
5. Klicken Sie auf **Aktionen > Ausgewählten Objekt abbrechen**.

Anzeigen der Übersichtsstatistik für einen Ad-hoc-Job

Sie können Durchsatz- und Ressourcennutzungsstatistiken für Ad-hoc-Mapping-Jobs anzeigen.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Überwachen**.
2. Klicken Sie auf die Ansicht für das **Ausführen von Statistiken**.
3. Erweitern Sie im Domänen-Navigator einen Datenintegrationsdienst und wählen Sie **Ad-hoc-Jobs** aus.
Im Inhaltsbereich wird eine Liste der Jobs angezeigt.
4. Im Inhaltsbereich wählen Sie einen Job aus.

Im Detailbereich werden die Eigenschaften für den Job angezeigt.

5. Klicken Sie im Detailbereich auf die Ansicht **Übersichtsstatistik**.

In der Ansicht **Übersichtsstatistik** werden Durchsatz- und Ressourcennutzungsstatistiken für die Quelle und das Ziel angezeigt.

Optional können Sie die Statistiken in auf- oder absteigender Reihenfolge sortieren. Klicken Sie auf einen Spaltenkopf, um die Spalte in aufsteigender Reihenfolge zu sortieren. Klicken Sie erneut auf den Spaltenkopf, um die Spalte in absteigender Reihenfolge zu sortieren.

Anzeigen von detaillierten Statistiken für einen Ad-hoc-Job

Sie können Diagramme zum Durchsatz und zur Ressourcennutzung für Ad-hoc-Mapping-Jobs anzeigen, die in separaten lokalen Prozessen ausgeführt werden. Es werden detaillierte Statistiken für Jobs angezeigt, die länger als eine Minute ausgeführt werden.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Überwachen**.
2. Klicken Sie auf die Ansicht für das **Ausführen von Statistiken**.
3. Erweitern Sie im Domänen-Navigator einen Datenintegrationsdienst und wählen Sie **Ad-hoc-Jobs** aus.
Im Inhaltsbereich wird eine Liste der Jobs angezeigt.
4. Im Inhaltsbereich wählen Sie einen Job aus.
Im Detailbereich werden die Eigenschaften für den Job angezeigt.
5. Klicken Sie im Detailbereich auf die Ansicht **Detaillierte Statistiken**.

In der Ansicht **Detaillierte Statistiken** werden das Diagramm für den Durchsatz und die Diagramme für die Ressourcennutzung angezeigt.

Optional können Sie folgende Aufgaben in der Ansicht **Detaillierte Statistiken** durchführen:

Aufgabe	Beschreibung
Grafik vergrößern	Bewegen Sie den Cursor über die Grafik und klicken Sie dann auf das Lupensymbol.
Einen Abschnitt einer vergrößerten Grafik vergrößern	Ziehen Sie den Cursor, um einen zu vergrößernden Bereich auszuwählen.
Zwischen Zeilen und Byte in der Durchsatzgrafik wechseln	Klicken Sie auf die Option „Byte“ oder auf die Option „Zeilen“.
Statistiken auswählen, die in der Durchsatzgrafik dargestellt werden sollen	Wählen Sie im Feld „Durchsatz“ die Quellen und Ziele aus, die angezeigt werden sollen.

Überwachen von Mapping-Audits

Wenn Sie ein Data Engineering-Mapping kontrollieren, können Sie den Überwachungsjob als Ad-hoc-Job überwachen.

Überwachungsjobs werden mit dem Typ *Audit-Mapping* aufgelistet.

Wenn eine Überwachungskonfiguration sowohl Regeln enthält, die vor dem Mapping ausgeführt werden, als auch Regeln, die nach dem Mapping ausgeführt werden, werden separate Überwachungsjobs für die Jobs vor und nach dem Mapping ausgeführt.

Überwachen von Anwendungen

Sie können Anwendungen auf der Registerkarte **Überwachen** überwachen.

Wenn Sie im Navigator der Ansicht **Ausführungsstatistiken** eine Anwendung auswählen, werden im Inhaltsbereich die folgenden Ansichten angezeigt:

- Ansicht **Eigenschaften**
- Ansicht **Berichte**

Sie können eine Anwendung im Navigator erweitern, um die Anwendungskomponenten zu überwachen.

Eigenschaftenansicht für eine Anwendung

Die Ansicht **Eigenschaften** zeigt allgemeine Informationen und Laufzeit-Statistiken zu den einzelnen Anwendungen und den Objekten in einer Anwendung. Anwendungen können bereitgestellte Mapping-Jobs, logische Datenobjekte, SQL-Datendienste, Webdienste und Arbeitsabläufe enthalten.

Wenn Sie eine Anwendung im Navigator der Ansicht **Ausführungsstatistiken** auswählen, können Sie allgemeine Eigenschaften und Laufzeitstatistiken einsehen.

Allgemeine Eigenschaften

Sie können die allgemeine Eigenschaften einsehen, wie z. B. Name und Beschreibung der Anwendung. Außerdem können Sie weitere Informationen zu den Objekten in einer Anwendung anzeigen. Um Informationen zu einem Objekt anzuzeigen, wählen Sie den Ordner im Navigator und das Objekt im Inhaltsbereich aus. Die Details zu dem Objekt erscheinen im Detailbereich.

Statistiken

Sie können Laufzeit-Statistiken über eine Anwendung und über die mit der Anwendung verknüpften Jobs, Verbindungen, Anfragen und Arbeitsabläufe anzeigen. Beispielsweise können Sie die Anzahl der aktivierten und deaktivierten Anwendungen, die Anzahl der abgebrochenen Verbindungen und die Anzahl der abgeschlossenen, fehlgeschlagenen und abgebrochenen Jobs und Arbeitsabläufe anzeigen.

Berichtsansicht einer Anwendung

Die Ansicht **Berichte** zeigt Überwachungsberichte zu der ausgewählten Anwendung an.

Wenn Sie im Navigator der Ansicht **Ausführungsstatistiken** eine Anwendung auswählen, werden in der Ansicht **Berichte** Berichte zu den Anwendungskomponenten angezeigt.

Überwachen bereitgestellter Zuordnungsjobs

Sie können bereitgestellte Mapping-Jobs auf der Registerkarte **Überwachen** in der Ansicht **Ausführungsstatistiken** oder im Monitoring Tool überwachen.

Sie können Informationen zu bereitgestellten Mapping-Jobs in einer Anwendung anzeigen.

Ein bereitgestelltes Mapping kann an folgenden Orten überwacht werden:

- **Monitoring tool.** Klicken Sie im Developer Tool in der Ansicht „Fortschritt“ auf die Schaltfläche **Menü** und wählen Sie **Jobs überwachen** aus. Wählen Sie den Datenintegrationsdienst aus, der das Mapping ausführt, und klicken Sie auf **OK**. Das Monitoring Tool wird geöffnet. Erweitern Sie im Navigator eine Anwendung und wählen Sie den Ordner **Bereitgestellte Zuordnungs-Jobs** aus. Im Inhaltsbereich wird eine Liste der bereitgestellten Mapping-Jobs angezeigt.
Sie können die Mapping-Ausführungsstatistiken im Monitoring Tool anzeigen. Der REST Operations Hub erzeugt Statistiken basierend auf der API-Konfiguration.
- **Administrator tool.** Erweitern Sie im Navigator eine Anwendung und wählen Sie den Ordner **Bereitgestellte Zuordnungs-Jobs** aus. Im Inhaltsbereich wird eine Liste der bereitgestellten Mapping-Jobs angezeigt.

Im Inhaltsbereich werden Eigenschaften zu jedem bereitgestellten Mapping-Job angezeigt, wie Job-ID, Mapping-Name, Jobstatus und Anfangszeitpunkt des Jobs. Wenn Sie den Job in einem Gitter ausführen, wird im Inhaltsbereich auch der Knoten angezeigt, auf dem der Datenintegrationsdienst läuft, der den Prozess ausführt.

Wählen Sie im Inhaltsbereich einen bereitgestellten Mapping-Job aus, um die Protokolle für den Job anzuzeigen, den Job zu wiederholen oder abubrechen bzw. Statistiken zu dem Job anzuzeigen. Sie können Statistiken zum Durchsatz und zur Ressourcennutzung für die Jobausführung anzeigen.

Logs für einen bereitgestellten Mapping-Job anzeigen

Sie können die Logs für einen bereitgestellten Mapping-Job herunterladen, um die Jobdetails zu sehen.

Hinweis: Die Protokollinhalte für einen bereitgestellten Mapping-Job hängen von der Konfiguration des Datenintegrationsdiensts ab. Weitere Informationen zu Protokollen für den Fall, dass ein Datenintegrationsdienst-Gitter zur Ausführung von Jobs in separaten Remoteprozessen konfiguriert wurde, finden Sie im *Informatica Application Service-Handbuch*.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Überwachen**.
2. Klicken Sie auf die Ansicht für das **Ausführen von Statistiken**.
3. Erweitern Sie im Domänen-Navigator einen Datenintegrationsdienst.
4. Erweitern Sie eine Anwendung und wählen Sie **Bereitgestellte Mapping-Jobs** aus.
Eine Liste der Mapping-Jobs erscheint im Inhaltsbereich.
5. Wählen Sie einen Mapping-Job aus.
6. Klicken Sie auf **Aktionen > Protokolle für gewähltes Objekt anzeigen**.
Es erscheint ein Dialog mit der Option zum Öffnen oder Speichern der Protokolldatei.

Bereitgestellten Zuordnungsjob erneut ausgeben

Sie können einen bereitgestellten Zuordnungsjob erneut ausgeben, wenn der Job fehlgeschlagen ist. Wenn Sie einen bereitgestellten Zuordnungsjob erneut ausgeben, führt der Datenintegrationsdienst den Job wieder aus.

1. Klicken Sie auf die Ansicht für das **Ausführen von Statistiken**.
2. Erweitern Sie im Domänen-Navigator einen Datenintegrationsdienst.
3. Erweitern Sie eine Anwendung und wählen Sie **Bereitgestellte Zuordnungsjobs** aus.
Im Inhaltsbereich erscheint eine Liste der bereitgestellten Zuordnungsjobs.
4. Wählen Sie einen bereitgestellten Zuordnungsjob aus.
5. Klicken Sie auf **Aktionen > Ausgewähltes Objekt erneut ausgeben**.

Bereitgestellten Mapping-Job abbrechen

Sie können einen bereitgestellten Mapping-Job abbrechen. Wenn ein bereitgestellter Mapping-Job zu umfangreich ist und zu viel Verarbeitungszeit benötigt, können Sie diesen wieder abbrechen.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Überwachen**.
2. Klicken Sie auf die Ansicht für das **Ausführen von Statistiken**.
3. Erweitern Sie im Domänen-Navigator einen Datenintegrationsdienst.
4. Erweitern Sie eine Anwendung und wählen Sie **Bereitgestellte Mapping-Jobs** aus.
Im Inhaltsbereich erscheint eine Liste der bereitgestellten Mapping-Jobs.
5. Wählen Sie einen bereitgestellten Mapping-Job aus.
6. Klicken Sie auf **Aktionen > Ausgewählten Job abbrechen**.

Anzeigen der Übersichtsstatistik für einen bereitgestellten Mapping-Job

Sie können Durchsatz- und Ressourcennutzungsstatistiken für bereitgestellte Mapping-Jobs anzeigen.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Überwachen**.
2. Klicken Sie auf die Ansicht für das **Ausführen von Statistiken**.
3. Erweitern Sie im Domänen-Navigator einen Datenintegrationsdienst.
4. Erweitern Sie eine Anwendung und wählen Sie **Bereitgestellte Mapping-Jobs** aus.
Im Inhaltsbereich wird eine Liste der Mapping-Jobs angezeigt.
5. Wählen Sie einen Mapping-Job aus.
Im Detailbereich werden die Eigenschaften für den Mapping-Job angezeigt.
6. Klicken Sie auf die Ansicht **Übersichtsstatistik**.
In der Ansicht **Übersichtsstatistik** werden Durchsatz- und Ressourcennutzungsstatistiken für die Quelle und das Ziel angezeigt.

Optional können Sie die Statistiken in auf- oder absteigender Reihenfolge sortieren. Klicken Sie auf einen Spaltenkopf, um die Spalte in aufsteigender Reihenfolge zu sortieren. Klicken Sie erneut auf den Spaltenkopf, um die Spalte in absteigender Reihenfolge zu sortieren.

Anzeigen von detaillierten Statistiken für einen bereitgestellten Mapping-Job

Sie können Diagramme zum Durchsatz und zur Ressourcennutzung für bereitgestellte Mapping-Jobs anzeigen, die in separaten lokalen Prozessen ausgeführt werden. Es werden detaillierte Statistiken für Jobs angezeigt, die länger als eine Minute ausgeführt werden.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Überwachen**.
2. Klicken Sie auf die Ansicht für das **Ausführen von Statistiken**.
3. Erweitern Sie im Domänen-Navigator einen Datenintegrationsdienst.
4. Erweitern Sie eine Anwendung und wählen Sie **Bereitgestellte Mapping-Jobs** aus.
Im Inhaltsbereich wird eine Liste der Mapping-Jobs angezeigt.
5. Wählen Sie einen Mapping-Job aus.
Im Detailbereich werden die Eigenschaften für den Mapping-Job angezeigt.

6. Klicken Sie auf die Ansicht **Detaillierte Statistiken**.

In der Ansicht **Detaillierte Statistiken** werden das Diagramm für den Durchsatz und die Diagramme für die Ressourcennutzung angezeigt.

Optional können Sie folgende Aufgaben in der Ansicht **Detaillierte Statistiken** durchführen:

Aufgabe	Beschreibung
Grafik vergrößern	Bewegen Sie den Cursor über die Grafik und klicken Sie dann auf das Lupensymbol.
Einen Abschnitt einer vergrößerten Grafik vergrößern	Ziehen Sie den Cursor, um einen zu vergrößernden Bereich auszuwählen.
Zwischen Zeilen und Byte in der Durchsatzgrafik wechseln	Klicken Sie auf die Option „Byte“ oder auf die Option „Zeilen“.
Statistiken auswählen, die in der Durchsatzgrafik dargestellt werden sollen	Wählen Sie im Feld „Durchsatz“ die Quellen und Ziele aus, die angezeigt werden sollen.

Anzeigen der Job-Statistiken für bereitgestellte Mappings mit dem REST Operations Hub-Dienst

Mit der REST-Funktionalität können Sie Überwachungsstatistiken für bereitgestellte Mapping-Jobs abrufen.

Logische Datenobjekte überwachen

Sie können logische Datenobjekte auf der Registerkarte **Überwachen** in der Ansicht **Ausführungsstatistiken** oder im Monitoring Tool überwachen.

Sie können Informationen über logische Datenobjekte anzeigen, die in einer Anwendung enthalten sind. Zum Überwachen eines logischen Datenobjekts erweitern Sie im Navigator einen Datenintegrationsdienst.

Erweitern Sie eine Anwendung und wählen Sie dann den Ordner **Logische Datenobjekte** aus. Im Inhaltsbereich wird eine Liste der logischen Datenobjekte eingeblendet. Im Inhaltsbereich erscheinen die Eigenschaften der logischen Datenobjekte.

Wählen Sie ein logisches Datenobjekt im Inhaltsbereich aus, um die Logs für ein Datenobjekt herunterzuladen.

Wenn Sie im Inhaltsbereich ein logisches Datenobjekt auswählen, werden im Detailbereich die folgenden Ansichten angezeigt:

- Ansicht **Eigenschaften**
- **Cache-Aktualisierungsdurchläufe**

Eigenschaftenansicht für ein logisches Datenobjekt

Die Ansicht **Eigenschaften** zeigt allgemeine Informationen und Laufzeitstatistiken zum gewählten Objekt an.

Sie können Eigenschaften wie den Datenobjektnamen, das logische Datenobjektmodell, den Ordnerpfad, Cache-Status und Informationen zur letzten Cache-Aktualisierung anzeigen.

Ansicht "Cache-Aktualisierungsdurchläufe" für ein logisches Datenobjekt

Die Ansicht **Cache-Aktualisierungsdurchläufe** zeigt Details zur Cache-Aktualisierung des ausgewählten logischen Datenobjekts.

Die Ansicht **Cache-Aktualisierungsdurchläufe** zeigt Details zur Cache-Aktualisierung wie zum Beispiel die Cache-Durchlauf-ID, die Anzahl der Cache-Anfragen und die Anzahl der Zeilen.

Logs für Datenobjekt-Cache-Aktualisierungsdurchläufe

Sie können die Logs für Datenobjekt-Cache-Aktualisierungsdurchläufe herunterladen, um die Cache-Aktualisierungsdetails anzuzeigen.

1. Klicken Sie auf die Ansicht **Ausführungsstatistiken**.
2. Erweitern Sie im Domänen-Navigator einen Datenintegrationsdienst.
3. Erweitern Sie eine Anwendung und wählen Sie **Logische Datenobjekte** aus.
Im Inhaltsbereich erscheint eine Liste der logischen Datenobjekte.
4. Wählen Sie ein logisches Datenobjekt aus.
Die Details zu dem gewählten Datenobjekt erscheinen im Detailbereich.
5. Wählen Sie die Ansicht **Cache-Aktualisierungsdurchläufe** aus.
6. Klicken Sie auf **Protokolle für ausgewähltes Objekt anzeigen**.

SQL-Datendienste überwachen

Sie können SQL-Datendienste auf der Registerkarte **Überwachen** in der Ansicht **Ausführungsstatistiken** überwachen. Ein SQL-Datendienst ist eine virtuelle Datenbank, die Sie abfragen können. Sie enthält ein Schema und andere Objekte, die die zugrunde liegenden physischen Daten repräsentieren.

Sie können Informationen zu SQL-Datendiensten in einer Anwendung anzeigen. Zum Überwachen eines SQL-Datendiensts erweitern Sie im Navigator eine Anwendung und wählen den Ordner **SQL-Datendienste** aus. Im Inhaltsbereich wird eine Liste der SQL-Datendienste eingeblendet. Der Inhaltsbereich zeigt die Eigenschaften zu den einzelnen SQL-Datendiensten an, wie z. B. Name, Beschreibung und Status.

Wenn Sie im Inhaltsbereich einen SQL-Datendienst auswählen, werden im Inhaltsbereich die folgenden Ansichten angezeigt:

- Ansicht **Eigenschaften**
- Ansicht **Verbindungen**
- Ansicht **Anfragen**
- **Virtuelle Tabellen**
- Ansicht **Berichte**

Eigenschaftenansicht für einen SQL-Datendienst

Die Ansicht **Eigenschaften** zeigt allgemeine Informationen und Laufzeitstatistiken für einen SQL-Datendienst an.

Wenn Sie einen SQL-Datendienst im Inhaltsbereich der Ansicht **Eigenschaften** auswählen, können Sie die allgemeinen Eigenschaften und die Laufzeitstatistiken anzeigen.

Allgemeine Eigenschaften für einen SQL-Datendienst

Hierzu gehören der Name des SQL-Datendienstes und die Beschreibung.

Statistiken für einen SQL-Datendienst

Sie können die Laufzeitstatistiken zu Verbindungen und Anfragen an den SQL-Datendienst anzeigen. Zu den Statistiken gehören die Anzahl der Verbindungen zum SQL-Datendienst, die Anzahl der Anfragen und die Anzahl der abgebrochenen Verbindungen.

Verbindungsansicht für einen SQL Data Service

In der Ansicht **Verbindungen** sind die Eigenschaften der Verbindungen von Drittparteien-Clients aufgelistet. Die Ansicht enthält Eigenschaften wie die Verbindungs-ID, den Verbindungsstatus, die Verbindungszeit, die abgelaufene Zeit und den Zeitpunkt der Trennung.

Beim Auswählen einer Verbindung in der Inhaltsübersicht können Sie die Verbindung abbrechen oder in die Ansicht **Eigenschaften** und die Ansicht **Anfragen** in der Maske Details gehen.

Eigenschaften-Ansicht

Die Ansicht **Eigenschaften** in der Maske Details zeigt den Benutzer, der die Verbindung nutzt, den Verbindungsstatus und den Zeitpunkt der Verbindung.

Anfragen-Ansicht

Die Ansicht **Anfragen** in der Maske Details enthält Informationen über die Anfragen für die SQL-Verbindung. Jede Verbindung kann mehr als eine Anfrage aufweisen. In jeder Ansicht sind die Eigenschaften der Anfrage eingeblendet, wie Anfrage-ID, Benutzername, Anfragestatus, Startzeit, abgelaufene Zeit und Endezeit.

Verbindung abbrechen

Sie können eine Verbindung abbrechen, um zu verhindern, dass weitere Anfragen an den SQL-Datendienst verschickt werden.

1. Klicken Sie auf die Ansicht **Ausführungsstatistiken**.
2. Erweitern Sie im Domänennavigator einen Datenintegrationsdienst.
3. Erweitern Sie eine Anwendung und wählen Sie **SQL-Datendienste** aus.
Im Inhaltsbereich werden die SQL-Datendienste in der Anwendung aufgeführt.
4. Wählen Sie einen SQL-Datendienst aus.
Im Inhaltsbereich erscheinen mehrere Ansichten des SQL-Datendienstes.
5. Klicken Sie auf die Ansicht **Verbindungen**.
Der Inhaltsbereich listet die aktiven Verbindungen zum SQL-Datendienst auf.
6. Wählen Sie eine Verbindung.
7. Klicken Sie auf **Aktionen > Ausgewählte Verbindung abbrechen**.

Anfrageansicht eines SQL-Datendienstes

Die Ansicht **Anfragen** zeigt die Eigenschaften für die Anfragen zu jeder SQL-Verbindung an.

Die Ansicht **Anfragen** zeigt die Eigenschaften für die Anfragen zu einer SQL-Verbindung an. Jede Verbindung kann mehr als eine Anfrage haben. Die Ansicht zeigt Anfrageeigenschaften wie die Anfrage-ID, die Verbindungs-ID, den Benutzernamen, den Status der Anfrage, die Startzeit, die Ausführungszeit und die Endezeit an.

Wählen Sie eine Anfrage im Inhaltsbereich aus, um zusätzliche Informationen zu der Anfrage im Detailbereich zu erhalten.

Abbrechen einer Verbindungsanfrage für SQL-Datendienst

Sie können eine Verbindungsanfrage für einen SQL-Datendienst jederzeit abbrechen. Wenn eine Verbindungsanfrage hängt oder zu viel Verarbeitungszeit benötigt, können Sie diese abbrechen.

1. Klicken Sie auf die Ansicht für das **Ausführen von Statistiken**.
2. Erweitern Sie im Domänennavigator einen Datenintegrationsdienst.
3. Erweitern Sie eine Anwendung und wählen Sie **SQL-Datendienste** aus.
Im Inhaltsbereich erscheint eine Liste der SQL-Datendienste.
4. Wählen Sie einen SQL-Datendienst aus.
5. Klicken Sie auf die Ansicht **Anfragen**.
Eine Liste der Verbindungsanfragen für den SQL-Datendienst wird angezeigt.
6. Wählen Sie eine Anfragezeile aus.
7. Klicken Sie auf **Aktionen > Abbrechen der ausgewählten Anfrage**.

Logs für eine SQL-Datendienstanfrage anzeigen

Sie können die Logs für eine SQL-Datendienstanfrage herunterladen, um die Abfragedetails zu sehen.

1. Klicken Sie auf die Ansicht für das **Ausführen von Statistiken**.
2. Erweitern Sie im Domänennavigator einen Datenintegrationsdienst.
3. Erweitern Sie eine Anwendung und wählen Sie **SQL-Datendienste** aus.
Im Inhaltsbereich erscheint eine Liste der SQL-Datendienste.
4. Wählen Sie einen SQL-Datendienst aus.
5. Klicken Sie auf die Ansicht **Anfragen**.
Eine Liste der Anfragen für den SQL-Datendienst wird angezeigt.
6. Wählen Sie eine Anfragezeile aus.
7. Klicken Sie auf **Aktionen > Logs für gewähltes Objekt anzeigen**.

Virtuelle Tabellen für einen SQL-Datendienst anzeigen

Die Ansicht **Virtuelle Tabellen** zeigt die Eigenschaften der virtuellen Tabellen im SQL-Datendienst an.

Zu den Eigenschaften für virtuelle Tabellen gehören zum Beispiel der Name und die Beschreibung. Wenn Sie im Inhaltsbereich eine virtuelle Tabelle wählen, können Sie die Ansicht **Eigenschaften** anzeigen lassen und im Detailbereich die Ansicht **Cache-Aktualisierungsdurchläufe**.

Die Eigenschaftenansicht

Die Ansicht **Eigenschaften** zeigt allgemeine Informationen und Laufzeitstatistiken zur gewählten virtuellen Tabelle an. Die allgemeinen Eigenschaften enthalten den Namen der virtuellen Tabelle und den Schemanamen. Das Überwachen von Statistiken beinhaltet die Anzahl von Anfragen, die Anzahl zwischengespeicherter Zeilen und den Zeitpunkt der letzten Cache-Aktualisierung.

Die Ansicht "Cache-Aktualisierungsdurchläufe"

Die Ansicht **Cache-Aktualisierungsdurchläufe** zeigt die Cache-Informationen für die gewählte virtuelle Tabelle an. Dazu gehören die Cache-Durchlauf-ID, die Anfragezählung, die Zeilenzählung und die Cache-Trefferquote. Die Cache-Trefferquote ist die Gesamtanzahl der Anfragen an den Cache dividiert durch die Gesamtanzahl der Anfragen für das Datenobjekt.

Logs für eine SQL-Datendienst-Tabellen-Cache anzeigen

Sie können die Logs für einen SQL-Datendienst-Tabellen-Cache herunterladen, um die Tabellen-Cache-Details zu sehen.

1. Klicken Sie auf die Ansicht für das **Ausführen von Statistiken**.
2. Erweitern Sie im Domänennavigator einen Datenintegrationsdienst.
3. Erweitern Sie eine Anwendung und wählen Sie **SQL-Datendienste** aus.
Im Inhaltsbereich erscheint eine Liste der SQL-Datendienste.
4. Wählen Sie einen SQL-Datendienst aus.
5. Klicken Sie auf die Ansicht **Virtuelle Tabellen**.
Eine Liste der virtuellen Tabellen für den SQL-Datendienst wird angezeigt.
6. Wählen Sie eine Tabellenzeile aus.
Die Details zu der gewählten Tabelle erscheinen im Detailbereich.
7. Wählen Sie die Ansicht **Cache-Aktualisierungsdurchläufe** aus.
8. Klicken Sie auf **Protokolle für ausgewähltes Objekt anzeigen**.

Berichtsansicht eines SQL-Datendienstes

Die Ansicht **Berichte** zeigt Überwachungsberichte zum ausgewählten SQL-Datendienst an.

Wenn Sie einen SQL-Datendienst überwachen, werden in der Ansicht **Berichte** Berichte über den SQL-Datendienst angezeigt. Zum Beispiel: Sie können den Bericht "Aktivste SQL-Verbindungen" anzeigen lassen, um jene SQL-Verbindungen zu ermitteln, die die meisten Verbindungsanfragen innerhalb eines bestimmten Zeitraums erhalten haben.

Web-Dienste überwachen

Sie können Webdienste auf der Registerkarte **Überwachen** in der Ansicht **Ausführungsstatistiken** überwachen. Web-Dienste sind Geschäftsfunktionen, die im Web operieren. Sie beschreiben eine Sammlung von Operationen, die durch das standardisierte XML-Messaging Zugang zu Netzwerken haben.

Sie können Informationen über Web-Dienste anzeigen, die in einer Anwendung enthalten sind. Zum Überwachen eines Webdiensts erweitern Sie im Navigator eine Anwendung und wählen den Ordner **Webdienste** aus. Im Inhaltsbereich wird eine Liste der Webdienste eingeblendet. Der Inhaltsbereich zeigt die

Eigenschaften eines jeden Web-Dienstes an, z. B. den Namen, die Beschreibung und den Status jedes Web-Dienstes.

Wenn Sie im Inhaltsbereich den Link zu einem Web-Dienst auswählen, zeigt das Inhaltsfenster die folgenden Ansichten:

- Ansicht **Eigenschaften**
- Ansicht **Berichte**
- **Ansicht Operationen**
- Ansicht **Anfragen**

Eigenschaftenansicht für einen Web-Dienst

Die Ansicht **Eigenschaften** zeigt allgemeine Informationen und Laufzeitstatistiken zum gewählten Web-Dienst an.

Wenn Sie einen Web-Dienst im Inhaltsbereich der Ansicht **Eigenschaften** auswählen, können Sie die allgemeinen Eigenschaften und die Überwachungsstatistiken anzeigen.

Allgemeine Eigenschaften für einen Web-Dienst

Zu den allgemeinen Eigenschaften eines Web-Dienstes gehören der Name und der Objekttyp.

Statistiken für einen Web-Dienst

Sie können die Laufzeitstatistiken zu den Anfragen an einen Web-Dienst innerhalb eines bestimmten Zeitraums anzeigen. Der Abschnitt **Statistiken** zeigt die Anzahl der abgeschlossenen und fehlgeschlagenen Anfragen sowie die Gesamtanzahl an.

Berichtsansicht eines Web-Dienstes

Die Ansicht **Berichte** zeigt Überwachungsberichte zum ausgewählten Web-Dienst an.

Beim Überwachen eines Webdiensts werden in der Ansicht **Berichte** Berichte über den Webdienst angezeigt. Sie können beispielsweise den Bericht „Aktivste Client-IP des Webdiensts“ anzeigen, um die IP-Adressen zu ermitteln, die die meisten Webdienstanfragen innerhalb eines bestimmten Zeitraums erhalten haben.

Ansicht „Operationen“ für einen REST- oder SOAP-Webdienst

Die Ansicht **Operationen** zeigt den Namen und die Beschreibung der einzelnen Operationen oder Ressourcen im Webdienst an. Außerdem zeigt die Ansicht auch Eigenschaften, Anfragen und Berichte zu jeder Operation.

Wenn Sie eine Web-Dienst-Operation im Inhaltsbereich auswählen, werden im Detailbereich die Ansichten **Eigenschaften**, **Anfragen** und **Berichte** angezeigt.

Eigenschaftenansicht

Die Ansicht **Eigenschaften** zeigt allgemeine Informationen und Statistiken zur ausgewählten Webdienst-Operation oder -Ressource an. Allgemeine Eigenschaften beinhalten den Namen der Operation oder Ressource und den Typ des Objekts. Die Ansicht zeigt auch Statistiken zur Web-Dienst-Operation während eines bestimmten Zeitraums. Die Statistik umfasst die Anzahl der abgeschlossenen und fehlgeschlagenen Web-Service-Anfragen sowie deren Gesamtanzahl.

Ansicht „Anfragen“

Die Ansicht **Anfragen** zeigt Eigenschaften zu den einzelnen Web-Dienst-Operationen, wie Nummer der Anfrage, Benutzernamen, Status, Startzeit, verstrichene Zeit und Endzeit. Sie können die Liste der Anfragen filtern. Außerdem können Sie Logs für die ausgewählte Web-Dienst-Anfrage anzeigen.

Ansicht „Berichte“ für einen SOAP-Webdienst

Die Ansicht **Berichte** zeigt Berichte über SOAP-Webdienst-Operationen.

Anfrageansicht eines Webdienstes

Die Ansicht **Anfragen** zeigt die Eigenschaften jeder Webdienstanfrage an, z. B. die Anfrage-ID, den Benutzernamen, Status, Startzeit, Ausführungszeit und Endezeit. Sie können diese Anfrageliste filtern.

Wenn Sie eine Webdienstanfrage im Inhaltsbereich auswählen, erscheinen die Protokolle zu der Anfrage im Detailbereich. Der Detailbereich zeigt die allgemeinen Eigenschaften und Statistiken zu der ausgewählten Webdienstanfrage an. Die Statistiken enthalten die Anzahl der abgeschlossenen und fehlgeschlagenen Anfragen sowie die Gesamtanzahl der Anfragen an den Webdienst.

Sie können auch eine Webdienstanfrage über die Ansicht **Anfragen** abbrechen. Wählen Sie zum Abbrechen einer Webdienstanfrage die Arbeitsablauf-Anfrage aus und klicken Sie im Inhaltsbereich auf **Aktionen** > **Ausgewählte Anfrage abbrechen**.

Überwachen von Arbeitsabläufen

Sie können Arbeitsabläufe auf der Registerkarte **Überwachen** in der Ansicht **Ausführungsstatistiken** überwachen.

Sie können Informationen über Arbeitsablaufinstanzen anzeigen, die über einen Arbeitsablauf in einer bereitgestellten Anwendung ausgeführt werden. Zum Überwachen eines Arbeitsablaufs erweitern Sie im Navigator eine Anwendung und wählen den Ordner **Arbeitsabläufe** aus. Im Inhaltsbereich wird eine Liste der Arbeitsablaufinstanzen angezeigt. Im Inhaltsbereich werden die Eigenschaften zu jeder Arbeitsablaufinstanz angezeigt, wie zum Beispiel Name, Status, Anfangszeitpunkt und verstrichene Zeit für jede Arbeitsablaufinstanz. Wenn die Arbeitsablaufinstanz in einem Gitter ausgeführt wurde, wird im Inhaltsbereich der Knoten angezeigt, der die einzelnen Mappings in der Ablaufinstanz ausgeführt hat.

Wählen Sie eine Arbeitsablaufinstanz im Inhaltsbereich, um die folgenden Aufgaben auszuführen:

- Anzeigen von Protokollen für die Arbeitsablaufinstanz
- Anzeigen des Kontexts der Arbeitsablaufinstanz, um andere Arbeitsablaufinstanzen anzuzeigen, die ungefähr zur gleichen Zeit wie die ausgewählte Arbeitsablaufinstanz begonnen hat.
- Abbrechen der Arbeitsablaufinstanz
- Wiederherstellen der unterbrochenen Arbeitsablaufinstanz

Erweitern Sie die Arbeitsablaufinstanz, um die Eigenschaften zu den Arbeitsablaufobjekten anzuzeigen.

Arbeitsablaufgrafik

Sie können die Details eines im Monitoring-Tool ausgeführten Arbeitsablaufs in einer Grafik anzeigen.

Nach dem Ausführen eines Arbeitsablaufs wird die Grafikanzeige des Arbeitsablaufs im Monitoring-Tool angezeigt. In der Arbeitsablaufgrafik wird die sequenzielle Ausführung der Mapping-Aufgaben im Arbeitsablauf dargestellt. In der Arbeitsablaufgrafik können Sie Fehlerpunkte in einem Arbeitsablauf sofort erkennen.

In der Arbeitsablaufgrafik werden die folgenden Details eines Arbeitsablaufs dargestellt:

- Mapping-Aufgaben im Arbeitsablauf

- Aufgabendetails
- Wiederherstellungsdetails

In der Arbeitsablaufgrafik können Sie die folgenden Aufgaben durchführen:

- Beenden eines laufenden Arbeitsablaufs
- Abbrechen eines laufenden Arbeitsablaufs
- Wiederherstellen eines fehlgeschlagenen Arbeitsablaufs
- Anzeigen der Arbeitsablaufprotokolle

Anzeigen einer Arbeitsablaufgrafik

In einer Arbeitsablaufgrafik können Sie die sequenzielle Ausführung der Zuordnungsaufgaben im Arbeitsablauf anzeigen.

1. Klicken Sie auf die Ansicht für das **Ausführen von Statistiken**.
2. Erweitern Sie im Domänennavigator eine Anwendung.
3. Wählen Sie den Ordner **Arbeitsabläufe** aus.
Eine Liste mit Arbeitsabläufen wird im Inhaltsbereich angezeigt.
4. Wählen Sie den Arbeitsablauf aus, den Sie anzeigen möchten.
5. Klicken Sie auf **Aktionen > Arbeitsablaufdiagramm anzeigen**.
Die Arbeitsablaufgrafik wird in einem neuen Fenster geöffnet.

Anzeigen von Arbeitsablaufobjekten

Wenn Sie eine Arbeitsablaufinstanz im Inhaltsbereich erweitern, können Sie die Eigenschaften der Arbeitsablaufobjekte anzeigen, wie zum Beispiel Name, Status, Anfangszeitpunkt und verstrichene Zeit für das Objekt.

Arbeitsablaufobjekte beinhalten Ereignisse, Aufgaben und Gateways. Wenn Sie Arbeitsabläufe überwachen, können Sie die in einer Arbeitsablaufinstanz ausgeführten Aufgaben überwachen. Auf der Registerkarte **Überwachen** werden keine Informationen über Ereignisse oder Gateways in der Arbeitsablaufinstanz angezeigt.

Wenn ein Ausdruck in einem bedingten Sequenzfluss als "false" bewertet wird, führt der Datenintegrationsdienst nicht das nächste Objekt oder nachfolgende Objekte in diesem Zweig aus. Auf der Registerkarte **Überwachen** werden nur Objekte aufgelistet, die in der Arbeitsablaufinstanz ausgeführt werden. Wenn eine Arbeitsablaufinstanz Objekte enthält, die nicht ausgeführt werden, kann die Instanz trotzdem erfolgreich abgeschlossen werden.

Sie können eine Aufgabe in der Inhaltskonsole erweitern, um Informationen über das Arbeitselement anzuzeigen, das von der Aufgabe ausgeführt wird. Wenn der Arbeitsablauf beispielsweise eine Zuordnungsaufgabe enthält, können Sie Statistiken zum Durchsatz und zur Ressourcennutzung für die Zuordnungsausführung anzeigen.

Anzeigen von Übersichtsstatistiken für Arbeitsablaufobjekte

Sie können Statistiken zum Durchsatz und zur Ressourcennutzung für Zuordnungsobjekte in Arbeitsabläufen anzeigen, die in separaten lokalen Prozessen ausgeführt werden.

1. Klicken Sie auf die Ansicht **Ausführungsstatistiken**.
2. Erweitern Sie im Domänennavigator einen Datenintegrationsdienst.

- Erweitern Sie eine Anwendung und wählen Sie den Ordner **Arbeitsabläufe** aus.

Eine Liste mit Arbeitsabläufen wird im Inhaltsbereich angezeigt.

- Erweitern Sie einen Arbeitsablauf, der ein Zuordnungsobjekt enthält.
- Erweitern Sie die Zuordnungsaufgabe und wählen Sie die Zuordnung aus.
- Klicken Sie im Detailbereich auf die Ansicht **Übersichtsstatistiken**.

In der Ansicht **Übersichtsstatistiken** werden Statistiken zum Durchsatz und zur Ressourcennutzung für die Quelle und das Ziel angezeigt.

Optional können Sie die Statistiken in auf- oder absteigender Reihenfolge sortieren. Klicken Sie auf einen Spaltenkopf, um die Spalte in aufsteigender Reihenfolge zu sortieren. Klicken Sie erneut auf den Spaltenkopf, um die Spalte in absteigender Reihenfolge zu sortieren.

Anzeigen detaillierter Statistiken für Arbeitsablaufobjekte

Sie können Grafiken zum Durchsatz und zur Ressourcennutzung für Zuordnungsobjekte in Arbeitsabläufen anzeigen, die in separaten lokalen Prozessen ausgeführt werden. Detaillierte Statistiken werden für Jobs angezeigt, deren Ausführung mehr als eine Minute in Anspruch nimmt.

- Klicken Sie auf die Ansicht **Ausführungsstatistiken**.
- Erweitern Sie im Domänennavigator einen Datenintegrationsdienst.
- Erweitern Sie eine Anwendung und wählen Sie den Ordner **Arbeitsabläufe** aus.

Eine Liste mit Arbeitsabläufen wird im Inhaltsbereich angezeigt.

- Erweitern Sie einen Arbeitsablauf, der ein Zuordnungsobjekt enthält.
- Erweitern Sie die Zuordnungsaufgabe und wählen Sie die Zuordnung aus.
- Klicken Sie im Detailbereich auf die Ansicht **Detaillierte Statistiken**.

In der Ansicht **Detaillierte Statistiken** werden die Durchsatzgrafik sowie Grafiken zur Ressourcennutzung angezeigt.

Optional können Sie folgende Aufgaben in der Ansicht **Detaillierte Statistiken** durchführen:

Aufgabe	Beschreibung
Grafik vergrößern	Bewegen Sie den Cursor über die Grafik und klicken Sie dann auf das Lupensymbol.
Einen Abschnitt einer vergrößerten Grafik vergrößern	Ziehen Sie den Cursor, um einen zu vergrößernden Bereich auszuwählen.
Zwischen Zeilen und Byte in der Durchsatzgrafik wechseln	Klicken Sie auf die Option „Byte“ oder auf die Option „Zeilen“.
Statistiken auswählen, die in der Durchsatzgrafik dargestellt werden sollen	Wählen Sie im Feld „Durchsatz“ die Quellen und Ziele aus, die angezeigt werden sollen.

Arbeitsablaufstatus

Wenn Sie eine Arbeitsablaufinstanz überwachen, können Sie den Status der Arbeitsablaufinstanz anzeigen. Wenn eine Arbeitsablaufinstanz nach der Unterbrechung einer Aufgabe wiederhergestellt wird, fügt die

Überwachungskomponente einen Eintrag für die Aufgabeninstanz hinzu, die im wiederhergestellten Arbeitsablauf ausgeführt wird.

Eine Arbeitsablaufinstanz kann einen der folgenden Status annehmen:

Vorzeitig beendet

Eine Arbeitsablaufinstanz wird vorzeitig beendet, wenn Sie die Arbeitsablaufinstanz über das Monitoring Tool oder mithilfe des infacmd-Befehls „wfs abortWorkflow“ vorzeitig abbrechen. Sie können eine laufende Arbeitsablaufinstanz vorzeitig beenden, wenn Sie die Anwendung, die den Arbeitsablauf enthält, beenden oder wenn Sie den Arbeitsablauf in der Anwendung deaktivieren.

Hinweis: Eine Arbeitsablaufinstanz wird auch abgebrochen, wenn der aktive Sequenzfluss im Workflow das Beenden-Ereignis erreicht.

Abgebrochen

Sie können die Arbeitsablaufinstanz auf der Registerkarte **Überwachen** oder über den Befehl „infacmd wfs cancelWorkflow“ abbrechen.

Der Arbeitsablauf kann auch den Status „Abgebrochen“ annehmen, wenn der Datenintegrationsdienst unerwartet heruntergefahren wird. Wenn der Arbeitsablauf nicht für die automatische Wiederherstellung konfiguriert ist, ändert der Dienstprozess bei einem Neustart den Status der Arbeitsablaufinstanz in „Abgebrochen“. Bevor der Datenintegrationsdienst neu gestartet wird, wird als Status für den Arbeitsablauf und die Aufgabe „Wird ausgeführt“ verwendet, obwohl der Arbeitsablauf und die Aufgabe nicht mehr ausgeführt werden. Wenn der Arbeitsablauf für die automatische Wiederherstellung konfiguriert ist, stellt der Dienstprozess bei einem Neustart die Arbeitsablaufinstanz wieder her und führt die unterbrochene Aufgabe erneut aus. Der Dienstprozess ändert den Status der Arbeitsablaufinstanz in „Wird ausgeführt“.

Abgeschlossen

Der Datenintegrationsdienst schließt die Arbeitsablaufinstanz erfolgreich ab. Eine abgeschlossene Arbeitsablaufinstanz gibt unter Umständen an, dass alle Aufgaben, Gateways und Sequenzflussauswertungen entweder erfolgreich abgeschlossen wurden oder sich in einer Struktur befanden, die nicht ausgeführt wurde.

Ein Arbeitsablauf kann auch den Status „Abgeschlossen“ annehmen, wenn eine Befehls-, Zuordnungs-, Benachrichtigungs- oder Human-Aufgabe auf einen behebbaren oder nicht behebbaren Fehler trifft. Wenn die Aufgabe den Fehler erreicht, schlägt die Aufgabe im Datenintegrationsdienst fehl. Der Datenintegrationsdienst führt nachfolgende Arbeitsablaufobjekte aus, wenn Ausdrücke in den konditionalen Sequenzflüssen mit „True“ ausgewertet werden oder wenn die Sequenzflüsse keine Bedingungen aufweisen. Wenn die Arbeitsablaufinstanz ohne weitere Unterbrechung ausgeführt wird, aktualisiert der Datenintegrationsdienst den Arbeitsablaufstatus in „Abgeschlossen“.

Bei einem Fehlschlagen der Aufgabe führt der Datenintegrationsdienst zusätzliche Objekte in der Arbeitsablaufinstanz weiter aus, wenn Ausdrücke in den konditionalen Sequenzflüssen als „True“ ausgewertet werden oder wenn die Sequenzflüsse keine Bedingungen enthalten. Wenn die Arbeitsablaufinstanz ohne weitere Unterbrechung ausgeführt wird, aktualisiert der Datenintegrationsdienst den Arbeitsablaufstatus in „Abgeschlossen“. Eine abgeschlossene Arbeitsablaufinstanz kann sowohl fehlgeschlagene als auch abgeschlossene Aufgaben enthalten.

Fehlgeschlagen

Eine Arbeitsablaufinstanz schlägt fehl, wenn ein Arbeitsablauffehler auftritt. Arbeitsablauffehler können auftreten, wenn der Datenintegrationsdienst die Parameterdatei am Anfang des Arbeitsablaufs liest, Arbeitsablaufparameter und Variablenwerte in die Aufgabeneingabe kopiert oder Ausdrücke in konditionalen Sequenzflüssen auswertet. Zusätzlich tritt ein Arbeitsablauffehler auf, wenn eine Zuweisungsaufgabe oder ein Gateway fehlschlägt.

Wenn ein Arbeitsablauffehler auftritt, beendet der Datenintegrationsdienst die Verarbeitung zusätzlicher Objekte und schlägt bei der Arbeitsablaufinstanz sofort fehl. Arbeitsablauffehler sind nicht behebbbar.

Wird ausgeführt

Der Datenintegrationsdienst führt die Arbeitsablaufinstanz aus.

Arbeitsablaufobjektstatus

Arbeitsabläufe beinhalten Aufgaben und Gateways. Wenn Sie eine Arbeitsablaufinstanz überwachen, können Sie den Status der Aufgaben anzeigen, die in der Arbeitsablaufinstanz ausgeführt werden.

Aufgaben können eine der folgenden Statusangaben aufweisen:

Vorzeitig beendet

Eine Aufgabe wird in folgenden Situationen vorzeitig beendet:

- Die Aufgabe erreicht einen nicht behebbaren Fehler.
- Sie beenden die Arbeitsablaufinstanz vorzeitig.

Wenn Sie die Arbeitsablaufinstanz vorzeitig beenden, beendet der Datenintegrationsdienst zuerst die Aufgabe und dann die Arbeitsablaufinstanz vorzeitig.

Wenn Sie die Arbeitsablaufinstanz während der Ausführung einer Zuweisungsaufgabe vorzeitig beenden, schließt der Datenintegrationsdienst die Ausführung der Aufgabe ab. Anschließend beendet der Datenintegrationsdienst die Arbeitsablaufinstanz vorzeitig und beginnt nicht mit der Ausführung anderer Objekte.

Abgeschlossen

Der Datenintegrationsdienst schließt die Aufgabe erfolgreich ab.

Fehlgeschlagen

Eine Aufgabe schlägt in folgenden Situationen fehl:

- Eine beliebige Aufgabe in einem Arbeitsablauf, der nicht für die Wiederherstellung aktiviert ist, trifft auf einen beliebigen Fehlertyp.
- Eine Zuweisungsaufgabe in einem Arbeitsablauf, der für die Wiederherstellung aktiviert ist, trifft auf einen beliebigen Fehlertyp.
- Eine Befehls-, Zuordnungs-, Benachrichtigungs- oder Human-Aufgabe mit einer Wiederherstellungsstrategie durch Neustarten in einem Arbeitsablauf, der für die Wiederherstellung aktiviert ist, trifft auf einen nicht behebbaren Fehler.
- Eine Zuordnungsaufgabe mit einer Wiederherstellungsstrategie durch Überspringen in einem Arbeitsablauf, der für die Wiederherstellung aktiviert ist, trifft auf einen beliebigen Fehlertyp.

Hinweis: Ein Arbeitsablauf kann durchgeführt werden, wenn eine Aufgabe fehlschlägt. Der Datenintegrationsdienst führt nachfolgende Arbeitsablaufobjekte aus, wenn Ausdrücke in den konditionalen Sequenzflüssen mit „True“ ausgewertet werden oder wenn die Sequenzflüsse keine Bedingungen aufweisen. Wenn die Arbeitsablaufinstanz ohne weitere Unterbrechung ausgeführt wird, aktualisiert der Datenintegrationsdienst den Arbeitsablaufstatus in „Abgeschlossen“.

Wird ausgeführt

Der Datenintegrationsdienst führt die Aufgabe aus.

Arbeitselementstatus der Mapping-Aufgabe

Wenn Sie eine Mapping-Aufgabe erweitern, können Sie den Status der Mapping-Ausführung anzeigen. Wenn Sie eine neu gestartete Zuordnungsaufgabe erweitern, können Sie die Zuordnungsjobs anzeigen, die für jeden Wiederherstellungsversuch der Arbeitsablaufinstanz ausgeführt wurden. Wenn eine Arbeitsablaufinstanz nach der Unterbrechung einer Zuordnungsaufgabe wiederhergestellt wird, fügt die Überwachungskomponente einen Eintrag für die Aufgabeninstanz hinzu, die im wiederhergestellten Arbeitsablauf ausgeführt wird.

Sie können auch den Status der Mapping-Ausführung im Arbeitsablaufdiagramm des Arbeitsablaufs anzeigen, der die Mapping-Aufgabe enthält.

Mappings, die von einer Mapping-Aufgabe ausgeführt werden, können einen der folgenden Status annehmen:

Vorzeitig beendet

Die Mapping-Aufgabe bricht ab, während das Mapping ausgeführt wird, da Sie sich entscheiden, die Arbeitsablaufinstanz abubrechen.

Abgeschlossen

Der Datenintegrationsdienst schließt das Mapping erfolgreich ab.

Fehlgeschlagen

Das Mapping trifft auf einen Fehler. Die Zuordnung und die Zuordnungsaufgabe werden in der Überwachungskomponente als fehlgeschlagen angezeigt. Die Statusangaben richten sich nicht nach der Wiederherstellungsstrategie der Zuordnungsaufgabe.

Wird ausgeführt

Der Datenintegrationsdienst führt das Mapping aus.

Abbrechen eines Arbeitsablaufs

Sie können eine Arbeitsablaufinstanz jederzeit abbrechen oder vorzeitig beenden. Sie möchten beispielsweise eine Arbeitsablaufinstanz abbrechen, die nicht mehr reagiert oder die zu viel Zeit in Anspruch nimmt, um abzuschließen.

Wenn Sie eine Arbeitsablaufinstanz abbrechen, beendet der Datenintegrationsdienst die Verarbeitung aller laufenden Aufgaben sowie die Verarbeitung der Arbeitsablaufinstanz. Der Dienst beginnt nicht mit der Ausführung von nachfolgenden Arbeitsablaufobjekten.

Wenn Sie eine Arbeitsablaufinstanz abbrechen, versucht der Datenintegrationsdienst, den Prozess für alle laufenden Aufgaben abubrechen. Wenn eine Zuweisungsaufgabe oder ein Gateway ausgeführt wird, schließt der Datenintegrationsdienst die Aufgabe oder das Gateway ab. Nach Abbruch oder Abschluss der Aufgabe bricht der Dienst die Arbeitsablaufinstanz ab. Der Dienst beginnt nicht mit der Ausführung von nachfolgenden Arbeitsablaufobjekten.

Sie können einen Arbeitsablauf auch im Arbeitsablaufdiagramm abbrechen oder daraus entfernen.

1. Klicken Sie auf die Ansicht für das **Ausführen von Statistiken**.
2. Erweitern Sie im Navigator einen Datenintegrationsdienst.
3. Erweitern Sie eine Anwendung und wählen Sie **Arbeitsabläufe** aus.
Eine Liste mit Arbeitsablaufinstanzen wird im Inhaltsbereich angezeigt.
4. Wählen Sie eine Arbeitsablaufinstanz aus.
5. Klicken Sie auf **Aktionen > Ausgewählten Arbeitsablauf stornieren** oder **Aktionen > Ausgewählten Arbeitsablauf abbrechen**.

Arbeitsablaufwiederherstellung

Bei der Arbeitsablaufwiederherstellung handelt es sich um den Abschluss einer Arbeitsablaufinstanz ab dem Unterbrechungspunkt.

Bei einem für die Wiederherstellung aktivierten Arbeitsablauf können Sie eine Arbeitsablaufinstanz wiederherstellen, wenn eine Aufgabe auf einen behebbaren Fehler trifft, Sie die Arbeitsablaufinstanz abbrechen oder der Datenintegrationsdienstprozess unerwartet heruntergefahren wird.

Zeigen Sie das Arbeitsablaufprotokoll an, um die Ursache der Unterbrechung zu identifizieren. Nach dem Beheben aller wiederherstellbaren Fehler können Sie die unterbrochene Arbeitsablaufinstanz wiederherstellen, wenn sie für die Wiederherstellung aktiviert ist.

Zwischen der unterbrochenen Ausführung und dem Wiederherstellungslauf kann eine Arbeitsablaufdefinition nicht geändert werden. Wenn eine Arbeitsablaufinstanz einen wiederherstellbaren Status hat und Sie die Arbeitsablaufmetadaten im Developer Tool ändern und die Anwendung erneut bereitstellen, die den Arbeitsablauf enthält, kann die Arbeitsablaufinstanz nicht wiederhergestellt werden.

Der Datenintegrationsdienst versucht, den vorherigen Status des Arbeitsablaufs wiederherzustellen, wenn der Dienst nach unerwartetem Herunterfahren neu startet. Standardmäßig stellt der Datenintegrationsdienst eine Arbeitsablaufinstanz nicht wieder her, die während einer Befehls-, Zuordnungs- oder Benachrichtigungsaufgabe gestoppt wurde. Darüber hinaus kann der Datenintegrationsdienst eine Arbeitsablaufinstanz nicht standardmäßig wiederherstellen, wenn Sie die Arbeitsablaufinstanz oder eine laufende Aufgabe in der Arbeitsablaufinstanz abbrechen. Sie können die Wiederherstellungsoptionen im Arbeitsablauf konfigurieren, damit der Datenintegrationsdienst in solchen Fällen eine Arbeitsablaufinstanz wiederherstellen kann.

Beim Konfigurieren der Arbeitsablaufoptionen können Sie manuelle oder automatische Wiederherstellung für den Arbeitsablauf festlegen. Wenn Sie automatische Wiederherstellung konfigurieren, startet der Datenintegrationsdienst den Arbeitsablauf ohne Benutzeraktion ab dem Punkt der Unterbrechung neu. Wenn Sie manuelle Wiederherstellung konfigurieren, können Sie den Arbeitsablauf neu starten.

Wenn eine Arbeitsablaufinstanz wiederhergestellt wird oder wenn Sie eine Arbeitsablaufinstanz wiederherstellen, startet der Datenintegrationsdienst die Aufgabe neu. Der Dienst fährt mit der Verarbeitung der nachfolgenden Arbeitsablaufobjekte fort. Wenn eine Arbeitsablaufinstanz nach der Unterbrechung einer Aufgabe wiederhergestellt wird, fügt die Überwachungskomponente einen Eintrag für die Aufgabeninstanz hinzu, die im wiederhergestellten Arbeitsablauf ausgeführt wird. Wenn ein Arbeitsablauf beispielsweise drei Mal wiederhergestellt wird und jedes Mal eine Zuordnungsaufgabe neu gestartet wird, enthält die Überwachungskomponente drei Einträge für die Zuordnungsaufgabe.

Wiederherstellungseigenschaften

Die schreibgeschützten Wiederherstellungseigenschaften werden für jede Arbeitsablaufinstanz angezeigt. Sie konfigurieren die Wiederherstellungseigenschaften für die Arbeitsablaufdefinition im Developer Tool. Sie können die Werte der Eigenschaften für die Arbeitsablaufinstanz nicht ändern.

Die folgende Tabelle beschreibt die schreibgeschützten Wiederherstellungseigenschaften für eine Arbeitsablaufinstanz:

Eigenschaft	Beschreibung
Wiederherstellung aktiviert	Gibt an, dass der Arbeitsablauf für die Wiederherstellung aktiviert ist.
Arbeitsabläufe automatisch wiederherstellen	Gibt an, dass der Datenintegrationsdienstprozess versucht, unterbrochene Arbeitsablaufinstanzen automatisch wiederherzustellen. Die Arbeitsablaufwiederherstellung beginnt nach dem Neustart des Datenintegrationsdienstprozesses.

Wiederherstellen eines Arbeitsablaufs

Sie können unterbrochene Arbeitsablaufinstanzen wiederherstellen, die für die Wiederherstellung aktiviert sind.

1. Klicken Sie auf die Ansicht für das **Ausführen von Statistiken**.
2. Erweitern Sie im Domänennavigator einen Datenintegrationsdienst.
3. Erweitern Sie eine Anwendung und wählen Sie **Arbeitsabläufe** aus.
Eine Liste mit Arbeitsablaufinstanzen wird im Inhaltsbereich angezeigt.
4. Wählen Sie die unterbrochene Arbeitsablaufinstanz aus, die Sie wiederherstellen möchten.
5. Klicken Sie auf **Aktionen > Ausgewählten Arbeitsablauf wiederherstellen**.
Überwachen Sie den Status der Arbeitsablaufwiederherstellung im Inhaltsbereich.

Arbeitsablaufprotokolle

Der Datenintegrationsdienst generiert Protokollereignisse, wenn Sie einen Arbeitsablauf ausführen. Protokollereignisse umfassen Informationen zu Arbeitsablauffehlern, zum Aufgabenfortschritt sowie zur Einstellung von Arbeitsablaufvariablen. Protokollereignisse umfassen des Weiteren die Analysen der Verknüpfungen, die vom Datenintegrationsdienst in einem Sequenzfluss überprüft werden.

Wenn eine Arbeitsablaufinstanz eine Mapping-Aufgabe enthält, generiert der Datenintegrationsdienst eine separate Protokolldatei für das Mapping. Die Mapping-Protokolldatei beinhaltet alle während der Mapping-Ausführung und aufgetretenen Fehler sowie eine Auslastungszusammenfassung und Umwandlungsstatistik.

Die Arbeitsablauf- und Mapping-Protokolle werden auf der Registerkarte „Überwachen“ angezeigt.

Wenn Sie eine unterbrochene Arbeitsablaufinstanz wiederherstellen, hängt der Datenintegrationsdienst Protokollereignisse an das aktuelle Arbeitsablaufprotokoll an. Wenn die wiederhergestellte Arbeitsablaufinstanz eine Zuordnungsaufgabe enthält, die neu gestartet wird, erstellt der Datenintegrationsdienst ein Zuordnungsprotokoll.

Wenn der Arbeitsablauf auf einem Raster läuft, wird die Wiederherstellung der Arbeitsablaufinstanz möglicherweise auf einem anderen Knoten als die ursprüngliche Arbeitsablaufinstanz ausgeführt. Wenn die Wiederherstellung auf einem anderen Knoten läuft und das Protokollverzeichnis kein gemeinsam genutzter Speicherort ist, erstellt der Datenintegrationsdienst eine Protokolldatei mit demselben Namen für den aktuellen Knoten.

Informationen im Arbeitsablaufprotokoll

Die Informationen in der Arbeitsablaufprotokolldatei geben die Abfolge von Ereignissen wieder, die bei der Ausführung des Arbeitsablaufs auftreten.

Der Datenintegrationsdienst schreibt Informationen in das Arbeitsablaufprotokoll, wenn Ereignisse der folgenden Typen auftreten:

- Der Datenintegrationsdienst beginnt mit der Ausführung einer Aufgabe oder eines anderen Objekts im Arbeitsablauf.
- Eine Aufgabe oder ein anderes Objekt im Arbeitsablauf wird zurzeit ausgeführt.
- Der Datenintegrationsdienst beendet die Ausführung einer Aufgabe oder eines anderen Objekts im Arbeitsablauf.
- Es wird eine Arbeitsablaufvariable vom Datenintegrationsdienst eingestellt oder aktualisiert.
- Der Datenintegrationsdienst überprüft die Verknüpfungen in einem Sequenzfluss und ermittelt den korrekten Pfad für den Arbeitsablauf-Prozess.

- Während des Arbeitsablaufs wird ein Arbeitsablauffehler erkannt.

Anzeigen von Protokollen für einen Arbeitsablauf

Sie können das Protokoll für eine Arbeitsablaufinstanz herunterladen, um die Details der Arbeitsablaufinstanz anzuzeigen.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Überwachen**.
2. Klicken Sie auf die Ansicht für das **Ausführen von Statistiken**.
3. Erweitern Sie im Domänennavigator einen Datenintegrationsdienst.
4. Erweitern Sie eine Anwendung und wählen Sie **Arbeitsabläufe** aus.
Eine Liste mit Arbeitsablaufinstanzen wird im Inhaltsbereich angezeigt.
5. Wählen Sie eine Arbeitsablaufinstanz aus.
6. Klicken Sie auf **Aktionen > Protokolle für gewähltes Objekt anzeigen**.
Es erscheint ein Dialog mit der Option zum Öffnen oder Speichern der Protokolldatei.

Anzeigen von Protokollen für eine Mapping-Ausführung in einem Arbeitsablauf

Sie können das Protokoll für eine Mapping-Ausführung in einen Arbeitsablauf herunterladen, um die Mapping-Details anzuzeigen.

1. Klicken Sie auf die Ansicht für das **Ausführen von Statistiken**.
2. Erweitern Sie im Domänennavigator einen Datenintegrationsdienst.
3. Erweitern Sie eine Anwendung und wählen Sie **Arbeitsabläufe** aus.
Eine Liste mit Arbeitsablaufinstanzen wird im Inhaltsbereich angezeigt.
4. Erweitern Sie eine Arbeitsablaufinstanz.
5. Erweitern Sie eine Mapping-Aufgabe und wählen Sie die Mapping-Ausführung anhand der Aufgabe aus.
6. Klicken Sie auf **Aktionen > Protokolle für gewähltes Objekt anzeigen**.
Es erscheint ein Dialog mit der Option zum Öffnen oder Speichern der Protokolldatei.

Jobstatus nach dem Neustart oder Failover des Anwendungsdiensts

Wenn der überwachende Modellrepository-Dienst einen Neustart oder ein Failover ausführt, während der Datenintegrationsdienst Jobs ausführt, stellt das Überwachungs-Tool den letzten bekannten Status aller Jobs bereit, nachdem der überwachende Modellrepository-Dienst verfügbar wird.

Wenn der Status eines Jobs nicht bekannt ist, meldet das Überwachungs-Tool den Status UNKNOWN. Wenn der überwachende Modellrepository-Dienst einen Neustart oder ein Failover auf einen Sicherungsknoten ausführt, wird das Überwachungs-Tool mit dem neuesten Status jedes Jobs aktualisiert, während der Job noch ausgeführt wird. Der Status eines Jobs, der abgeschlossen wird, bevor der Überwachungsmodellrepository-Dienst zur Verfügung steht, lautet weiterhin UNKNOWN.

Beispiel: Ein Datenintegrationsdienst wird in einer Tabelle ausgeführt. Zwei Zuordnungen werden ausgeführt, als überwachende Modellrepository-Dienst fehlschlägt. Das Überwachungs-Tool kennt den aktuellen Status dieser Zuordnungen nicht. Eine Zuordnung wird erfolgreich abgeschlossen, bevor der überwachende

Modellrepository-Dienst verfügbar wird. Die andere Zuordnung wird weiterhin ausgeführt, nachdem der überwachende Modellrepository-Dienst verfügbar ist. Das Überwachungs-Tool meldet den Status der ersten Zuordnung als UNKNOWN. Es zeigt den Status der zweiten Zuordnung als RUNNING.

Überwachen eines Ordners von Objekten

Sie können die Eigenschaften und Statistiken zu Objekten in einem Ordner im Navigator der Ansicht **Ausführungsstatistiken** anzeigen. Sie können einen der folgenden Ordner auswählen: „Jobs“, „Bereitgestellte Zuordnungs-Jobs“, „Logische Datenobjekte“, „SQL-Datendienste“, „Webdienste“ oder „Arbeitsabläufe“.

Sie können einen Filter für die Anzahl der Objekte angeben, die im Inhaltsbereich erscheinen. Sie können benutzerdefinierte Filter basierend auf einem Zeitbereich erstellen. Benutzerdefinierte Filter ermöglichen es Ihnen, bestimmte Termine und Zeiten für Job-Startzeiten, -Endzeiten, und verstrichene Zeit auszuwählen. Benutzerdefinierte Filter können Sie auch zum Filtern der Ergebnisse von mehreren Filterkriterien verwenden.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Überwachen**.
2. Klicken Sie auf die Ansicht für das **Ausführen von Statistiken**.
3. Wählen Sie im Domänen-Navigator den Ordner aus.
Der Inhaltsbereich zeigt eine Liste der Objekte im Ordner an.
4. Klicken Sie mit der rechten Maustaste auf die Kopfzeile der Tabelle, um Spalten hinzuzufügen oder zu entfernen.
5. Wählen Sie **Neue Benachrichtigungen empfangen** aus, um neue Jobs, Vorgänge, Anfragen oder Arbeitsabläufe auf der Registerkarte **Überwachen** dynamisch anzuzeigen.
6. Geben Sie Filterkriterien ein, um die Anzahl der Objekte zu reduzieren, die im Inhaltsbereich erscheinen.
7. Wählen Sie das Objekt im Inhaltsbereich, um Details über das Objekt im Detailbereich anzuzeigen.
Der Detailbereich zeigt im Inhaltsbereich mehr Informationen über das ausgewählte Objekt.
8. Um andere Jobs anzuzeigen, die ungefähr zur gleichen Zeit wie der gewählte Job begonnen wurden, klicken Sie auf **Aktionen > Kontext anzeigen**.
Der ausgewählte Job und andere Jobs, die etwa zur gleichen Zeit begonnen wurden, werden auf der Registerkarte **Kontextansicht** angezeigt. Sie können auch den Kontext von Verbindungen, bereitgestellten Mappings, Anfragen und Arbeitsabläufen anzeigen.
9. Klicken Sie auf die Schaltfläche **Schließen**, um die Registerkarte **Kontextansicht** zu schließen.

Anzeigen des Kontexts eines Objekts

Sie können den Kontext eines Objekts anzeigen, um andere Objekte desselben Typs sichtbar zu machen, die zur selben Zeit gestartet wurden wie das ausgewählte Objekt. Dies kann sinnvoll sein, um ein Problem zu lösen oder ein besseres Verständnis davon zu erhalten, was innerhalb einer bestimmten Zeitperiode passiert ist. Sie können den Kontext von Jobs, bereitgestellten Mappings, Verbindungen, Anfragen und Arbeitsabläufen anzeigen.

Angenommen, Sie stellen fest, dass ein bereitgestelltes Mapping fehlgeschlagen ist. Wenn Sie den Kontext dieses bereitgestellten Mappings anzeigen, erscheint eine ungefilterte Liste der bereitgestellten Mappings in einer eigenen Arbeitsansicht. Dieser Liste können Sie entnehmen, welche bereitgestellten Mappings etwa zu derselben Zeit gestartet wurden wie Ihr Mapping. Sie stellen fest, dass auch andere bereitgestellte Mappings

fehlgeschlagen sind. Als Ursache des Problems ermitteln Sie, dass der Datenintegrationsdienst nicht verfügbar war.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Überwachen**.
2. Klicken Sie auf die Ansicht für das **Ausführen von Statistiken**.
3. Erweitern Sie im Domänen-Navigator einen Datenintegrationsdienst und wählen Sie die Kategorie der Objekte aus.
Wählen Sie beispielsweise **Jobs**.
4. Im Inhaltsbereich wählen Sie das Objekt aus, dessen Kontext Sie anzeigen möchten.
Wählen Sie beispielsweise einen Job aus.
5. Klicken Sie auf **Aktionen > Kontext anzeigen**.

Konfigurieren des benutzerdefinierten Filters für Datum und Uhrzeit

Zum Filtern von Ergebnissen können Sie auf der Registerkarte **Überwachen** in den Spalten „Startzeit“ oder „Endezeit“ des Inhaltsbereichs einen benutzerdefinierten Filter anwenden.

1. Wählen Sie als Filteroption "Benutzerdefiniert" für die Spalten Startzeit oder Endezeit.
Der **benutzerdefinierte Filter: Das Dialogfeld Datum und Uhrzeit** erscheint.
2. Geben Sie die Datumsbereich mit den vorgegebenen Datums- und Uhrzeitformaten an.
3. Klicken Sie auf **OK**.

Konfigurieren des benutzerdefinierten Filters für abgelaufene Zeit

Zum Filtern von Ergebnissen können Sie auf der Registerkarte **Überwachen** in der Spalte „Abgelaufene Zeit“ des Inhaltsbereichs einen benutzerdefinierten Filter anwenden.

1. Wählen Sie als Filteroption "Benutzerdefiniert" für die Spalte Abgelaufene Zeit.
Der **benutzerdefinierte Filter: Das Dialogfeld Abgelaufene Zeit** erscheint.
2. Geben Sie den Zeitbereich ein.
3. Klicken Sie auf **OK**.

Konfigurieren des benutzerdefinierten Filters Mehrfachauswahl

Zum Filtern von Ergebnissen können Sie auf der Registerkarte **Überwachen** für die Spalten im Inhaltsbereich mehrere benutzerdefinierte Filter anwenden.

1. Wählen Sie für eine Spalte als Filteroption "Benutzerdefiniert".
Der **benutzerdefinierte Filter: Das Dialogfeld Mehrfachauswahl** erscheint.
2. Wählen Sie einen oder mehrere Filter aus.
3. Klicken Sie auf **OK**.

KAPITEL 14

Log-Verwaltung

Dieses Kapitel umfasst die folgenden Themen:

- [Protokollverwaltung - Übersicht, 289](#)
- [Architektur des Protokollmanagers, 290](#)
- [Protokollspeicherort, 292](#)
- [Systemprotokolle, 293](#)
- [Log-Verwaltung - Konfiguration, 293](#)
- [Die Registerkarte Logs, 295](#)
- [Protokollereignisse, 300](#)
- [Mapping-Aufgabenprotokolle, 307](#)

Protokollverwaltung - Übersicht

Der Dienstmanager sammelt Protokollereignisse für Domäne, Anwendungsdienste, Benutzer sowie PowerCenter-Sitzungen und -Arbeitsabläufe. Um die Protokollierungsfunktion durchzuführen, führt der Dienstmanager einen Protokollmanager und einen Protokollagenten aus.

Der Protokollmanager wird auf dem Master-Gateway-Knoten ausgeführt. Er sammelt und verarbeitet Protokollereignisse für Domänenoperationen des Dienstmanagers, Anwendungsdienste und Benutzeraktivitäten. Die Protokollereignisse enthalten Betriebs- und Fehlermeldungen für eine Domäne. Der Dienstmanager und die Anwendungsdienste senden Protokollereignisse an den Protokollmanager. Wenn der Protokollmanager Protokollereignisse empfängt, erstellt er Protokollereignisdateien. Sie können Dienstprotokollereignisse im Administrator Tool basierend auf von Ihnen bestimmten Kriterien anzeigen.

Der Protokollagent wird auf allen Knoten der Domäne ausgeführt. Der Protokollagent ruft die Protokollereignisse von Sitzungen und Arbeitsabläufen ab, die der PowerCenter-Integrationsdienst schreibt, und zeigt sie im Arbeitsablauf-Monitor an. Die Arbeitsablaufprotokollereignisse umfassen Informationen über die Verarbeitung und Fehler von Arbeitsabläufen sowie über Aufgaben, die der PowerCenter-Integrationsdienst durchführt. Zu den Sitzungsablaufprotokollereignissen gehören Informationen über die vom PowerCenter-Integrationsdienst ausgeführten Aufgaben, Sitzungsverarbeitung, Sitzungsfehler sowie Ladeübersichten und Umwandlungsstatistiken für die Sitzung. Sie können Protokollereignisse für den letzten ausgeführten Arbeitsablauf im Fenster Protokollereignisse im Workflow Monitor anzeigen.

Der Log Agent sammelt und verarbeitet auch Protokollereignisse für Jobs, die vom Datenintegrationsdienst ausgeführt werden. Hierzu zählen Profil-, Scorecard-, Vorschau- und Mapping-Jobs sowie SQL-Datendienste. Sie können Protokollereignisse für diese Jobs auf der Registerkarte „Überwachen“ anzeigen.

Protokollereignisdateien sind Binärdateien, die vom Log Viewer des Administrator tool zur Anzeige von Protokollereignissen verwendet werden. Wenn Sie Protokollereignisse im Administrator Tool anzeigen, nutzt der Protokollmanager die Protokollereignisdateien zur Anzeige der Protokollereignisse für Domäne, Anwendungsdienste und Benutzeraktivitäten.

Die Domänenprotokolle umfassen Protokolle über Domäne, Anwendungsdienste und Benutzeraktivität. Sie können im Administrator tool angezeigt werden. Systemprotokolle werden seitens des Informatica-Supports nur verwendet, um offene Probleme bezüglich Support zu beheben.

Verwenden Sie das Administrator Tool, um die folgenden Aufgaben mit dem Protokollmanager auszuführen:

- Konfigurieren des Speicherorts für Protokolle. Konfigurieren des Knotens, auf dem der Protokollmanager ausgeführt wird, des Verzeichnispfads für die Protokolldateien, der Löschoptionen und der Zeitzone für Protokollereignisse.
- Konfigurieren der Protokollverwaltung. Konfigurieren des Protokollmanagers für das automatische oder manuelle Löschen von Protokollen. Speichern von Protokollereignissen im XML-, Text- oder Binärformat. Konfigurieren der Zeitzone für den Zeitstempel in den Protokollereignisdateien.
- Anzeigen von Protokollereignissen. Anzeigen von Protokollereignissen für Domänenfunktion, Anwendungsdienst und Benutzeraktivitäten auf der Registerkarte "Protokolle". Filtern nach Domänenprotokollereignissen, Anwendungsdiensttyp und Benutzer.

Architektur des Protokollmanagers

Der Dienstmanager auf dem Master-Gateway-Knoten steuert den Protokollmanager. Der Protokollmanager startet, wenn Sie die Informatica-Dienste starten. Nach dem Start wartet der Protokollmanager auf Protokollereignisse vom Dienstmanager und von den Anwendungsdiensten. Wenn der Protokollmanager Protokollereignisse empfängt, erstellt er Protokollereignisdateien.

Der Protokollmanager erzeugt folgenden Arten von Protokolldateien:

- Protokollereignisdateien. Speichert Protokollereignisse im Binärformat. Der Protokollmanager erzeugt Protokollereignisdateien zur Anzeige von Protokollereignissen auf der Registerkarte "Protokolle". Wenn Sie Ereignisse im Administrator Tool anzeigen, ruft der Protokollmanager die Protokollereignisse von den Ereignisknoten ab.

Der Protokollmanager speichert die Dateien nach Datum und Knoten geordnet. Legen Sie den Verzeichnispfad mit der Option „-ld“ des Befehls `defineDomain` der `infasetup-Tools` fest.

- Dateien für die garantierte Meldungsauslieferung. Speichert Protokollereignisse für Domäne, Anwendungsdienst und Benutzeraktivität. Der Dienstmanager schreibt die Protokollereignisse in temporäre Dateien für die garantierte Meldungsauslieferung und sendet die Protokollereignisse an den Protokollmanager.

Wenn der Protokollmanager nicht mehr verfügbar ist, bleiben die Dateien für die garantierte Meldungsauslieferung im Standardprotokollverzeichnis auf dem Knoten stehen, auf dem der Dienst ausgeführt wird. Der Verzeichnispfad ist standardmäßig `<Informatica_installation_directory>/logs/<Node_Name>`. Wenn die Protokollmanager verfügbar wird, liest der Dienstmanager für den Knoten die Protokollereignisse aus den temporären Dateien, sendet die Protokollereignisse an den Protokollmanager und löscht die temporären Dateien.

Log-Ereignisse der PowerCenter-Sitzung und des Arbeitsablaufs

PowerCenter-Sitzungs- und Arbeitsablauf-Logs werden an einem Speicherort getrennt von Domänen-, Anwendungsdienst- und Benutzeraktivitäten-Logs gespeichert. Der PowerCenter Integration Service schreibt

Sitzungs- und Arbeitsablauf-Log-Ereignisse in Binärdateien auf dem Knoten, auf dem der PowerCenter Integration Service läuft.

Der Log Manager führt die folgenden Tasks zur Verarbeitung der PowerCenter Sitzungs- und Arbeitsablauf-Log-Ereignisse durch:

1. Während einer Sitzung oder eines Arbeitsablaufs schreibt der PowerCenter Integration Service binäre Log-Dateien auf dem Knoten. Er sendet Informationen über die Logs an den Log Manager.
2. Der Log Manager speichert Informationen über Arbeitsablauf- und Sitzungs-Logs in der Domänenendatenbank. Die Domänenendatenbank speichert Informationen, wie z. B. den Pfad zum Speicherort der Log-Datei, den Knoten, der das Log enthält, und den PowerCenter Integration Service, der das Log erstellt hat.
3. Wenn Sie eine Sitzung oder einen Arbeitsablauf im Fenster "Log-Ereignisse" des Workflow Monitor anzeigen, ruft der Log Manager die Informationen aus der Domänenendatenbank ab. Der Log Manager verwendet die Informationen, um den Speicherort der Logs zu ermitteln.
4. Der Log Manager nutzt einen Log Agent, um die Log-Ereignisse auf den einzelnen Knoten abzurufen, die im Fenster "Log-Ereignisse" angezeigt werden.

Job-Protokollereignisse des Datenintegrationsdiensts

Die Protokolle für die vom Datenintegrationsdienst ausgeführten Jobs werden an einem von den Protokollen für die Domäne, den Anwendungsdienst und die Benutzeraktivitäten getrennten Speicherort abgelegt. Der Datenintegrationsdienst schreibt Job-Protokollereignisse in Textdateien auf dem Knoten, auf dem er ausgeführt wird.

Der Datenintegrationsdienst und der Protokollmanager führen die folgenden Aufgaben durch, um Job-Protokollereignisse für den Datenintegrationsdienst zu verarbeiten:

1. Wenn der Datenintegrationsdienst einen Job ausführt, schreibt er die Protokollereignisse in Textdateien auf dem Knoten. Der Datenintegrationsdienst sendet Informationen über die Protokolle an den Protokollmanager.
2. Der Protokollmanager speichert Protokollinformationen in der Modellrepository-Datenbank. Die Modellrepository-Datenbank speichert Informationen, wie z. B. den Pfad zum Speicherort der Protokolldatei, den Knoten, der das Protokoll enthält, und den Datenintegrationsdienst, der das Protokoll erstellt hat.
3. Wenn Sie ein Job-Protokoll auf der Registerkarte „Überwachen“ im Administrator Tool anzeigen, ruft der Protokollmanager die Informationen aus der Modellrepository-Datenbank ab. Der Log Manager verwendet die Informationen, um den Speicherort der Protokolle zu ermitteln.
4. Der Log Manager nutzt einen Log Agent, um die Protokollereignisse auf den einzelnen Knoten abzurufen und das Protokoll anzuzeigen.

Protokollmanager-Wiederherstellung

Wenn ein Dienst Protokollereignisse generiert, sendet er sie an die Protokollmanager auf dem Master-Gateway-Knoten. Wenn Sie über die Hochverfügbarkeitsoption verfügen und der Master-Gateway-Knoten nicht mehr erreichbar ist, senden die Anwendungsdienste Protokollereignisse an den Protokollmanager auf einem neuen Master-Gateway-Knoten.

Der Dienstmanager, die Anwendungsdienste und der Protokollmanager führen die folgenden Tasks aus:

1. Ein Anwendungsdienstprozess schreibt Protokollereignisse in eine Datei für die garantierte Meldungsauslieferung.

2. Der Anwendungsdienstprozess sendet die Protokollereignisse an den Dienstmanager auf dem Gateway-Knoten für die Domäne.
3. Der Protokollmanager verarbeitet die Protokollereignisse und schreibt Protokollereignis-Dateien. Der Anwendungsdienstprozess löscht die temporäre Datei.
4. Wenn der Protokollmanager nicht verfügbar ist, bleibt die Datei für die garantierte Meldungsauslieferung auf dem Knoten, auf dem der Dienstprozess läuft. Der Dienstmanager für den Knoten sendet die Protokollereignisse in den Dateien für die garantierte Meldungsauslieferung, wenn der Protokollmanager wieder bereitsteht, und der Protokollmanager schreibt die Protokollereignis-Dateien.

Fehlersuche für den Log Manager

Domänen- und Anwendungsdienste schreiben Protokollereignisse in die Dienstmanager-Protokolldateien, wenn der Protokollmanager keine Protokollereignisse verarbeiten kann. Die Dienstmanager-Protokolldateien befinden sich im Standardprotokollverzeichnis. Zu den Service Manager-Log-Dateien gehören `catalina.out`, `localhost_<date>.txt`, und `node.log`. Dienste schreiben Log-Ereignisse in unterschiedliche Log-Dateien, abhängig von der Art des Fehlers.

Verwenden Sie die Service Manager-Log-Dateien, um Probleme zu beheben, wenn der Log Manager Log-Ereignisse nicht verarbeiten kann. Außerdem benötigen Sie diese Dateien auch zum Beheben von Problemen, wenn Sie sich an den globalen Kundensupport von Informatica wenden.

Hinweis: Sie können Fehler in einer Informatica-Installation beheben, wenn Sie die Log-Dateien benutzen, die während der Installation generiert wurden. Sie können die zusammenfassende Log-Datei der Installation benutzen, um herauszufinden, welche Komponenten bei der Installation gescheitert sind.

Protokollspeicherort

Der Dienstmanager auf dem Master-Gateway-Knoten schreibt Protokollereignisdateien in das Protokollereignisverzeichnis. Wenn Sie einen Knoten für die Verwendung als Gateway konfigurieren, müssen Sie das Verzeichnis konfigurieren, in das der Dienstmanager des Knotens die Protokollereignisdateien schreibt. Jeder Gateway-Knoten muss Zugriff auf den Verzeichnispfad haben.

Konfigurieren Sie den Protokollspeicherort in der Ansicht "Eigenschaften" für die Domäne. Konfigurieren Sie einen Verzeichnisspeicherort, auf den beim Installieren oder beim Definieren der Domäne zugegriffen werden kann. Haben Sie mehr als einem Gateway-Knoten, speichern Sie die Protokolle auf einem gemeinsamen Laufwerk. Ist der Protokollmanager nicht in der Lage, in den Verzeichnispfad zu schreiben, schreibt er die Protokollereignisse in `node.log` auf dem Master-Gateway-Knoten.

Beim Konfigurieren des Protokollspeicherorts validiert das Administrator tool das Verzeichnis während der Konfigurationsaktualisierung. Ist das Verzeichnis ungültig, schlägt die Aktualisierung fehl. Der Protokollmanager überprüft, ob das Protokollverzeichnis nach dem Starten über Lese- und Schreibberechtigung verfügt. Erfolgt die gemeinsame Nutzung des Protokollverzeichnisses nicht in einer hochverfügbaren Umgebung, besteht die Gefahr, dass die Protokolldateien Widersprüche aufweisen.

Sie können den Verzeichnispfad für Domänenprotokolle im Administrator Tool oder mit dem Protokolldienstverzeichnis-Parameter „-ld“ ändern. Der Parameter „-ld“ kann mit den folgenden Befehlen verwendet werden:

- `infacmd isp SwitchToGatewayNode`
- `infasetup DefineDomain`

- infasetup DefineGatewayNode
- infasetup UpdateGatewayNode

Systemprotokolle

Systemprotokolle enthalten Informationen, die der Informatica-Support einsieht, um Sie bei der Lösung von supportbezogenen Problemen zu unterstützen. Im Normalfall ist es nicht notwendig, dass Sie diese Protokolle anzeigen.

Der Verzeichnispfad ist standardmäßig `<Informatica_installation_directory>/logs/<Node_Name>/`. Sie können den Standardverzeichnispfad für Protokolle mit dem Systemprotokoll-Verzeichnisparameter „-sld“ ändern. Der Parameter „-sld“ kann mit den folgenden Befehlen verwendet werden:

- infasetup DefineDomain
- infasetup DefineGatewayNode
- infasetup DefineWorkerNode
- infasetup UpdateGatewayNode
- infasetup UpdateWorkerNode

Bei der Erstellung eines benutzerdefinierten Speicherorts können Sie einen lokalen Speicherort oder einen von allen Knoten genutzten Speicherort verwenden. Der Dienstmanager fügt den Knotennamen zum Pfad hinzu und generiert separate Protokollverzeichnisse für jeden Knoten.

Wenn Sie den Gateway- oder Worker-Knoten mit einem neuen Standardspeicherort für Systemprotokolle aktualisieren, bleiben die vorhandenen Protokolle intakt. Der Server erstellt künftige Protokolle am neuen Speicherort und nicht weiterhin am bisherigen Speicherort.

Wenn Sie bei der Änderung des Standardpfades einen Knotennamen angeben, fügt der Dienstmanager diesen zum Pfad hinzu. Wenn Sie beispielsweise `C:/logs/node1/` als Systemprotokollverzeichnis angeben, erstellt der Dienstmanager die Protokolle in Verzeichnissen unter `C:/logs/node1/node1/`.

Bei mehreren Informatica-Domänen müssen Sie einen anderen Verzeichnispfad für den Protokollmanager in jeder Domäne konfigurieren. Die gemeinsame Nutzung desselben Verzeichnisses durch mehrere Domänen ist nicht möglich.

Hinweis: Wenn Sie den Verzeichnispfad ändern, müssen Sie die Informatica-Dienste auf dem Knoten neu starten, den Sie geändert haben.

Log-Verwaltung - Konfiguration

Der Service Manager und die Anwendungsdienste senden kontinuierlich Log-Ereignisse an den Log Manager. Im Laufe der Zeit kann der Inhalt des Verzeichnisses eine große Anzahl von Log-Ereignissen enthalten.

Sie können die Log-Ereignisse periodisch löschen, um die Anzahl der im Log Manager gespeicherten Log-Ereignisse optimal zu verwalten. Sie können die Logs vor dem Löschen exportieren und eine Sicherungskopie der älteren Log-Ereignisse aufbewahren.

Bereinigen von Log-Ereignissen.

Sie können Log-Ereignisse automatisch oder manuell entfernen. Der Service Manager entfernt die Log-Ereignisse gemäß den Bereinigungseigenschaften aus dem Log-Verzeichnis. Die Bereinigungseigenschaften definieren Sie im Dialogfeld "Log-Verwaltung". Sie können Log-Ereignisse manuell bereinigen, um die automatischen Bereinigungseigenschaften zu überschreiben.

Löschen von Protokollereignissen - Automatisch

Der Dienstmanager entfernt die Protokollereignisse gemäß den Bereinigen-Eigenschaften aus dem Protokollverzeichnis.

Wenn die Anzahl der Tage oder die Größe des Protokollverzeichnisses die Grenze überschreitet, löscht der Log-Manager die Protokollereignisdateien, beginnend beim ältesten Protokollereignis. Der Protokoll-Manager prüft periodisch die Bereinigungsoptionen und entfernt die Protokollereignisse. Der Protokoll-Manager entfernt nicht die Ereignisdaten und den Ereignisordner des aktuellen Tages.

Die folgende Tabelle enthält eine Auflistung der Bereinigen-Eigenschaften:

Option	Beschreibung
Behält Logs für eine bestimmte Anzahl an Tagen bei	Die Anzahl der Tage der Protokollaufbewahrung. Standardwert ist „30“.
Maximale Größe für Protokolle in MB	Für die Speicherung von Protokollen reservierter Festplattenspeicher in Megabyte. Standardwert ist „200“.

Hinweis: Der Log-Manager entfernt keine PowerCenter-Sitzungs- und Arbeitsablaufprotokolldateien.

Löschen von Log-Ereignissen - Manuell

Sie können Log-Ereignisse für die Domäne, Anwendungsdienste oder Benutzeraktivität löschen. Beim Löschen von Log-Ereignissen entfernt der Log Manager die Log-Ereignisdateien aus dem Log-Verzeichnis. Der Log Manager entfernt die Log-Ereignisdateien nicht, die derzeit in die Logs geschrieben werden.

Optional können Sie den Befehl *infacmd* PurgeLog zum Löschen von Log-Ereignissen verwenden.

In der folgenden Tabelle sind die Optionen für das Löschen von Logs aufgelistet:

Option	Beschreibung
Log-Typ	Typ des zu löschenden Log-Ereignisses. Sie können Domänen-, Dienst-, Benutzeraktivitäten- oder alle Log-Ereignisse löschen.
Diensttyp	Beim Löschen von Anwendungsdienst-Log-Ereignissen können Sie Log-Ereignisse für einen bestimmten Anwendungsdiensttyp oder für alle Anwendungsdiensttypen löschen.
Einträge bereinigen	Datumsbereich der zu löschenden Log-Ereignisse. Sie können die folgenden Optionen wählen: <ul style="list-style-type: none">- Alle Einträge Löscht alle Log-Ereignisse.- Vor Datum Löscht Log-Ereignisse, die vor diesem Datum eingetreten sind. Verwenden Sie zur Eingabe des Datums das Format yyyy-mm-dd. Optional können Sie den das Datum mithilfe des Kalenders auswählen. Um den Kalender zu verwenden, klicken Sie auf das Datumsfeld.

Zeitzone

Wenn der Log Manager Log-Ereignisdateien erstellt, generiert er basierend auf der Zeitzone für jedes Log-Ereignis einen Zeitstempel. Der Zeitstempel des Protokollereignisses enthält Informationen zu Datum, Uhrzeit und Zeitzone. Erstellt der Log Manager Log-Ordner, beschriftet er die Ordner entsprechend einem Zeitstempel. Beim Exportieren oder Bereinigen von Log-Ereignisdateien verwendet der Log Manager diese Eigenschaft für die Berechnung, welche Log-Ereignisdateien bereinigt oder exportiert werden sollen. Stellen Sie als Zeitzone den Speicherort des Computers ein, auf dem die Log-Ereignisdateien gespeichert sind.

Überprüfen Sie, dass Sie keine Log-Ereignisdateien verlieren, wenn Sie die Zeitzone für den Log Manager konfigurieren. Befindet sich der Anwendungsdienst, der die Log-Ereignisse zum Log Manager überträgt, in einer anderen Zeitzone als der Master-Gateway-Knoten, verlieren Sie möglicherweise Log-Ereignisdateien, die Sie eigentlich nicht löschen wollten. Konfigurieren Sie für jeden Gateway-Knoten dieselbe Zeitzone.

Hinweis: Beim Ändern der Zeitzone müssen Sie Informatica Services auf dem geänderten Knoten neu starten.

Log-Management-Eigenschaften konfigurieren

Konfigurieren Sie die Protokollverwaltungseigenschaften in Informatica Administrator im Dialogfeld **Protokollverwaltung**.

1. Klicken Sie in der Administrator Console auf die Registerkarte **Protokolle**.
2. Wählen Sie **Protokollaktionen > Protokollverwaltung** aus.
3. Geben Sie die Anzahl von Tagen an, die der Log Manager die Log-Events aufbewahren soll.
4. Geben Sie die maximale Festplattenspeichergröße für das Verzeichnis an, das die Log-Ereignisdateien enthält.
5. Geben Sie die Zeitzone im folgenden Format an:
`GMT (+|-) <hours>:<minutes>`
Beispiel: GMT+08:00
6. Klicken Sie auf **OK**.

Die Registerkarte Logs

Auf der Registerkarte Logs des Administrator Tool können Sie Domänen, Anwendungsdienste und Log-Ereignisse für Benutzeraktivitäten anzeigen. Wenn Sie Log-Ereignisse auf der Registerkarte Logs anzeigen, erscheinen die generierten Log-Ereignisdateien im Log-Verzeichnis des Log-Managers. Erscheint eine Fehlermeldung im Administrator Tool, enthält diese einen Link zur Registerkarte Logs.

Die Registerkarte Logs lässt sich für folgende Aufgaben verwenden:

- Anzeigen von Log-Ereignissen und Operationsfehlern des Administrator Tools. Anzeigen von Log-Ereignissen für die Domäne, eines Anwendungsdienstes oder einer Benutzeraktivität.
- Zum Filtern der Ergebnisse von Log-Ereignissen. Nach der Anzeige der Log-Ereignisse können Sie diese nach bestimmten Kriterien filtern.
- Konfigurieren von Spalten. Legen Sie fest, welche Spalten auf der Registerkarte Logs erscheinen sollen.
- Speichern von Log-Ereignissen. Sie können Log-Ereignisse im Format XML, im Textformat oder im Binärformat abspeichern.
- Löschen von Log-Ereignissen. Sie können Log-Ereignisse manuell entfernen.
- Kopieren der Log-Ereignisse. Die Zeilen der einzelnen Log-Ereignisse lassen sich kopieren.

Anzeigen von Protokollereignissen

Um Protokollereignisse auf der Registerkarte "Protokolle" des Administrator-Tools anzuzeigen, wählen Sie die Domänenansicht, die Dienstanzeige oder die Benutzeraktivitätsansicht aus. Konfigurieren Sie dann die Filteroptionen. Sie können die Protokollereignisse auf der Basis der Attribute (z. B. Logtyp, Domänenfunktionskategorie, Anwendungsdiensttyp, Anwendungsdienstname, Benutzer, Meldungscode, Aktivitätscode, Zeitstempel und Sicherheitslevel) filtern. Welche Option verfügbar ist, hängt davon ab, ob Sie Ereignisse der Domäne des Anwendungsdienstes oder der Benutzeraktivitätsprotokolle anzeigen.

Um weitere Informationen zu einem Protokollereignis anzuzeigen, klicken Sie in den Suchergebnissen auf das Protokollereignis.

Wenn der Protokoll-Manager eine interne Fehlermeldung vom PowerCenter Integration Service erhält, wird unter AIX und Linux ein Stacktrace in das Protokollereignisfenster geschrieben.

Sie können die Protokolle anzeigen, um zusätzliche Informationen über Fehler zu bekommen, die Sie während der Arbeit im Administrator-Tool erhalten haben.

1. Klicken Sie im Administrator-Tool auf die Registerkarte "Protokolle".
2. Wählen Sie im Inhaltsbereich die Ansicht "Domäne", "Dienst" oder "Benutzeraktivität" aus.
3. Konfigurieren Sie die Filterkriterien, um einen bestimmten Protokollereignistyp anzuzeigen.

In der folgenden Tabelle sind die Abfragemöglichkeiten aufgelistet:

Protokolltyp	Option	Beschreibung
Domäne	Kategorie	Die Kategorie des Domänendienstes, die Sie anzeigen möchten.
Dienst	Diensttyp	Der Anwendungsdienst, den Sie anzeigen möchten.
Dienst	Dienstname	Name des Anwendungsdienstes, für den Protokollereignisse angezeigt werden sollen. Sie können den Namen eines einzelnen Anwendungsdienstes wählen oder alle Anwendungsdienste.
Domäne Dienst	Schweregrad	Der Log-Manager gibt die Protokollereignisse mit dem zugehörigen Schweregrad aus.
Benutzeraktivität	Benutzer	Name des Benutzers des Administrator-Tools
Benutzeraktivität	Sicherheitsdomäne	Sicherheitsdomäne, zu welcher der Benutzer gehört.
Domäne Dienst, Benutzeraktivität	Zeitstempel	Datenbereich für Protokollereignisse, die Sie anzeigen möchten. Sie können die folgenden Optionen wählen: <ul style="list-style-type: none"> - Leer. Zeigt alle Protokollereignisse an. - Innerhalb des letzten Tages - Innerhalb des letzten Monats - Benutzerdefiniert Gibt Start- und Enddatum an. Voreinstellung ist "Innerhalb des letzten Tages"
Domäne Dienst	Thread	Filterkriterien für Text, der in Thread-Daten erscheint. In diesem Textfeld können Sie Platzhalter (*) verwenden.

Protokolltyp	Option	Beschreibung
Domäne Dienst	Meldungscode	Filterkriterien für Text, der in Meldungscode erscheint. In diesem Textfeld können Sie Platzhalter (*) verwenden.
Domäne Dienst	Meldung	Filterkriterien für Text, der in Meldungscode erscheint. In diesem Textfeld können Sie Platzhalter (*) verwenden.
Domäne Dienst	Knoten	Name des Knotens, für den Protokollereignisse angezeigt werden sollen.
Domäne, Dienst	Prozess	Die Prozessidentifikationsnummer derjenigen Windows- oder UNIX-Dienstprozesse, die das Protokollereignis generiert haben. Sie können die Prozessidentifikationsnummer dazu nutzen, Protokollereignisse von einem Prozess zu identifizieren, wenn ein Anwendungsdienst mehrere Prozesse auf demselben Knoten ausführt.
Benutzeraktivität	Aktivitätscode	Filterkriterien für Text, der im Aktivitätscode erscheint. In diesem Textfeld können Sie Platzhalter (*) verwenden.
Benutzeraktivität	Aktivität	Filterkriterien für Text, der in der Aktivität erscheint. In diesem Textfeld können Sie Platzhalter (*) verwenden.

- Klicken Sie auf die Schaltfläche "Filter".

Der Log-Manager ruft die Protokollereignisse ab und zeigt sie in der Registerkarte "Protokolle" an, wobei das zuletzt eingetretene Protokollereignis zuerst angezeigt wird.

- Klicken Sie auf die Schaltfläche "Filter zurücksetzen", um einen anderen Satz an Protokollereignissen anzuzeigen.

Tipp: Um nach Protokollen zu suchen, die zu einem Fehler oder einem fatalen Protokollereignis gehören, beachten Sie den Zeitstempel auf dem Protokollereignis. Setzen Sie dann den Filter zurück und verwenden Sie einen benutzerdefinierten Filter, um nach weiteren Protokollereignissen zu suchen, die während des Zeitstempels des Ereignisses aufgetreten sind.

Konfigurieren von Log-Spalten

Die Registerkarte Logs können Sie so konfigurieren, dass sie folgende Spalten aufweist:

- Kategorie
- Diensttyp
- Dienstname
- Schweregrad
- Benutzer
- Sicherheitsdomäne
- Zeitstempel
- Thread
- Meldungscode
- Meldung
- Knoten

- Prozess
- Aktivitätscode
- Aktivität

Hinweis: Die Spalten werden basierend auf den von Ihnen gewählten Abfrageoptionen angezeigt. Zeigen Sie zum Beispiel einen Diensttyp an, steht der Dienstname auf der Registerkarte Logs.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Logs**.
2. Wählen Sie die Ansicht **Domäne, Dienst** oder **Benutzeraktivität**.
3. Um eine Spalte hinzuzufügen, klicken Sie mit der rechten Maustaste auf einen Spaltennamen, wählen Sie **Spalten** und danach auf den Namen der Spalte, die Sie hinzufügen möchten.
4. Zum Entfernen einer Spalte klicken Sie mit der rechten Maustaste auf einen Spaltennamen, wählen Sie **Spalten** und löschen Sie die Markierung neben dem Spaltennamen, den Sie entfernen möchten.
5. Wenn Sie eine Spalte verschieben möchten, wählen Sie den Spaltennamen und ziehen Sie ihn an die Stelle, an der er stehen soll.

Der Log Manager aktualisiert die Spalten auf der Registerkarte Logs gemäß Ihren Angaben.

Speichern von Log-Ereignissen

Sie können die Log-Ereignisse speichern, die Sie im Log Viewer filtern und anzeigen. Wenn Sie Log-Ereignisse speichern, speichert der Log Manager die von Ihnen entsprechend den Filterkriterien angezeigten Logs. Um Log-Ereignisse in einer Datei zu speichern, klicken Sie im Log-Aktionen-Menü auf "Logs speichern".

Der Log Manager löscht die Log-Ereignisse nicht, wenn Sie sie speichern. Das Administrator Tool fordert Sie auf, die gespeicherte Datei der Log-Ereignisse zu speichern oder zu öffnen.

Optional können Sie mit dem Befehl *infacmd isp GetLog* Log-Ereignisse abrufen.

Das von Ihnen gewählte Format zum Speichern von Log-Ereignissen hängt davon ab, wie Sie die exportierte Datei der Log-Ereignisse verwenden möchten:

- XML-Datei Verwenden Sie das XML-Format, wenn Sie die Log-Ereignisse in einem externen Tool analysieren möchten, das XML verwendet, oder wenn Sie XML-Tools wie zum Beispiel XSLT benutzen möchten.
- Textdatei. Verwenden Sie eine Text-Datei, wenn Sie die Log-Ereignisse in einem Texteditor analysieren möchten.
- Binärdatei. Verwenden Sie das Binärformat, um die Log-Ereignisse im binären Format zu sichern. Möglicherweise müssen Sie dieses Format verwenden, um Log-Ereignisse an den globalen Kundensupport von Informatica zu senden.

Exportieren von Log-Ereignissen

Sie können die Log-Ereignisse im Format XML, im Textformat oder im Binärformat abspeichern. Um Log-Ereignisse in eine Datei zu exportieren, klicken Sie im Menü Log-Aktionen auf Logs exportieren.

Beim Exportieren von Log-Ereignissen können Sie wählen, welche Logs Sie speichern möchten. Wenn Sie Dienst-Logs gewählt haben, können Sie Logs für einen bestimmten Diensttyp exportieren. Sie können die Sortierreihenfolge für die Log-Ereignisse in der Exportdatei auswählen.

Die exportierten Log-Ereignisse werden nicht vom Log-Manager gelöscht. Das Administrator Tool fordert Sie auf, die exportierte Log-Ereignisdatei zu speichern oder zu öffnen.

Optional können Sie Log-Ereignisse auch mit dem GetLog-Befehl *infacmd* abrufen.

Welches Format Sie zum Exportieren von Log-Ereignissen auswählen, ist davon abhängig, wie Sie die exportierte Log-Ereignisdatei verwenden möchten:

- **XML-Datei** Verwenden Sie das XML-Format, wenn Sie die Log-Ereignisse in einem externen Tool analysieren möchten, das XML verwendet, oder wenn Sie XML-Tools wie zum Beispiel XSLT benutzen möchten.
- **Textdatei.** Verwenden Sie eine Text-Datei, wenn Sie die Log-Ereignisse in einem Texteditor analysieren möchten.
- **Binärdatei.** Verwenden Sie das Binärformat, um die Log-Ereignisse im binären Format zu sichern. Möglicherweise müssen Sie dieses Format verwenden, um Log-Ereignisse an den globalen Kundensupport von Informatica zu senden.

Die folgende Tabelle beschreibt die Optionen zum Export von Logs für die einzelnen Logtypen:

Option	Log-Typ	Beschreibung
Typ	Domäne, Dienst, Benutzeraktivität	Geben Sie die Logs an, die Sie exportieren möchten.
Diensttyp	Dienst	Typ des Anwendungsdienstes, für den Log-Ereignisse exportiert werden sollen. Sie können auch Log-Ereignisse für alle Diensttypen exportieren.
Exportieren von Einträgen	Domäne, Dienst, Benutzeraktivität	Datumsbereich der Log-Ereignisse, die Sie exportieren möchten. Sie können die folgenden Optionen wählen: <ul style="list-style-type: none"> - Alle Einträge Exportiert alle Log-Ereignisse. - Vor Datum. Exportiert Log-Ereignisse, die vor dem angegebenen Datum eingetreten sind. Das Datum muss im Format yyyy-mm-dd eingegeben werden. Optional können Sie das Datum auch aus dem Kalender auswählen. Um den Kalender zu benutzen, klicken Sie auf das Datumsfeld.
Exportieren von Logs in absteigender chronologischer Reihenfolge	Domäne, Dienst, Benutzeraktivität	Exportiert Log-Ereignisse beginnend mit dem neuesten Log-Ereignis.

XML-Format

Wenn Sie Log-Ereignisse in eine XML-Datei exportieren, exportiert der Log-Manager jedes Log-Ereignis als separates Element in die XML-Datei. Das nachstehende Beispiel zeigt einen Auszug aus einer XML-Datei mit Log-Ereignissen:

```
<log xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:common="http://
www.informatica.com/pcsf/common" xmlns:metadata="http://www.informatica.com/pcsf/
metadata" xmlns:domainservice="http://www.informatica.com/pcsf/domainservice"
xmlns:logservice="http://www.informatica.com/pcsf/logservice" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">
<logEvent xsi:type="logservice:LogEvent" objVersion="1.0.0" timestamp="1129098642698"
severity="3" messageCode="AUTHEN_USER_LOGIN_SUCCEEDED" message="User Admin successfully
logged in." user="Admin" stacktrace="" service="authenticationservice"
serviceType="PCSF" clientNode="sapphire" pid="0" threadName="http-8080-Processor24"
context="" />
<logEvent xsi:type="logservice:LogEvent" objVersion="1.0.0" timestamp="1129098517000"
severity="3" messageCode="LM 36854" message="Connected to node [garnet] on outbound
connection [id = 2]." user="" stacktrace="" service="Copper" serviceType="IS"
clientNode="sapphire" pid="4484" threadName="4528" context="" />
```

Text-Format

Wenn Sie Log-Ereignisse in eine Textdatei exportieren, exportiert der Log-Manager die Log-Ereignisse in ein ICE-Protokoll (Information and Content Exchange). Das nachstehende Beispiel zeigt einen Auszug aus einer Textdatei mit Log-Ereignissen:

```
2006-02-27 12:29:41 : INFO : (2628 | 2768) : (IS | Copper) : sapphire : LM_36522 :  
Started process [pid = 2852] for task instance Session task instance  
[s_DP_m_DP_AP_T_DISTRIBUTORS4]:Executor - Master.  
2006-02-27 12:29:41 : INFO : (2628 | 2760) : (IS | Copper) : sapphire : CMN_1053 :  
Starting process [Session task instance [s_DP_m_DP_AP_T_DISTRIBUTORS4]:Executor -  
Master].  
2006-02-27 12:29:36 : INFO : (2628 | 2760) : (IS | Copper) : sapphire : LM_36522 :  
Started process [pid = 2632] for task instance Session task instance  
[s_DP_m_DP_AP_T_DISTRIBUTORS4]:Preparer.  
2006-02-27 12:29:35 : INFO : (2628 | 2760) : (IS | Copper) : sapphire : CMN_1053 :  
Starting process [Session task instance [s_DP_m_DP_AP_T_DISTRIBUTORS4]:Preparer].
```

Binärformat

Wenn Sie Log-Ereignisse in eine Binärdatei exportieren, exportiert der Log-Manager die Log-Ereignisse in eine Datei, die der globale Kundensupport von Informatica importieren kann. Sie können die Datei erst anzeigen, wenn Sie diese in Text konvertiert haben. Verwenden Sie den Befehl *infacmd* ConvertLogFile, um die Log-Datei im Binärformat in Textdateien, XML-Dateien oder auf dem Bildschirm lesbaren Text zu konvertieren.

Fehlerprotokoll im Administrator Tool

Wenn ein Fehler auftritt, während Sie einen Dienst im Administrator Tool starten, aktualisieren oder entfernen, erscheint im Inhaltsbereich des Dienstes eine Fehlermeldung, die einen Link zur Registerkarte Logs enthält. Klicken Sie diesen Link in der Fehlermeldung an, um detaillierte Informationen über den Fehler in der Registerkarte Logs zu finden.

Protokollereignisse

Der Dienstmanager und die Anwendungsdienste senden kontinuierlich Protokollereignisse an den Protokollmanager. Der Protokollmanager generiert Protokollereignisse für jeden Diensttyp.

Protokollereignisse beinhalten einen Zeitstempel in Millisekunden und einen Thread-Namen, der das Ereignis identifiziert.

Sie können die folgenden Protokollereignistypen auf der Registerkarte „Protokolle“ anzeigen:

- Domänenprotokollereignisse Von Dienstmanager-Funktionen generierte Protokollereignisse.
- Protokollereignisse im Analyst-Dienst. Protokollereignisse zu den einzelnen Analyst-Diensten, die in der Domäne ausgeführt werden.
- Content-Managementdienst-Protokollereignisse. Protokollereignisse zu jedem in der Domäne ausgeführten Content-Managementdienst.
- Datenintegrationsdienst-Protokollereignisse. Protokollereignisse zu den einzelnen Datenintegrationsdiensten, die in der Domäne ausgeführt werden.
- Protokollereignisse des Metadata Manager-Diensts. Protokollereignisse zu den einzelnen Metadata Manager-Diensten, die in der Domäne ausgeführt werden.
- Protokollereignisse des Modellrepository. Protokollereignisse zu den einzelnen Modellrepository-Diensten, die in der Domäne ausgeführt werden.

- Protokollereignisse des PowerCenter-Integrationsdiensts. Protokollereignisse zu den einzelnen PowerCenter-Integrationsdiensten, die in der Domäne ausgeführt werden.
- Protokollereignisse des PowerCenter-Repository-Diensts. Protokollereignisse von den einzelnen PowerCenter-Repository-Diensten, die in der Domäne ausgeführt werden.
- Protokollereignisse des Ressourcenmanager-Diensts. Protokollereignisse über den in der Domäne ausgeführten Ressourcenmanager-Dienst.
- Protokollereignisse des SAP BW-Diensts. Protokollereignisse zur Interaktion zwischen dem PowerCenter und dem SAP NetWeaver BI-System.
- Protokollereignisse des Webdienst-Hub. Protokollereignisse zur Interaktion zwischen Anwendungen und dem Webdienst-Hub.
- Protokollereignisse der Benutzeraktivität. Protokollereignisse zu Domänen und des Sicherheitsmanagement-Aufgaben, die ein Benutzer ausführt.

Darüber hinaus werden in Drittanbietersystemen unter Umständen eigene Protokolle generiert. Wenn beispielsweise ein Kerberos-Server eine Authentifizierungsanfrage ablehnt, generiert der Kerberos-Server Fehlermeldungen, die nicht in Informatica-Protokollen erscheinen.

Protokollereignisse - Komponenten

Der Log Manager verwendet ein gemeinsames Format zum Speichern und Anzeigen von Protokollereignissen. Die Komponenten der Protokollereignisse können zur Fehlerbehebung bei Informatica verwendet werden.

Jedes Protokollereignis enthält folgende Komponenten:

- Diensttyp, Kategorie oder Benutzer. Auf der Registerkarte Logs sind die Ereignisse nach Domänenkategorie, Diensttyp oder Benutzer kategorisiert. Wenn Sie Anwendungsdienst-Logs anzeigen, enthält die Registerkarte Logs die Namen der Anwendungsdienste. Wenn Sie Domänen-Logs anzeigen, enthält die Registerkarte Logs die Domänenkategorien im Log. Wenn Sie Benutzeraktivitäten-Logs anzeigen, enthält die Registerkarte Logs die Benutzer im Log.
- Meldung oder Aktivität. Meldungs- oder Aktivitätstext für das Protokollereignis. Verwenden Sie den Meldungstext, um weitere Informationen zu den Protokollereignissen für Domänen- und Anwendungsdienste zu erhalten. Verwenden Sie den Aktivitätstext, um weitere Informationen zu den Protokollereignissen für Benutzeraktivitäten zu erhalten. Einige Protokollereignisse enthalten eingebettete Protokollereignisse in den Meldungstexten. Das folgende Protokollereignis enthält beispielsweise ein eingebettetes Protokollereignis:

```
Client application [PmDTM], connection [59]: recv failed.
```

Bei diesem Protokollereignis ist das folgende Protokollereignis das eingebettete Protokollereignis:

```
[PmDTM], connection [59]: recv failed.
```

Wenn der Log Manager das Protokollereignis anzeigt, wird der Schweregrad für das eingebettete Protokollereignis angezeigt.

- Sicherheitsdomäne. Wenn Sie Benutzeraktivitäten-Logs anzeigen, enthält die Registerkarte Logs die Sicherheitsdomäne für die einzelnen Benutzer.
- Meldungs- oder Aktivitätscode. Protokollereigniscode. Wenn der Meldungstyp einen Fehler oder einen schwerwiegenden Fehler darstellt, klicken Sie auf den Meldungscode, um die Informatica-Wissensdatenbank zu öffnen und die Nachricht zu suchen. Sie müssen Anmeldedaten für das Supportportal im Benutzerkonto konfigurieren, um die Suche durchzuführen.
- Prozess Die Prozessidentifikationsnummer des Windows- oder UNIX-Dienstprozesses, der das Protokollereignis generiert hat. Sie können die Prozessidentifikationsnummer dazu nutzen,

Protokollereignisse von einem Prozess zu identifizieren, wenn ein Anwendungsdienst mehrere Prozesse auf demselben Knoten ausführt.

- Knoten Name des Knotens, auf dem der Prozess ausgeführt wird, der das Protokollereignis generiert hat.
- Thread Identifikationsnummer oder Namen des von einem Dienstprozess gestarteten Threads.
- Zeitstempel Datum, Uhrzeit und Zeitzone des aufgetretenen Protokollereignisses.
- Schweregrad Der Schweregrad für das Protokollereignis. Wenn Sie Protokollereignisse anzeigen, können Sie die Registerkarte Logs so konfigurieren, dass Protokollereignisse für einen bestimmten Schweregrad angezeigt werden.

Domänenprotokollereignisse

Domänenprotokollereignisse sind Protokollereignisse, die von den vom Dienstmanager ausgeführten Domänenfunktionen generiert werden.

Anhand von Domänenprotokollereignissen können Sie Informationen über die Domäne und Fehlersuchprobleme einblenden. Die Domänenprotokollereignisse können zur Fehlersuche bei Problemen während des Hochfahrens und der Initialisierung von Knoten und Anwendungsdiensten für die Domäne genutzt werden.

Domänenprotokollereignisse umfassen Protokollereignisse der folgenden Funktionen:

- **Autorisierung.** Diese Protokollereignisse treten auf, wenn der Service Manager Benutzeranfragen für die Dienste autorisiert. Anfragen können vom Administrator-Tool ausgehen.
Hinweis: Vertrauliche Informationen werden möglicherweise nicht im Domänenprotokoll angezeigt. Im Falle einer fehlgeschlagenen Benutzerauthentifizierung werden beispielsweise der Benutzer und die Sicherheitsdomäne für fehlgeschlagene Anmeldeversuche nicht angezeigt. Das Benutzeraktivitätsprotokoll enthält vollständige Informationen.
- **Containerverwaltung.** Diese Protokollereignisse treten auf, wenn der Dienstmanager Container auf Knoten mit der Berechnungsrolle verwaltet.
- **Domänenkonfiguration.** Protokollereignisse, die bei der Verwaltung der Domänenkonfigurations-Metadaten durch den Service Manager auftreten.
- **Lizenzierung.** Protokollereignisse, die beim Registrieren von Lizenzinformationen durch den Service Manager auftreten.
- **Lizenznutzung.** Diese Protokollereignisse treten auf, wenn der Service Manager Lizenzinformationen der Anwendungsdienste überprüft.
- **Protokoll-Manager.** Protokollereignisses des Log-Managers. Der Log-Manager wird auf dem Master-Gateway-Knoten ausgeführt. Er erfasst und verarbeitet Protokollereignisse für Service-Manager-Domänenoperationen und Anwendungsdienste.
- **Log Agent.** Protokollereignisses des Log Agent. Der Log Agent wird auf allen Knoten der Domäne ausgeführt. Er ruft PowerCenter-Arbeitsablauf- und Sitzungs-Log-Ereignisse ab, um sie zur Überwachung des Arbeitsablaufs anzuzeigen.
- **Überwachen.** Protokollereignisse zu Domänenfunktionen.
- **Knotenkonfiguration.** Protokollereignisse, die bei der Verwaltung der Knotenkonfigurations-Metadaten in der Domäne durch den Service Manager auftreten.
- **Benutzerverwaltung.** Protokollereignisse, die eintreten, wenn der Service Manager Benutzer, Gruppen und Berechtigungen verwaltet.

- Service Manager. Protokollereignisse des Service Managers und Signalausnahmen von DTM-Prozessen. Der Service Manager verwaltet alle Domänenoperationen. Wurde der Fehlerschweregrad eines Knotens beim Starten des Dienstes auf Debug gesetzt, umfassen die Protokollereignisse die von diesem Dienst verwendeten Umgebungsvariablen.

Log-Ereignisse im Analyst Service

Log-Ereignisse im Analyst Service enthalten die folgenden Informationen

- Projektverwaltung. Log-Ereignisse zum Verwalten der Projekte im Informatica Analyst, z.B. zum Erstellen von Objekten, Ordnen und Projekten. Log-Ereignisse zum Erstellen von Profilen, Scorecards und Referenztabelle.
- Jobs ausführen. Log-Ereignisse zum Ausführen von Profilen und Scorecards. Logs über die Vorschau von Daten.
- Benutzerberechtigungen Log-Ereignisse über die Verwaltung von Benutzerberechtigungen in Projekten.

Protokollereignisse des Data Integration Service

Die Data Integration-Service-Protokolle enthalten Protokolle zu folgenden Ereignissen:

- Konfiguration. Protokollereignisse über Änderungen der Dienstkonfiguration, Anwendungsbereitstellung oder -entfernung und Protokolle über das zugehörige Profiling Warehouse.
- Data Integration Service - Prozesse Protokollereignisse über die Anwendungsbereitstellung, Data Object Cacheaktualisierung und Benutzeranfragen zum Ausführen von Mappings, Jobs oder Arbeitsabläufen.
- Dienstaussfälle. Protokollereignisse über Fehler, die dazu führen, dass der Datenintegrationsdienst nicht verfügbar ist, z. B. Verbindungsfehler des Modellrepositors oder Fehler beim Start eines Dienstes.

Log-Ereignisse des Listener Service

Die Protokolle des PowerExchange Listener enthalten Informationen über den Anwendungsdienst, der den PowerExchange Listener verwaltet.

Die Protokolle des Listener Service enthalten die folgenden Informationen:

- Client-Kommunikation. Log-Ereignisse zur Kommunikation zwischen dem PowerCenter oder dem PowerExchange-Client und der Datenquelle.
- Listener Service. Log-Ereignisse zum Listener Service, einschließlich der Konfiguration, Aktivierung und Deaktivierung des Dienstes.
- Operationen des Listener Service. Log-Ereignisse zu Operationen wie Verwalten von Massendatenverschiebungen und Erfassen von Änderungsdaten.

Logger Service Konfigurationseigenschaften

Die Logs des PowerExchange Logger Service enthalten Informationen über den Anwendungsdienst, der den PowerExchange Logger verwaltet.

Der Logger Service enthält die folgenden Informationen:

- Verbindungen Log-Ereignisse zu Verbindungen zwischen dem Logger Service und den Quelldatenbanken.
- Logger Service. Log-Ereignisse zum Logger Service, einschließlich der Konfiguration, Aktivierung und Deaktivierung des Dienstes.

- Operationen des Logger Service. Log-Ereignisse für Operationen z. B. das Auffangen geänderter Daten und das Schreiben der Daten in die PowerExchange-Logger-Dateien.

Protokollereignisse des Modellrepository-Dienst

Protokollereignisse im Modellrepository-Dienst enthalten die folgenden Informationen:

- Modellrepository-Verbindungen. Protokollereignisse für Verbindungen zum Repository aus Informatica Developer, Informatica Analyst und dem Datenintegrationsdienst.
- Modellrepository-Dienst Protokollereignisse zum Modellrepository-Dienst, einschließlich der Aktivierung, Deaktivierung, des Startens und des Anhaltens des Diensts.
- Repository-Operationen. Protokollereignisse zu Repository-Operationen, z. B. dem Erstellen und Löschen von Repository-Inhalten und das Hinzufügen bereit gestellter Anwendungen.
- Benutzerberechtigungen Protokollereignisse über das Verwalten von Benutzerberechtigungen im Repository.

Benutzerdefinierte Rollen für den Metadata Manager Service

Die Log-Ereignisse des PowerCenter Integration Service enthalten Informationen zu jedem PowerCenter Integration Service, der in der Domäne ausgeführt wird.

Log-Ereignisse des Metadata Manager Service enthalten die folgenden Informationen:

- Repository-Operationen. Log-Ereignisse für den Zugriff auf Metadaten im Metadata Manager-Repository.
- Konfiguration Log-Ereignisse über die Konfiguration des Metadata Manager Service.
- Laufzeitprozesse. Log-Ereignisse für die Ausführung eines Metadata Manager Service, wie z. B. fehlende native Bibliotheksdateien.
- Log-Ereignisse des PowerCenter Integration Service. Sitzungs- und Arbeitsablaufstatus für Sitzungen und Arbeitsabläufe, die eine PowerCenter Integration Service-Prozess verwenden, um Daten in das Metadata Manager Warehouse zu laden oder Quell-Metadaten zu extrahieren.

Um Log-Ereignisse anzuzeigen, wie der PowerCenter Integration Service einen PowerCenter-Arbeitsablauf verarbeitet, um Daten in das Metadata Manager-Warehouse zu laden, müssen Sie das Sitzungs- oder Arbeitsablauf-Log einsehen.

Log-Ereignisse des PowerCenter Integration Service

Die Log-Ereignisse des PowerCenter Integration Service enthalten Informationen zu jedem PowerCenter Integration Service, der in der Domäne ausgeführt wird.

Die Log-Ereignisse im PowerCenter Integration Service enthalten die folgenden Informationen:

- PowerCenter Integration Service-Prozesse. Log-Ereignisse zu den PowerCenter Integration Service-Prozessen, einschließlich Dienst-Ports, Codepage, Betriebsmodus, Dienstnamen sowie zum zugeordneten Repository und dem Status des PowerCenter Repository Service.
- Lizenzierung Log-Ereignisse für Lizenzverifikationen für das PowerCenter Integration Service durch den Service Manager.

Log-Ereignisse des PowerCenter Repository Service

Die Log-Ereignisse des PowerCenter Repository Service enthalten Informationen zu den einzelnen PowerCenter Repository Services, die in der Domäne laufen.

Log-Ereignisse des PowerCenter Repository Service enthalten die folgenden Informationen:

- PowerCenter Repository-Verbindungen. Protokollieren von Ereignissen für Verbindungen zum Repository von PowerCenter-Client-Anwendungen, einschließlich Benutzernamen und Hostnamen und Portnummer der Client-Anwendung.
- PowerCenter Repository-Objekte: Protokollieren von Ereignissen für Repository-Objekte, die durch den PowerCenter Repository Service gesperrt, geholt, eingefügt oder aktualisiert wurden.
- PowerCenter Repository Service-Prozesse. Protokollieren von Ereignissen zu PowerCenter Repository Service-Prozessen, einschließlich Starten und Stoppen des PowerCenter Repository Service und Informationen über die Repository-Datenbanken, die von den PowerCenter Repository Service-Prozessen genutzt werden. Hierzu gehören auch der Repository-Betriebsmodus, die Knoten, auf denen der PowerCenter Repository Service-Prozess läuft, Initialisierungsinformationen und genutzte interne Funktionen verwendet.
- Repository-Operationen. Protokollieren von Ereignissen für Repository-Operationen, einschließlich Erstellen, Löschen, Wiederherstellen und Aktualisieren von Repository-Contents, Kopieren von Repository-Contents und die Registrierung sowie Deregistrierung lokaler Repositories.
- Lizenzierung Protokollieren von Ereignissen zur PowerCenter Repository Service-Lizenzprüfung.

Protokollereignisse des Ressourcenmanager-Diensts

Protokollereignisse des Ressourcenmanager-Diensts enthalten die folgenden Informationen:

- Ressourcenmanager-Dienst. Protokollereignisse zum Ressourcenmanager-Dienst, einschließlich der Aktivierung, Deaktivierung, des Starten und des Anhaltens des Diensts.
- Berechnungsknoten. Protokollereignisse zu Knoten mit der Berechnungsrolle, die über den Ressourcenmanager-Dienst registriert sind.

Log-Ereignisse des SAP BW Service

Die Log-Ereignisse des SAP BW Service enthalten Informationen über die Interaktion zwischen dem PowerCenter und dem SAP NetWeaver BI-System.

Die Log-Ereignisse des SAP NetWeaver BI enthalten die folgenden Log-Ereignisse für einen SAP BW Service:

- Log-Ereignisse des SAP NetWeaver BI-Systems. Fordert das SAP NetWeaver BI-System auf, einen Arbeitsablauf zu starten und Statusinformationen vom ZPMSENDSTATUS ABAP-Programm in der Prozesskette anzugeben.
- Log-Ereignisse des PowerCenter Integration Service. Sitzungs- und Arbeitsablaufstatus für Sitzungen und Arbeitsabläufe, die einen PowerCenter Integration Service-Prozess verwenden, um Daten zu laden oder Daten aus SAP NetWeaver BI zu extrahieren.

Um Log-Ereignisse zu der Verfahrensweise anzuzeigen, mit der der PowerCenter Integration Service einen SAP NetWeaver BI-Arbeitsablauf verarbeitet, müssen Sie den Sitzungs- oder Arbeitsablauf-Log anzeigen.

Protokollereignisse des Scheduler-Diensts

Scheduler-Dienstprotokolle enthalten Informationen zu den folgenden Ereignissen:

- Scheduler-Dienstereignisse. Protokollereignisse zum Scheduler-Dienst, einschließlich der Aktivierung, Deaktivierung, des Startens und des Anhaltens des Diensts.
- Ereignisse zu geplanten Objekten. Protokollereignisse zum Starten von geplanten Objektausführungen.

Log-Ereignisse des Web Services Hub

Die Log-Ereignisse des Web Services Hub enthalten Informationen über die Interaktion zwischen Anwendungen und dem Web Services Hub.

Die Log-Ereignisse des Web Services Hub enthalten folgende Log-Ereignisse:

- Web Services-Prozesse Log-Ereignisse über Web-Dienstprozesse, einschließlich Starten und Stoppen des Web Services Hub, Web-Dienst-Anfragen, den Status der Anfragen und Fehlermeldungen zu Web-Dienstaufrufen. Die Log-Ereignisse enthalten Informationen darüber, welche Dienstarbeitsabläufe vom Repository abgerufen werden.
- Log-Ereignisse des PowerCenter Integration Service. Arbeitsablauf- und Sitzungsstatus für Dienstarbeitsabläufe, einschließlich ungültiger Arbeitsablauffehler.

Protokollereignisse der Benutzeraktivität

Benutzeraktivitäts-Protokollereignisse beschreiben alle Domänen- und Sicherheitsmanagementaufgaben, die ein Benutzer ausführt.

Verwenden Sie die Protokollereignisse der Benutzeraktivität, um festzustellen, wann ein Benutzer Dienste, Knoten, Benutzer, Gruppen oder Rollen erstellt, aktualisiert oder gelöscht hat.

Der Dienstmanager schreibt Benutzeraktivitäts-Protokollereignisse, wenn der Dienstmanager einen Benutzer genehmigen muss, damit er eine der folgenden Domänenaktionen durchführen kann:

- Einen Dienstprozess aktivieren oder deaktivieren
- Einen Dienst starten, anhalten, aktivieren oder deaktivieren
- Einen Knoten hinzufügen, aktualisieren oder herunterfahren
- Die Domäneneigenschaften bearbeiten
- Einen Ordner in die Domäne verschieben

Der Dienstmanager schreibt auch jedes Mal ein Benutzeraktivitäts-Protokollereignis, wenn ein Benutzer einen Benutzer, eine Gruppe, eine Rolle oder ein Betriebssystemprofil hinzufügt, aktualisiert oder entfernt.

Das Benutzeraktivitätsprotokoll zeigt Informationen über den Benutzer an, der die Sicherheitsaktion durchgeführt oder sich nicht angemeldet hat. Wenn der Dienstmanager einen erfolglosen Anmeldeversuch protokolliert, zeigen die Protokolle eine Fehlermeldung mit den folgenden Informationen an:

- Benutzer-ID, deren Anmeldeversuch fehlgeschlagen ist
- Sicherheitsdomäne, die den Anmeldeversuch zurückgewiesen hat
- Anwendung und Version, bei der der Benutzer sich anzumelden versucht hat. Beispiel: Anwendung [Informatica Administrator] Version [10.5.2]
- Client-IP-Adresse, von der der Anmeldeversuch ausgegangen ist
- Grund für die Ablehnung. Beispiel: [<Fehlercode>] Der Benutzer [<Benutzer-ID>] in der Sicherheitsdomäne [Nativ] ist in der Domäne nicht vorhanden.]

In den Benutzeraktivitätsprotokollen werden außerdem Informationen zu Sicherheits-Audit-Trails und Protokollereignissen für Änderungen an Benutzern, Gruppen und Berechtigungen angezeigt.

Der Dienstmanager schreibt jedes Mal ein Benutzeraktivitäts-Protokollereignis, wenn ein Benutzerkonto gesperrt oder entsperrt wird. Der Dienstmanager schreibt auch jedes Mal ein Benutzeraktivitäts-Protokollereignis, wenn ein Benutzer versucht, sich bei der Domäne mit einer Clientanwendung anzumelden.

Um die Sicherheits-Audit-Trails in die Ereignisse des Benutzeraktivitätsprotokolls aufzunehmen, müssen Sie die allgemeine Eigenschaft „SecurityAuditTrail“ für den PowerCenter-Repository-Dienst im Administrator Tool aktivieren.

Wenn Sie ein oder mehrere Repository-Objekte importieren, können Sie Audit-Protokolle generieren.

Die Audit-Protokolle enthalten die folgenden Informationen über die importierte XML-Datei:

- Hostname und IP-Adresse des Clientcomputers, von dem aus die XML-Datei importiert wurde
- Vollständigen lokalen Pfad der XML-Importdatei
- Dateiname
- Dateigröße in Byte
- Name des angemeldeten Benutzers
- Anzahl der importierten Objekte
- Zeitstempel des Importvorgangs

Mapping-Aufgabenprotokolle

Sie können die Mapping-Aufgabenprotokolle anzeigen, um Probleme bei Mapping-Aufgaben zu beheben oder Informationen zur Mapping-Ausführung anzuzeigen.

Der Datenintegrationsdienst schreibt eine neue Protokolldatei für jede Mapping-Aufgabenausführung. Die Protokolldatei enthält Informationen über die Ereignisse in der Mapping-Aufgabe. Protokollereignisse sind Textzeilen, die einen Zeitstempel, einen Thread-Bezeichner, einen Schweregrad und die Protokollnachricht enthalten. Die Meldung kann allgemeine Informationen oder eine Fehlermeldung enthalten.

Der folgende Text zeigt das Format für Mapping-Aufgabenprotokollmeldungen an:

```
2022-03-03 12:28:05,409 IST <MappingCompiler-pool-4-thread-5> INFO: [MPSVCCMN_10081]
Mapping service is running [flatFile_allTransformations_mapping/
flatFile_allTransformations_mapping] deployed in [QueueApplication]
2022-03-03 12:28:05,409 IST <MappingCompiler-pool-4-thread-5> INFO: [MPSVCCMN_10083] The
Mapping Service Module submitted a job to the Integration Service. Job ID : [wyMK5pq-
BeyQm_HZtnihOw]
```

Wenn Sie die Tracingebene auf „verboseData“ festlegen, zeigt das Mapping-Aufgabenprotokoll die Parameter und Parameterwerte für die Mapping-Ausführung an.

Der folgende Text zeigt einige Mapping-Aufgabenprotokollmeldungen an, die Parameterwerte enthalten:

```
Integration Service will use override value [C:\Source] for parameter [ff_SrcDir] in
transformation [map_AllTx\read_src1].
Integration Service will use override value [8] for parameter [exp_Int] in
transformation [map_AllTx\Expression].
Integration Service will use override value [Mapping_New] for parameter [exp_String] in
transformation [map_AllTx\Expression].
Integration Service will use override value [C:\Source] for parameter [ldo_SrcDir] in
mapping \ mapplet [map_AllTx\DO_Lookup\DO_FF_REL_SRC_Read_Mapping].
```

Nachdem Sie ein Mapping auf der Spark-Engine auf einem Hadoop-Cluster ausgeführt haben, wird die Gesamtzahl der für die Ausführung des Mapping verwendeten Clusterknoten im Mapping-Aufgabenprotokoll angezeigt. Auf der Blaze-Engine wird die Anzahl der gesunden Clusterknoten angezeigt, die vom Gitter-Manager im Mapping-Aufgabenprotokoll verwendet werden.

KAPITEL 15

Domänenberichte

Dieses Kapitel umfasst die folgenden Themen:

- [Domänenberichte - Übersicht, 308](#)
- [Lizenzverwaltungsbericht, 308](#)
- [Web Services-Bericht, 315](#)

Domänenberichte - Übersicht

Aus der Registerkarte Berichte im Administrator Tool heraus können Sie die folgenden Domänenberichte ausführen:

- **Lizenzverwaltungsbericht** Überwachen der Liste der für eine Lizenz erworbenen Softwareoptionen und der Anzahl von Überschreitungen des Nutzungslimits Im Lizenzmanagerbericht werden die Informationen zur Verwendung der Lizenz wie CPU- und Repository-Nutzung und die Knotenkonfigurationsdetails eingeblendet.
- **Web Services Report** Zur Überwachung der auf einem Web Services Hub laufenden Web-Dienste. Der Web-Dienste-Bericht enthält Informationen wie die Anzahl erfolgreicher oder fehlgeschlagener Anfragen und durchschnittliche Dauer des Dienstes Sie können auch Verlaufsstatistiken für einen bestimmten Zeitraum anzeigen.

Hinweis: Läuft der Master-Gateway-Knoten auf einem UNIX-Computer und der UNIX-Computer hat keinen Grafikanzeigeserver, müssen Sie X Virtual Frame Buffer auf dem UNIX-Computer aktivieren, um die Berichtsdiagramme im Lizenzbericht oder im Web-Dienste-Bericht anzuzeigen. Laufen mehrere Gateway-Knoten auf UNIX-Computern, installieren Sie X Virtual Frame Buffer auf jedem UNIX-Computer.

Lizenzverwaltungsbericht

Sie haben die Möglichkeit, die Liste der mit Lizenz erworbenen Software-Optionen zu überwachen und zu überprüfen, wie oft die Benutzungsgrenzen einer Lizenz überschritten wurden. Im Lizenzverwaltungsbericht werden die allgemeinen Eigenschaften, die CPU- und Repository-Nutzung, die Benutzerdetails, die Details der Hardware- und Knotenkonfiguration sowie die für jede Lizenz erworbenen Optionen angezeigt.

Sie können den Lizenzverwaltungsbericht in PDF-Format auf Ihrem lokalen Computer speichern. Außerdem können Sie eine PDF-Berichtsversion per E-Mail versenden.

Führen Sie den Lizenzverwaltungsbericht aus, um folgende Informationen über die Nutzung der Lizenz zu überwachen:

- **Lizenzdetails.** Zeigt die allgemeinen Eigenschaften jeder in der Domäne zugeordneten Lizenz an.
- **CPU-Nutzung** Die Anzahl der für die Ausführung von Anwendungsdiensten in der Domäne verwendeten logischen CPUs wird eingeblendet. Zum Zweck der Lizenzerzwingung werden im Lizenzverwaltungsbericht anstatt der physischen CPUs die logischen CPUs gezählt. Übersteigt die Anzahl der logischen CPUs die Anzahl der autorisierten CPUs, steht im Lizenzverwaltungsbericht, dass die CPU-Grenze der Domäne überschritten wurde.
- **Repository-Nutzung** Zeigt die Anzahl der PowerCenter-Repository-Dienste in der Domäne.
- **Benutzerinformationen.** Zeigt Informationen über die Benutzer in der Domäne.
- **Hardwarekonfiguration** Enthält Details zu den in der Domäne eingesetzten Computern.
- **Knotenkonfiguration.** Gibt die Details jedes Knotens in der Domäne an.
- **Lizenzierte Optionen.** Blendet eine Liste der für jede Lizenz erworbenen PowerCenter- und anderen Informatica-Optionen ein.

Lizenzierung

Der Lizenzierungsabschnitt im Lizenzverwaltungsbericht enthält Informationen zu jeder Lizenz in der Domäne.

Die folgende Tabelle beschreibt die Lizenzierungsinformationen im Lizenzverwaltungsbericht:

Eigenschaft	Beschreibung
Name	Name der Lizenz.
Edition	PowerCenter Edition
Version	Version der Informatica-Plattform.
Ablaufdatum	Datum, an dem die Lizenz erlischt
Seriennummer	Seriennummer der Lizenz. Die Seriennummer kennzeichnet den Kunden oder das Projekt. Hat der Kunde mehrere multiple PowerCenter-Installationen, erhält jedes Projekt eine separate Seriennummer. Die Original- und inkrementellen Schlüssel für eine Lizenz haben dieselbe Seriennummer.
Bereitstellungsebenen	Ebene der Bereitstellung Die Werte sind Bereitstellung und Produktion.
Betriebssystem/Bitmodus	Betriebssystem und Bitmodus, zu der/dem die Lizenz gehört. Gibt an, ob die Lizenz auf einem 32-Bit- oder einem 64-Bit-Betriebssystem installiert ist.
CPU	Maximale Anzahl der autorisierten logischen CPUs.
Repository	Maximale Anzahl der autorisierten PowerCenter Repositories.
AT-benannte Benutzer	Maximale Anzahl der Benutzer, denen der Lizenzzugriff für die Informatica Analyst Berechtigung zugeordnet wurde.
Produkt-Bitmodus	Bitmodus der installierten Server-Binaries auf dem Server. Die Werte sind 32 Bit oder 64 Bit.

CPU-Zusammenfassung

Im Abschnitt CPU-Zusammenfassung des Lizenzverwaltungsberichts steht die maximale Anzahl der logischen CPUs, die zum Ausführen von Anwendungsdiensten in der Domäne verwendet werden. Anhand der Informationen aus der CPU-Zusammenfassung können Sie erkennen, ob die CPU-Nutzung die Lizenzgrenzwerte überschreitet. Ist die Anzahl der logischen CPUs größer als die per Lizenz zugelassene Gesamtanzahl CPUs, weist der Lizenzverwaltungsbericht darauf hin, dass der CPU-Grenzwert überschritten wurde.

Der Lizenzverwaltungsbericht bestimmt die Anzahl der logischen CPUs basierend auf der Anzahl von Prozessoren, Cores und Threads. Mit folgender Formel können Sie die Anzahl logischer CPUs berechnen:

$N \times C \times T$, wobei

N die Anzahl der Prozessoren angibt.

C die Anzahl der Cores in jedem Prozessor darstellt.

und T die Anzahl der Threads in jedem Knoten beziffert.

Beispiel: Ein Computer enthält 4 Prozessoren. Jeder Prozessor hat 2 Cores. Der Computer enthält 8 (4*2) physische Cores. Hyper-Threading ist aktiviert, wobei auf jeden Core 3 Threads entfallen. Die Anzahl der logischen CPUs beträgt 24 (4*2*3).

Hinweis: Obwohl der Lizenzverwaltungsbericht Threads in die Berechnung der logischen CPUs mit einbezieht, basiert die Einhaltung der Informatica Lizenzvorschriften auf der Anzahl physischer Cores, nicht auf Threads. Um die Lizenzvorschriften einzuhalten, muss die Anzahl der physischen Cores kleiner oder gleich der maximalen Anzahl lizenzierter CPUs sein. Zeigt der Lizenzverwaltungsbericht, dass Sie die Lizenzgrenze zwar überschritten haben, die Anzahl der physischen Cores jedoch kleiner oder gleich der maximalen Anzahl lizenzierter CPUs ist, können Sie die Meldung ignorieren. Sollten Sie Probleme mit der Einhaltung der Lizenzvorschriften haben, setzen Sie sich bitte mit Ihrem Informatica-Kontoverwalter in Verbindung.

Die folgende Tabelle beschreibt die zusammenfassenden Informationen über die CPUs im Lizenzverwaltungsbericht.

Eigenschaft	Beschreibung
Domäne	Name der Domäne, auf der der Bericht ausgeführt wird.
Aktuelle Nutzung	Maximale Anzahl der logischen CPUs, die zum Datum der Berichtsausführung gleichzeitig verwendet werden.
Spitzenauslastung	Maximale Anzahl der logischen CPUs, die in den letzten 12 Monaten gleichzeitig genutzt wurden.
Spitzenauslastungsdatum	Datum der gleichzeitigen Nutzung der maximalen Anzahl logischer CPUs in den letzten 12 Monaten.
Tage Überschreitung Lizenzlimit	Anzahl der Tage, an denen die CPU-Nutzung die Lizenzgrenzen überschritten hat. Überschreitet die Anzahl gleichzeitig genutzter logischer CPUs die zulässige Anzahl CPUs, bedeutet dies, dass die Domäne die CPU-Lizenzgrenze überschreitet.

CPU-Detail

Im Abschnitt CPU-Details des Lizenzverwaltungsberichts erhalten Sie Informationen zur Nutzung der CPU für jeden Host in der Domäne. Der Abschnitt CPU-Details zeigt die maximale Anzahl der logischen CPUs, die während eines ausgewählten Zeitraums täglich verwendet werden.

Der Bericht zählt die Anzahl der logische CPUs auf jedem Host, auf dem Anwendungsdienste in der Domäne laufen. Im Bericht sind die Gesamtzahlen der logischen CPUs nach Knoten aufgeführt.

Die folgende Tabelle beschreibt die CPU-Detailinformationen im Lizenzverwaltungsbericht:

Eigenschaft	Beschreibung
Hostname	Hostname des Computers.
Aktuelle Nutzung	Maximale Anzahl der logischen CPUs, die der Host am Tage der Berichtsausführung gleichzeitig nutzt.
Spitzenauslastung	Maximale Anzahl der logischen CPUs, die der Host in den letzten 12 Monaten gleichzeitig genutzt hat.
Spitzenauslastungsdatum	Datum innerhalb der letzten 12 Monate, an dem der Host die maximale Anzahl logischer CPUs gleichzeitig genutzt hat.
Zugewiesene Lizenzen	Name aller Lizenzen, die auf dem Knoten laufenden Diensten zugeordnet sind.

Repository-Zusammenfassung

Der Abschnitt Repository-Zusammenfassung des Lizenzverwaltungsberichts enthält Informationen zur Verwendung des Repositories für die Domäne. Verwenden Sie die Repository-Zusammenfassungsinformationen, um festzulegen, wann die Repository-Verwendung die Lizenzbeschränkungen übersteigt.

Die nachstehende Tabelle beschreibt die Repository-Zusammenfassungsinformationen im Lizenzverwaltungsbericht:

Eigenschaft	Beschreibung
Aktuelle Verwendung	Maximale Anzahl von aktuell in der Domäne verwendeten Repositories zum Zeitpunkt der Berichtsausführung.
Spitzenauslastung	Maximale Anzahl von gleichzeitig in der Domäne verwendeten Repositories während der letzten 12 Monate.
Spitzenauslastungsdatum	Datum innerhalb der letzten 12 Monate, an dem gleichzeitig eine maximale Anzahl von Repositories ausgeführt wurde.
Tage haben Lizenzlimit überschritten	Anzahl von Tagen, die die Repository-Verwendung das Limit bereits überschreitet.

Benutzerzusammenfassung

Der Abschnitt Benutzerzusammenfassung des Lizenzverwaltungsberichts enthält Informationen über die Benutzer des Analyst Tools in der Domäne.

Die nachstehende Tabelle beschreibt die Benutzerzusammenfassungen im Lizenzverwaltungsbericht:

Eigenschaft	Beschreibung
Benutzertyp	Typ des Benutzers in der Domäne.
Aktuell benannter Benutzer	Maximale Anzahl der Benutzer, denen die Informatica Analyst Berechtigung des Lizenzzugriffs am Tag der Berichtsausführung zugewiesen wurde.
Höchste Anzahl benannter Benutzer	Maximale Anzahl der Benutzer, denen die Informatica Analyst Berechtigung des Lizenzzugriffs in den letzten 12 Monaten zugewiesen wurde.
Höchstwert für benannte Benutzer - Datum	Datum während der letzten 12 Monate, an dem einer maximalen Anzahl gleichzeitiger Nutzer die Informatica Analyst Berechtigung des Lizenzzugriffs zugewiesen wurde.

Benutzerdetail

Der Bereich "Benutzerdetail" im Lizenzverwaltungsbericht liefert Details zu den einzelnen Benutzern des Analyst Tools in der Domäne.

Die folgende Tabelle beschreibt die Benutzerdetails im Lizenzverwaltungsbericht:

Eigenschaft	Beschreibung
Benutzertyp	Typ des Benutzers in der Domäne.
Benutzername	Benutzername
Tage seit der Anmeldung	Anzahl der Tage, die der Benutzer während der letzten 12 Monate beim Analyst Tool angemeldet war und Profiling durchgeführt hat
Höchstwert für eindeutige IP-Adressen an einem Tag	Anzahl der Computer, bei denen der Benutzer an einem einzelnen Tag während der letzten 12 Monate angemeldet war und Profiling durchgeführt hat.
Durchschnittswert für eindeutige IP-Adressen	Tagesdurchschnitt der Computer, bei denen der Benutzer an einem während der letzten 12 Monate angemeldet war und Profiling ausführen hat.
Höchstwert für IP-Adressdatum	Datum, wann der Benutzer an einem einzelnen Tag während der letzten 12 Monate bei der Höchstanzahl der Computer angemeldet war und Profiling durchgeführt hat.
Höchstwert für tägliche Sitzungen	Maximale Häufigkeit an einem einzigen Tag während der letzten 12 Monate, die der Benutzer bei einem Analyst Tool angemeldet war und Profiling durchgeführt hat.
Durchschnittswert für tägliche Sitzungen	Durchschnittliche Häufigkeit pro Tag während der letzten 12 Monate, die der Benutzer bei einem Analyst Tool angemeldet war und Profiling durchgeführt hat.
Höchstwert für Sitzungsdatum	Datum in den letzten 12 Monaten, wann der Benutzer die meisten täglichen Sitzungen im Analyst Tool hatte.

Hardwarekonfiguration

Der Abschnitt Hardwarekonfiguration des Lizenzverwaltungsberichts enthält Details über die in der Domäne verwendeten Maschinen.

Die nachstehende Tabelle beschreibt die Hardwarekonfigurationsinformationen im Lizenzverwaltungsbericht:

Eigenschaft	Beschreibung
Hostname	Hostname des Computers.
Logische CPUs	Anzahl der logischen CPUs, die zur Ausführung von Anwendungsdiensten in der Domäne verwendet werden.
Sockets	Anzahl der Sockets auf dem Computer.
Benutzte Kerne	Anzahl der Kerne auf dem Computer.
Kerne pro Socket	Anzahl der Kerne für jedes Socket auf dem Computer.
CPU-Modell	Modell der CPU.
Hyperthreading aktiviert	Gibt an, ob die Hyperthread-Funktion aktiv ist.
Virtuelle Maschine	Gibt an, ob der Computer eine virtuelle Maschine ist.

Knotenkonfiguration

Der Bereich "Knotenkonfiguration" im Lizenzverwaltungsbericht liefert Details zu den einzelnen Knoten in der Domäne.

Die folgende Tabelle beschreibt die Knotenkonfigurationsinformationen im Lizenzverwaltungsbericht:

Eigenschaft	Beschreibung
Knotenname	Name der Knoten, die einem Computer für eine Lizenz zugeordnet sind.
Hostname	Hostname des Computers.
IP-Adresse	IP-Adresse des Knotens.
Betriebssystem	Betriebssystem des Computers, auf dem der Knoten läuft.
Status	Status des Knotens.
Gateway	Gibt an, ob der Knoten ein Gateway ist.
Diensttyp	Typ des Anwendungsdienstes, der auf dem Knoten laufen soll.
Dienstname	Name des Anwendungsdienstes, der auf dem Knoten laufen soll.
Dienststatus	Status des Anwendungsdienstes.
Zugewiesener Dienst	Dem Anwendungsdienst zugeordnete Lizenz.

Lizenzierte Optionen

Der Abschnitt Lizenzierte Optionen des Lizenzverwaltungsberichts enthält Details über jede Option für jede Lizenz, die einer Domäne zugewiesen ist.

Die nachstehende Tabelle beschreibt die Lizenzoptionsinformationen im Lizenzverwaltungsbericht:

Eigenschaft	Beschreibung
Lizenzname	Name der Lizenz.
Beschreibung	Name der Lizenzoption.
Status	Status der Lizenzoption.
Ausstellungsdatum	Datum, an dem die Lizenzoption ausgestellt wurde.
Ablaufdatum	Datum, an dem die Lizenzoption abläuft.

Lizenzverwaltungsbericht ausführen

Führen Sie den Lizenzverwaltungsbericht von der Registerkarte **Berichte** im Administrator Tool aus.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Berichte**.
2. Klicken Sie auf die Ansicht **Lizenzverwaltungsbericht**.
Der Lizenzverwaltungsbericht erscheint.
3. Klicken Sie auf **Speichern**, um den Lizenzverwaltungsbericht als PDF-Datei zu speichern.
Wenn ein Lizenzverwaltungsbericht Multibyte-Zeichen enthält, müssen Sie den Service Manager so konfigurieren, dass er eine Unicode-Schriftart verwendet.
4. Klicken Sie auf **E-Mail**, um eine Kopie des Lizenzverwaltungsberichts in einer E-Mail zu versenden.
Die Seite **Lizenzverwaltungsbericht senden** erscheint.

Konfigurieren der Unicode-Schriftart für den Bericht

Bevor Sie einen Lizenzverwaltungsbericht speichern können, der Multibyte-Zeichen enthält, müssen Sie den Dienstmanager für die Nutzung einer Unicode-Schriftart beim Generieren der PDF-Datei konfigurieren.

1. Installieren Sie eine Unicode-Schriftart auf dem Master-Gateway-Knoten.
2. Verwenden Sie einen Texteditor, um eine Datei mit dem Namen AcUtil.properties zu erstellen.
3. Fügen Sie der Datei die folgenden Eigenschaften hinzu:

```
PDF.Font.Default=Unicode_font_name
PDF.Font.MultibyteList=Unicode_font_name
```

Unicode_font_name ist der Name der auf dem Master-Gateway-Knoten installierten Unicode-Schriftart.

Möglicherweise müssen Sie auch die folgende Eigenschaft hinzufügen, wenn die Schriftartdatei im Gebietsschema nicht verfügbar ist:

```
Unicode_font_name_path=Unicode_font_file_location
```

Beispiel:

```
PDF.Font.Default=Arial Unicode MS
PDF.Font.MultibyteList=Arial Unicode MS
Arial Unicode MS_path=/usr/lib/X11/fonts/TrueType
```

4. Speichern Sie die Datei AcUtil.properties an folgendem Speicherort:
InformaticaInstallationDir\services\AdministratorConsole\administrator
5. Benutzen Sie einen Texteditor, um die Datei licenseUtility.css am folgenden Speicherort zu öffnen:
InformaticaInstallationDir\services\AdministratorConsole\administrator\css

6. Hängen Sie den Namen der Unicode-Schriftart an den Wert jeder Eigenschaft der Schriftartenfamilie an.
Beispiel:
`Schriftartenfamilie: Arial Unicode MS, Verdana, Arial, Helvetica, sans-serif;`
7. Starten Sie die Informatica-Dienste auf jedem Knoten der Domäne neu.

Lizenzverwaltungsbericht in einer E-Mail verschicken

Sie müssen die SMTP-Einstellungen für die Domäne konfigurieren, bevor Sie den Lizenzverwaltungsbericht in einer E-Mail verschicken können.

Der Domänen-Administrator kann den Lizenzverwaltungsbericht von der Lizenzverwaltungsbericht-Seite im Administrator Tool in einer E-Mail verschicken.

1. Geben Sie die folgenden Informationen ein:

Eigenschaft	Beschreibung
E-Mail-Empfänger	E-Mail-Adresse, an die Sie den Lizenzverwaltungsbericht senden.
Betreff	Betreff der E-Mail.
Kundenname	Name der Organisation, die die Lizenz erworben hat.
Anforderungs-ID	Nummer der Anfrage, die das Projekt identifiziert, für das die Lizenz erworben wurde.
Kontakt: Name	Name der Kontaktperson in der Organisation.
Kontakt: Telefonnummer	Telefonnummer der Kontaktperson.
Kontakt: E-Mail	E-Mail-Adresse der Kontaktperson beim Kunden vor Ort.

2. Klicken Sie auf OK.

Das Administrator Tool verschickt den Lizenzverwaltungsbericht in einer E-Mail.

Web Services-Bericht

Um die Performance von Web-Diensten zu analysieren, die auf einem Web Services Hub ausgeführt werden, können Sie einen Bericht für den Web Services Hub oder einen Web-Dienst, der auf dem Web Services Hub ausgeführt wird, erstellen.

Der Web-Dienste-Bericht enthält Laufzeit- und Historieninformationen zu denjenigen Web-Dienst-Anfragen, die von diesem Web Services Hub behandelt werden. Der Bericht zeigt die gesammelten Informationen für alle Web-Dienste in diesem Web Services Hub an und Informationen für alle Web-Dienste, die auf diesem Web Services Hub ausgeführt werden. Der Web-Dienst-Bericht enthält auch historische Informationen.

Über den Web-Dienste-Bericht

Sie können den Web-Dienste-Bericht für ein gewähltes Zeitintervall ausführen. Der Web-Dienste-Hub sammelt Informationen zu den Aktivitäten des Web-Dienstes und speichert diese 24 Stunden zur Verwendung im Web-Dienste-Bericht. Ferner schreibt er die Informationen in einen Historiendatei.

Zeitintervall

Standardmäßig zeigt der Web-Dienste-Bericht die Aktivitätsinformationen in einem Fünf-Minuten-Intervall an. Sie können eines der folgenden Zeitintervalle wählen, in denen die Aktivitätsinformationen für einen Web-Dienst oder Web Service Hub angezeigt werden sollen:

- 5 Sekunden
- 1 Minute
- 5 Minuten
- 1 Stunde
- 24 Stunden

Der Web-Dienste-Bericht zeigt die Aktivitätsinformationen für das gewählte Zeitintervall an, das vor der Ausführung des Berichts endet. Zum Beispiel: Wenn Sie den Web-Dienste-Bericht um 8:05 Uhr für ein Zeitintervall von einer Stunde ausführen, so zeigt der Web-Dienste-Bericht die Aktivität des Web Service Hub für die Zeit von 7:05 Uhr bis 8:05 Uhr an.

Zwischenspeichern

Der Web-Dienst-Hub speichert die Aktivitätsdaten im Zeitraum von 24 Stunden. Der Cache wird jedes Mal neu initialisiert, wenn der Web-Dienst-Hub neu gestartet wird. Der Web-Dienstbericht enthält die statistischen Daten des Caches für das Zeitintervall, in dem der Bericht ausgeführt wurde.

Historiendatei

Der Web Services Hub schreibt die zwischengespeicherten Aktivitätsdaten in eine Historiendatei. Der Web Services Hub speichert die Daten in der Historiendatei für die Anzahl von Tagen, die Sie in der Eigenschaft MaxStatsHistory des Web Services Hub angegeben haben. Zum Beispiel: Wenn der Wert in der Eigenschaft MaxStatsHistory 5 beträgt, bewahrt der Web Services Hub die Daten fünf Tage lang in der Historiendatei auf.

Inhalte des Web-Dienste-Berichts

Die Ansicht „Web Services Report“ enthält Informationen über die Webdienste in einer Domäne. Wenn Sie einen Webdienst-Hub im Navigator auswählen, können Sie die folgenden Informationen über die darin enthaltenen Webdienste anzeigen:

- **Eigenschaftenansicht:** Zeigt Allgemeine Eigenschaften, Zusammenfassung für Webdienst-Hub und historische Statistiken für den Webdienst-Hub an.
- **Ansicht „Webdienste“:** Enthält eine Liste der Webdienste im Webdienst-Hub. Wenn Sie einen Webdienst auswählen, können Sie Eigenschaften, Top-IP-Adressen und Historische Statistik für den Webdienst anzeigen.

Allgemeine Eigenschaften und Zusammenfassung für den Web Services Hub

Zum Einblenden der allgemeinen Eigenschaften und der Zusammenfassung für den Web Services Hub wählen Sie bitte die Ansicht Eigenschaften in der Inhaltsübersicht.

In der folgenden Tabelle werden die allgemeinen Eigenschaften beschrieben:

Eigenschaft	Beschreibung
Name	Name des Web Services Hub
Beschreibung	Kurzbezeichnung des Web Services Hub
Diensttyp	Typ des Dienstes. Bei einem Web Services Hub ist der Diensttyp ServiceWSHubService.

Die folgende Tabelle beschreibt die zusammengefassten Eigenschaften des Web Services Hub:

Eigenschaft	Beschreibung
Anzahl der erfolgreichen Nachrichten	Anzahl der Anfragen, die der Web Services Hub erfolgreich bearbeitet hat
Anzahl der Fehler-Antworten	Anzahl der von Web-Diensten im Web Services Hub generierten Fehlerantworten. Die Fehlerantworten können durch einen beliebigen Fehler bedingt sein:
Nachrichten gesamt	Gesamtanzahl der vom Web Services Hub erhaltenen Anfragen
Neustart-Zeit des letzten Servers	Datum und Uhrzeit des letzten Starts des Web Services Hub
Durchschnittliche Anzahl von Dienstpartitionen	Durchschnittliche Anzahl der Partitionen, die für alle Web-Dienste im Web Services Hub zugewiesen wurden
% verwendeter Partitionen	Prozentuale Angabe der Web-Dienst-Partitionen, die für alle Web-Dienste im Web Services Hub benutzt werden.
Durchschnittliche Anzahl der Ausführungsinstanzen	Durchschnittliche Anzahl der für alle Web-Dienste ausgeführten Instanzen im Web Services Hub.

Historienstatistik-Tabelle für Web Services

Um die Historienstatistik für die Web-Dienste im Web Services Hub anzuzeigen, wählen Sie die Ansicht Eigenschaften im Inhaltsbereich. Der Detailbereich zeigt die Daten aus der Historiendatei des Web Services Hub für das Datum an, das Sie angegeben haben.

Die folgende Tabelle beschreibt die Historienstatistik:

Eigenschaft	Beschreibung
Uhrzeit	Zeitpunkt des Ereignisses
Web-Dienst	Name des Web-Dienstes, für den die Informationen angezeigt werden. Wenn Sie den Namen eines Web-Dienstes anklicken, zeigt der Web-Dienst-Bericht das Fenster Dienststatistiken an.
Erfolgreiche Anfragen	Anzahl der Anfragen, die erfolgreich vom Web-Dienst verarbeitet wurden.
Antwort vom Typ 'Fault'	Anzahl der fehlerhaften Anfragen, die vom Web-Dienst verarbeitet wurden.
Dienstzeit (Durchschnitt)	Durchschnittliche Zeit, die zur Verarbeitung einer Dienstanfrage vom Web-Dienst erforderlich war.
Maximale Dienstzeit	Maximale Zeit, die zur Verarbeitung einer Dienstanfrage vom Web-Dienst erforderlich war.
Minimale Dienstzeit	Minimale Zeit, die zur Verarbeitung einer Dienstanfrage vom Web-Dienst erforderlich war.
DTM-Zeit (Durchschnitt)	Durchschnittliche Anzahl von Sekunden, die der PowerCenter Integration Service benötigte, um eine Anfrage vom Web Services Hub zu verarbeiten.
Dienstpartitionen (Durchschnitt)	Durchschnittliche Anzahl der Sitzungspartitionen, die dem Web-Dienst zugeteilt wurden.
% verwendete Partitionen	Prozentualer Anteil der vom Web-Dienst benutzten Partitionen.
Ausführungsinstanzen (Durchschnitt)	Durchschnittliche Anzahl der für den Web-Dienst ausgeführten Instanzen.

Laufzeitstatistiken für Web Services

Um die Laufzeitstatistiken für die Web-Dienste im Web Services Hub anzuzeigen, wählen Sie die Ansicht Web-Dienste im Inhaltsbereich. Die Ansicht Web-Dienste für die Statistiken für jeden Web-Dienst auf.

Der Bericht enthält folgende Informationen für jeden Web-Dienst innerhalb des gewählten Zeitintervalls:

Eigenschaft	Beschreibung
Dienstname	Name des Web-Dienstes, für den die Informationen angezeigt werden.
Erfolgreiche Anfragen	Anzahl der Anfragen, die der Web-Dienst erhalten hat und die der Web Services Hub erfolgreich verarbeiten konnte.
Antwort vom Typ 'Fault'	Anzahl der fehlerhaften Antworten, die von den Web-Diensten im Web Services Hub generiert wurden.

Eigenschaft	Beschreibung
Dienstzeit (Durchschnitt)	Durchschnittliche Zeit, die zur Verarbeitung einer Dienstanfrage vom Web-Dienst erforderlich war.
Dienstpartitionen (Durchschnitt)	Durchschnittliche Anzahl der Sitzungspartitionen, die dem Web-Dienst zugeteilt wurden.
Ausführungsinstanzen (Durchschnitt)	Durchschnittliche Anzahl von Instanzen des Web-Dienstes, die während des Intervalls ausgeführt wurden.

Web-Dienst-Eigenschaften

Um die Eigenschaften eines Web-Dienstes anzuzeigen, wählen Sie den Web-Dienst in der Ansicht Web-Dienste des Inhaltsbereichs aus. Im Detailsbereich zeigt die Ansicht Eigenschaften die Eigenschaften für den aktuell gewählten Web-Dienst an.

Der Bericht stellt die folgenden Informationen zum ausgewählten Web-Dienst bereit:

Eigenschaft	Beschreibung
Anzahl von erfolgreichen Anfragen	Anzahl der Anfragen, die der Web-Dienst erhalten hat und die der Web Services Hub erfolgreich verarbeiten konnte.
Anzahl von Antworten vom Typ 'Fault'	Anzahl der fehlerhaften Antworten, die von den Web-Diensten im Web Services Hub generiert wurden.
Nachrichten gesamt	Anzahl der gesamten Anfragen, die der Web Services Hub erhalten hat.
Letzter Serverneustart - Uhrzeit	Datum und Uhrzeit des letzten Starts des Web Services Hub.
Letzte Dienstzeit	Anzahl in Sekunden, die die letzte Dienstanfrage für die Verarbeitung benötigte
Durchschnittliche Dienstzeit	Durchschnittliche Zeit, die zur Verarbeitung einer Dienstanfrage vom Web-Dienst erforderlich war.
Durchschnittliche Anzahl von Dienstpartitionen	Durchschnittliche Anzahl der Sitzungspartitionen, die dem Web-Dienst zugeteilt wurden.
Durchschnittliche Anzahl von Ausführungsinstanzen	Durchschnittliche Anzahl von Instanzen des Web-Dienstes, die während des Intervalls ausgeführt wurden.

Top IP-Adressen des Web-Dienstes

Um die wichtigsten IP-Adressen für einen Web-Dienst anzuzeigen, wählen Sie die Ansicht Web-Dienste im Inhaltsbereich und wählen im Detailbereich die Ansicht "Top IP-Adressen". In dieser Ansicht werden die am

häufigsten aktiven IP-Adressen für den Web-Dienst angezeigt und in der Reihenfolge der am längsten bis zu den kürzesten beanspruchten Dienstzeiten aufgelistet.

Der Bericht stellt folgende Information für jede der am meisten aktiven IP-Adressen bereit:

Eigenschaft	Beschreibung
Top 10 Client-IP-Adressen	Die Liste der Client-IP-Adressen und die längste Zeit, die ein Web-Dienst benötigt hat, um die Anfrage eines Client zu verarbeiten. Die Client-IP-Adressen werden in der Reihenfolge von längster bis kürzester Dienstzeit aufgeführt. Verwenden Sie den Link <i>Hier klicken</i> , um die Liste der IP-Adressen und Dienstzeiten anzuzeigen.

Historienstatistik-Tabelle für Web-Dienst

Um die Tabelle der Historienstatistik für einen Web-Dienst anzuzeigen, wählen Sie in der Ansicht Web-Dienst im Inhaltsbereich einen Web-Dienst aus und aktivieren im Detailbereich die Tabellenansicht. Der Detailsbereich zeigt eine Tabelle der Historienstatistik für den Web-Dienst an.

Die Tabelle stellt die folgenden Informationen zum ausgewählten Web-Dienst bereit.

Eigenschaft	Beschreibung
Uhrzeit	Zeitpunkt des Ereignisses
Web-Dienst	Name des Web-Dienstes, für den die Informationen angezeigt werden.
Erfolgreiche Anfragen	Anzahl der Anfragen, die erfolgreich vom Web-Dienst verarbeitet wurden.
Antwort vom Typ 'Fault'	Anzahl der Anfragen, die vom Web-Dienst empfangen, aber nicht erfolgreich verarbeitet wurden, sondern Fehlerantworten generierten.
Dienstzeit (Durchschnitt)	Durchschnittliche Zeit, die zur Verarbeitung einer Dienstanfrage vom Web-Dienst erforderlich war.
Min. Dienstzeit	Minimale Zeit, die zur Verarbeitung einer Dienstanfrage vom Web-Dienst erforderlich war.
Max. Dienstzeit	Maximale Zeit, die zur Verarbeitung einer Dienstanfrage vom Web-Dienst erforderlich war.
DTM-Zeit (Durchschnitt)	Durchschnittliche Zeit, die der PowerCenter Integration Service benötigte, um eine Anfrage vom Web Services Hub zu verarbeiten.
Dienstpartitionen (Durchschnitt)	Durchschnittliche Anzahl der Sitzungspartitionen, die dem Web-Dienst zugeteilt wurden.
% verwendete Partitionen	Prozentualer Anteil der vom Web-Dienst benutzten Partitionen.
Ausführungsinstanzen (Durchschnitt)	Durchschnittliche Anzahl der für den Web-Dienst ausgeführten Instanzen.

Ausführen des Web Services Report

Führen Sie den Web-Dienst-Bericht von der Registerkarte Berichte im Administrator Tool aus.

Bevor Sie den Web-Dienst-Bericht für ein Web-Dienste-Hub ausführen, stellen Sie sicher, dass das Web-Dienste-Hub aktiviert ist. Bevor Sie den Web-Dienst-Bericht nicht für ein deaktiviertes Web-Dienste-Hub ausführen.

1. Klicken Sie im Administrator Tool auf die Registerkarte Sicherheit.
2. Klicken Sie auf "Web-Dienste".
3. Im Navigator wählen Sie das Web-Dienste-Hub, für das Sie den Bericht auszuführen möchten.
Im Inhaltsbereich zeigt die Ansicht Eigenschaften die Eigenschaften für das aktuell gewählte Web-Dienste-Hub an. Die Detailansicht zeigt historische Statistiken zu den Diensten im Web-Dienste-Hub.
4. Um ein Datum für die historischen Statistiken anzugeben, klicken Sie auf das Datumsfilter-Symbol im Detailbereich und wählen das Datum aus.
5. Um die Eigenschaften eines Web-Dienstes anzuzeigen, wählen Sie den Web-Dienst in der Ansicht Web-Dienste des Inhaltsbereichs aus.
Die Ansicht Web-Dienste zeigt Übersichtsstatistiken zu den einzelnen Diensten im Web-Dienste-Hub.
6. Um weitere Informationen zu einem Dienst anzuzeigen, wählen Sie den Dienst aus der Liste.
Im Detailbereich zeigt die Ansicht Eigenschaften die Eigenschaften des Dienstes an.
7. Zur Anzeige der wichtigsten IP-Adressen für den Dienst wählen Sie im Detailbereich die Ansicht "Top IP-Adressen".
8. Zur Anzeige der Tabellenattribute für den Dienst wählen Sie im Detailbereich die Ansicht "Tabelle".

Web Services Report für einen sicheren Web Services Hub ausführen

Um einen Web-Dienste-Hub auf HTTPS auszuführen, müssen Sie über eine SSL-Zertifikatsdatei für die Authentifizierung der Nachrichtenübertragungen verfügen. Wenn Sie einen Web-Dienste-Hub erstellen, der auf HTTPS ausgeführt werden soll, müssen Sie den Speicherort der Schlüsselspeicherdatei angeben, die das Zertifikat für den Web-Dienste-Hub enthält. Um die den Web-Dienste-Bericht im Administrator Tool für einen sicheren Web-Dienste-Hub ausführen zu können, müssen Sie das SSL-Zertifikat in das Java-Zertifikat importieren. Die Java-Zertifikatsdatei hat den Namen *cacerts* und befindet sich im Verzeichnis */lib/security* unter dem Java-Verzeichnis. Das Administrator Tool verwendet die *cacerts*-Zertifikatsdatei, um festzustellen, ob ein SSL-Zertifikat vertrauenswürdig ist.

In einer Domäne mit mehreren Knoten beeinflusst der Knoten, auf dem Sie das SSL-Zertifikat generieren, wie Sie auf den Web-Dienste-Bericht für einen sicheren Web-Dienste-Hub zugreifen können.

Beachten Sie die folgenden Regeln und Richtlinien bei der Ausführung des Web-Dienste-Berichts für einen sicheren Web-Dienste-Hub in einer Domäne mit mehreren Knoten:

- Generieren Sie für jeden sicheren Web-Dienste-Hub, der in einer Domäne läuft, ein SSL-Zertifikat und importieren Sie es in eine Java-Zertifikatsdatei.
- Das Administrator Tool sucht nach SSL-Zertifikaten in der Zertifikatsdatei eines Gateway-Knotens. Das SSL-Zertifikat für einen Web-Dienste-Hub, der auf einem Worker-Knoten läuft, muss auf einem Gateway-Knoten erzeugt werden und in die Zertifikatsdatei mit dem gleichen Gateway-Knoten importiert werden.
- Zur Anzeige des Web-Dienste-Berichts für einen sicheren Web-Dienste-Hub melden Sie sich beim Administrator Tool von dem Gateway-Knoten aus an, auf dem sich die Zertifikatsdatei mit dem SSL-Zertifikat des Web-Dienste-Hubs befindet, für den Sie Berichte anzeigen möchten.
- Wenn ein sicherer Web-Dienste-Hub auf einem Worker-Knoten läuft, muss das SSL-Zertifikat erzeugt und in die Zertifikatsdatei des Gateway-Knotens importiert werden. Wenn ein sicherer Web-Dienste-Hub auf einem Gateway- und einem Worker-Knoten läuft, muss das SSL-Zertifikat erzeugt und in die

Zertifikatsdatei des Gateway-Knotens importiert werden. Um Berichte für den sicheren Web-Dienste-Hub anzuzeigen, melden Sie sich beim Administrator Tool vom Gateway-Knoten aus an.

- Wenn die Domäne über zwei Gateway-Knoten verfügt und einen sicheren Web-Dienste-Hub auf jedem der Gateway-Knoten läuft, hängt der Zugriff auf die Web-Dienste-Bereich davon ab, wo sich das SSL-Zertifikat befindet.

Zum Beispiel: Auf dem Gateway-Knoten GWN01 läuft der Web-Dienste-Hub WSH01 und auf dem Gateway-Knoten GWN02 läuft der Web-Dienste-Hub WSH02. Sie können die Berichte für die Web-Dienste-Hubs abhängig vom Standort der SSL-Zertifikate anzeigen:

- Wenn das SSL-Zertifikat für WSH01 in der Zertifikatsdatei von GWN01, aber nicht von GWN02, steht, können Sie die Berichte für WSH01 anzeigen, wenn Sie sich über GWN01 beim Administrator Tool anmelden. Sie können die Berichte für WSH01 nicht anzeigen, wenn Sie sich über GWN02 beim Administrator Tool anmelden. Wenn GWN01 ausfällt, können Sie keine Berichte für WSH01 anzeigen.
 - Wenn das SSL-Zertifikat für WSH01 in den Zertifikatsdatei von GWN01 und GWN02 steht, können Sie die Berichte für WSH01 anzeigen, wenn Sie sich über GWN01 oder GWN02 beim Administrator Tool anmelden. Wenn GWN01 fehlschlägt, können Sie die Berichte für WSH01 anzeigen, wenn Sie sich über GWN02 beim Administrator Tool anmelden.
- Um ein erfolgreiches Failover zu gewährleisten, wenn ein Gateway-Knoten ausfällt, erzeugen und importieren Sie die SSL-Zertifikate von allen Web-Dienste-Hubs in der Domäne in die Zertifikatsdateien aller Gateway-Knoten in der Domäne.

KAPITEL 16

Knotendiagnostiken

Dieses Kapitel umfasst die folgenden Themen:

- [Knotendiagnostiken - Übersicht, 323](#)
- [Informatica-Netzwerk-Anmeldung, 324](#)
- [Generieren der Knotendiagnostik, 325](#)
- [Knotendiagnostiken herunterladen, 326](#)
- [Knotendiagnostiken hochladen, 326](#)
- [Knotendiagnostik analysieren, 327](#)

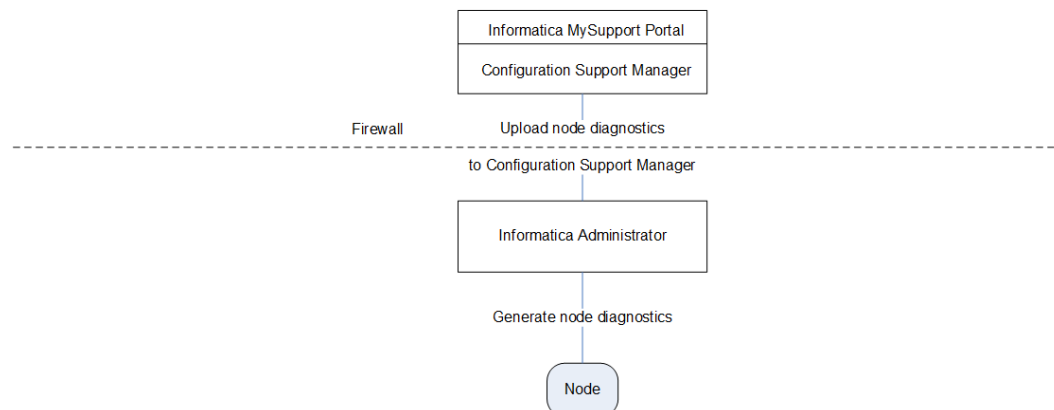
Knotendiagnostiken - Übersicht

Beim Configuration Support Manager handelt es sich um eine webbasierte Anwendung, mit der Sie Informatica-Updates verfolgen und Probleme in Ihrer Umgebung diagnostizieren können.

Sie können umfassende Informationen über Ihre technische Umgebung einsehen und Probleme diagnostizieren, bevor sie kritisch werden.

Generieren Sie aus dem Informatica Administrator heraus eine Knotendiagnose und laden Sie sie im Informatica MySupport-Portal in den Configuration Support Manager. Überprüfen Sie dann im Configuration Support Manager die Knotendiagnose gegen Geschäftsregeln und Empfehlungen.

Die folgende Abbildung zeigt den Arbeitsablauf zum Generieren und Hochladen von Knotendiagnosen:



Führen Sie die folgenden Schritte aus, um die Diagnose zu erstellen und hochzuladen:

1. Melden Sie sich beim Informatica MySupport-Portal an.

2. Generieren Sie eine Knotendiagnose. Der Dienstmanager analysiert die Dienste des Knotens und Knoten erzeugt Knotendiagnosen, die Informationen wie Details zu Betriebssystem, CPU, Datenbank und Patches enthalten.
3. Wahlweise können Sie die Knotendiagnose auf Ihre lokale Festplatte herunterladen.
4. Laden Sie Knotendiagnose in den Configuration Support Manager (ein Web-Anwendung zur Diagnose außerhalb der Firewall). Der Configuration Support Manager ist ein Bestandteil des Informatica MySupport-Portals. Der Dienstmanager stellt die Verbindung zum Configuration Support Manager über das HTTPS-Protokoll her und lädt die Knotendiagnose hoch.
5. Überprüfen Sie die Knotendiagnose im Configuration Support Manager, um Informationen zur Fehlerbehebung für Ihre Umgebung zu finden.

Informatica-Netzwerk-Anmeldung

Um die Knotendiagnostik zum Configuration Support Manager hochzuladen, müssen Sie sich beim Informatica-Netzwerk anmelden. Die Anmeldedaten sind nicht benutzerspezifisch festgelegt. Für alle Benutzer, die auf das Administrator-Tool Zugriff haben, gelten dieselben Anmeldedaten. Registrieren Sie sich bei <http://communities.informatica.com>, wenn Sie die Anmeldedaten für das Kundenportal nicht haben. Sie müssen die Anmeldedaten für das Kundenportal eingeben und diese Daten speichern. Alternativ können Sie die Daten des Kundenportals auch jedes Mal beim Hochladen von Knotendiagnostik in den Configuration Support Manager eingeben. Die Knotendiagnostik können Sie konfigurieren, ohne die Anmeldedaten einzugeben.

Zur Gewährleistung der Anmeldesicherheit müssen Sie sich vom Configuration Support Manager und von der Seite zum Hochladen der Knotendiagnostik im Administrator-Tool abmelden.

- Klicken Sie auf den Link zum Abmelden, um sich beim Configuration Support Manager abzumelden.
- Zum Abmelden von der Seite zum Hochladen, klicken Sie auf **Fenster schließen**.

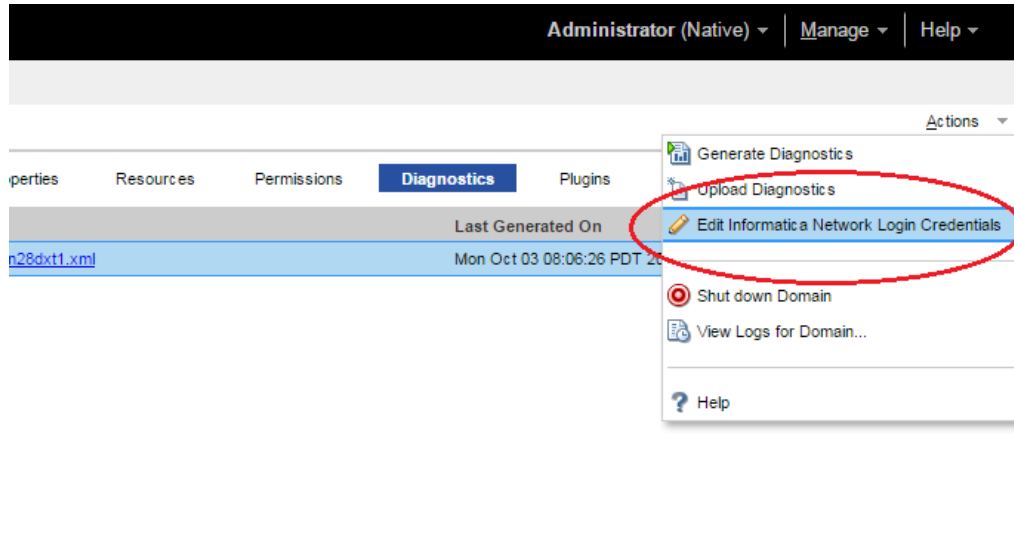
Hinweis: Wenn Sie diese Fenster über die Schließen-Schaltfläche des Webbrowsers schließen, bleiben Sie beim Configuration Support Manager angemeldet. Weitere Benutzer können ohne gültige Anmeldedaten auf den Configuration Support Manager zugreifen.

Anmelden beim Informatica-Netzwerk

Ehe Sie Knotendiagnostiken generieren und hochladen, müssen Sie sich beim Informatica-Netzwerk angemeldet haben.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten** > Ansicht **Dienste und Knoten**.
2. Wählen Sie die Domäne im Domänennavigator aus.
3. Klicken Sie im Inhaltsbereich auf die Ansicht **Diagnostiken**
Eine Liste aller Knoten in der Domäne erscheint.

- Klicken Sie auf das Menü **Aktionen** in der oberen rechten Ecke der Seite, und wählen Sie **Informatica-Netzwerk-Anmeldedaten bearbeiten** aus:



Das Dialogfeld **Informatica-Netzwerk-Anmeldedaten bearbeiten** erscheint.

- Geben Sie die folgenden Anmeldedaten ein:

Feld	Beschreibung
E-Mail-Adresse	E-Mail-Adresse, mit der Sie Ihr Benutzerkonto beim Kundenportal angemeldet haben.
Passwort	Passwort für Ihr Benutzerkonto beim Kundenportal.
Projekt-ID	Einmalige ID, die Ihrem Supportprojekt zugewiesen wurde.

- Klicken Sie auf **OK**.

Generieren der Knotendiagnostik

Wenn Sie Knotendiagnostik generieren, generiert das Administrator Tool die Knotendiagnostik in einer XML-Datei.

Die XML-Datei enthält Details zu den Diensten, Logs, Umgebungsvariablen, Betriebssystemparametern, Systeminformationen und Datenbank-Clients. Worker-Knotendiagnosen enthalten nur Knotenmetadaten. Sie umfassen keine Domänenmetadaten.

- Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten** > Ansicht **Dienste und Knoten**.
- Wählen Sie im Domänen-Navigator die Domäne aus.
- Klicken Sie im Inhaltsbereich auf die Ansicht **Diagnostiken**
Eine Liste aller Knoten in der Domäne erscheint.
- Wählen Sie den Knoten aus.
- Klicken Sie auf **Diagnostikdatei generieren**.

6. Zur Bestätigung, dass Sie Knotendiagnostik generieren möchten, klicken Sie auf **Ja**.

Hinweis: Sie können auch aus dem Menü **Aktionen** auf der Registerkarte **Diagnostik** heraus Diagnostik generieren.

Die Datei `csmagent<Hostname>.xml`, die die Knotendiagnostik enthält, wird unter `INFA_HOME/server/csm/output` erstellt. Die Knotendiagnostik und der Zeitstempel der generierten Datei werden eingeblendet.

7. Um Diagnostik für Ihre Umgebung auszuführen, laden Sie die Datei `csmagent<Hostname>.xml` auf den Configuration Support Manager hoch.

Alternativ können Sie die XML-Datei auch auf Ihr lokales Laufwerk hochladen.

Nachdem Sie erstmals Knotendiagnostik erstellt haben, können Sie sie erneut generieren oder hochladen.

Knotendiagnostiken herunterladen

Nachdem Sie Knotendiagnostiken generiert haben, können Sie die Datei auf Ihr lokales Laufwerk herunterladen.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten** > Ansicht **Dienste und Knoten**.
2. Wählen Sie im Domänen-Navigator die Domäne aus.
3. Klicken Sie im Inhaltsbereich auf die Ansicht **Diagnostiken**
Eine Liste aller Knoten in der Domäne erscheint.
4. Klicken Sie auf den Diagnostikdateinamen des Knotens.
Die Datei wird in einem eigenen Browserfenster angezeigt.
5. Klicken Sie auf **Datei** > **Speichern unter**. Geben Sie dann den Speicherort der Datei an.
6. Klicken Sie auf **Speichern**.
Die XML-Datei ist auf Ihrem lokalen Laufwerk gesichert.

Knotendiagnostiken hochladen

Sie können die Knotendiagnostik über das Administrator Tool in den Configuration Support Manager hochladen. Sie müssen die Anmeldedaten für das Kundenportal eingeben, bevor Sie die Knotendiagnostik hochladen.

Beim Hochladen der Knotendiagnostik können Sie eine Konfiguration im Configuration Support Manager aktualisieren oder erstellen. Erstellen Sie eine Konfiguration, wenn Sie die Knotendiagnostik zum ersten Mal hochladen. Aktualisieren Sie eine Konfiguration, um die aktuellste Diagnose der Konfiguration anzuzeigen. Um aktuellen und vorherigen Knotenkonfigurationen einer bestehenden Konfiguration zu vergleichen, laden Sie die aktuelle Knotendiagnostik als neue Konfiguration hoch.

Hinweis: Wenn Sie keinen Zugang zum Internet haben, können Sie die Datei herunterladen und sie zu einem späteren Zeitpunkt hochladen. Außerdem können Sie die Datei in einer E-Mail an den Informatica Global Customer Support für eine Fehlerbehebung oder ein Upload senden.

1. Klicken Sie im Administrator Tool auf die Registerkarte **Verwalten** > Ansicht **Dienste und Knoten**.

2. Wählen Sie im Domänen-Navigator die Domäne aus.
3. Klicken Sie im Inhaltsbereich auf die Ansicht **Diagnostiken**
Eine Liste aller Knoten in der Domäne erscheint.
4. Wählen Sie den Knoten aus.
5. Generieren Sie eine Knotendiagnose.
6. Klicken Sie auf **Diagnostikdatei auf CSM hochladen**.
Sie können die Knotendiagnose als eine neue Konfiguration oder als Aktualisierung einer bestehenden Konfiguration hochladen.
7. Um eine neue Konfiguration hochzuladen, fahren Sie mit Schritt [10](#) fort.
Um eine Konfiguration zu aktualisieren, wählen Sie **Vorhandene Konfiguration aktualisieren**.
8. Wählen Sie die zu aktualisierende Konfiguration aus der Liste der Konfigurationen aus.
9. Fahren Sie mit Schritt [12](#) fort.
10. Wählen Sie **Als neue Konfiguration hochladen**.
11. Geben Sie die folgenden Konfigurationsdetails ein:

Feld	Beschreibung
Name	Konfigurationsname.
Beschreibung	Konfigurationsbeschreibung.
Typ	Typ des Knotens, wobei es sich um einen der folgenden Typen handeln kann: <ul style="list-style-type: none"> - Produktion - Entwicklung - Test/QA

12. Klicken Sie auf **Jetzt hochladen**.
Nachdem Sie die Knotendiagnostik hochgeladen haben, wechseln Sie zum Configuration Support Manager, um die Knotendiagnostik zu analysieren.
13. Klicken Sie auf **Fenster schließen**
Hinweis: Wenn Sie das Fenster mit der Schaltfläche "Schließen" im Browser schließen, endet die Benutzerauthentifizierungssitzung nicht, und Sie können die Knotendiagnostik nicht mit einem anderen Satz von Anmeldeinformationen im Kundenportal zum Configuration Support Manager hochladen.

Knotendiagnostik analysieren

Zur Analyse der Knotendiagnostik verwenden Sie den Configuration Support Manager.

Verwenden Sie den Configuration Support Manager, um folgende Tasks auszuführen:

- Probleme diagnostizieren, ehe diese kritisch werden.
- Fehlerbehebungsmöglichkeiten erkennen.
- Empfehlungen erkennen, die das Risiko ungeplanter Ausfälle minimieren können.
- Anzeigen der Details zu Ihrer technischen Umgebung.

- Ihre Konfigurationen effizient verwalten.
- Proaktive Alarme per E-Mail und RSS abonnieren.
- Erweiterte Diagnostiken mit einer Vergleichskonfiguration ausführen.

Fehlerbehebungsmöglichkeiten erkennen

Sie können den Configuration Support Manager dazu benutzen, Probleme zu beheben, die während der Operationen aufgetreten sind. Um die Lösung von Supportthemen zu beschleunigen, können Sie Knotendiagnostiken generieren und in den Configuration Support Manager hochladen. Die Knotendiagnostiken lassen sich im Configuration Support Manager analysieren und liefern eine Lösung für Ihr Problem.

Angenommen, Sie führen eine Sorter-Sitzung aus, die große Datenmengen verarbeitet, und Sie bemerken, dass es zu einem Datenverlust kommt. Generieren Sie Knotendiagnostiken und laden Sie diese in den Configuration Support Manager hoch. Wenn Sie die Knotendiagnostiken nach Fehlerbehebungsalarmen durchsuchen, stoßen Sie auf die Fehlerbehebung EBF178626, die für diesen Fall verfügbar ist. Wenden Sie EBF178626 an und führen Sie die Sitzung erneut aus. Alle Daten werden erfolgreich geladen.

Identifizieren von Empfehlungen

Der Configuration Support Manager hilft Ihnen, Probleme in Ihrem Umfeld zu vermeiden. Bei Problemen, die entstehen, nachdem Sie Änderungen an den Knoteneigenschaften vorgenommen haben, können Sie anhand des Vergleichs der verschiedenen Knotendiagnostiken im Configuration Support Manager eine Fehlersuche durchführen. Der Configuration Support Manager hilft Ihnen außerdem, Empfehlungen oder Aktualisierungen zu finden, mit denen Sie die Knotenleistung verbessern können.

So können Sie zum Beispiel den Knotenspeicher auf die Kapazität für ein größeres Datenvolumen upgraden. Sie generieren Knotendiagnostik und laden sie auf den Configuration Support Manager hoch. Wenn Sie die Diagnostik auf Betriebssystemwarnungen überprüfen, finden Sie die Empfehlungen zum Steigern der Gesamt-Swap-Speicherkapazität des Knotens auf die doppelte Menge des Knotenspeichers, die Sie zur Leistungsoptimierung verwenden können. Erhöhen Sie nach der Empfehlung des Configuration Support Manager die Swap-Speicherkapazität und verhindern Sie auf diese Weise die Verschlechterung der Leistung.

Tipp: Laden Sie regelmäßig Knotendiagnostik auf den Configuration Support Manager hoch und überprüfen Sie die Knotendiagnostik, um die Effizienz Ihrer Umgebung zu gewährleisten.

KAPITEL 17

Informationen zur Globalisierung

Dieses Kapitel umfasst die folgenden Themen:

- [Globalisierung - Übersicht, 329](#)
- [Gebietsschemata, 331](#)
- [Datenverschiebungsmodi, 332](#)
- [Codepages - Übersicht, 334](#)
- [Codepage-Kompatibilität, 336](#)
- [Codepage-Validierung, 344](#)
- [Entspannte Codepage-Validierung, 345](#)
- [PowerCenter Codepage-Umwandlung, 347](#)
- [Fallstudie: ISO 8859-1 Datenverarbeitung, 348](#)
- [Fallstudie: Verarbeiten von Unicode UTF-16LE Daten, 351](#)

Globalisierung - Übersicht

Informatica ist in der Lage, Daten in verschiedenen Sprachen zu verarbeiten. Einige Sprachen erfordern Einzelbytedaten, während andere Mehrbytedaten benötigen. Für die korrekte Datenverarbeitung in Informatica müssen Sie folgende Parameter einrichten:

- **Gebietsschema** Bei Informatica müssen die Einstellungen für das Gebietsschema auf Computern, die auf Informatica-Anwendungen zugreifen, mit den Codepages in der Domäne kompatibel sein. Es kann vorkommen, dass Sie die Einstellungen für das Gebietsschema ändern müssen. Das Gebietsschema gibt die Sprache an, das Territorium, die Zeichensatz-Verschlüsselung und die Sortierreihenfolge.
- **Datenverschiebungsmodus** Der PowerCenter Integration Service kann Einzelbyte- oder Multibytedaten verarbeiten und sie in Targets hineinschreiben. Zur Verarbeitung von Einzelbyte-Daten ist der ASCII-Datenverschiebungsmodus vorgesehen. Mehrbytedaten erfordern den Unicode-Datenverschiebungsmodus.
- **Codepages** Codepages enthalten die Verschlüsselung für die Angabe von Zeichen in einem Set aus einer oder mehreren Sprachen. Sie wählen eine Codepage basierend auf dem Typ der Zeichendaten, die Sie verarbeiten möchten. Um die präzise Datenverschiebung zu gewährleisten, müssen Sie dafür sorgen, dass die Codepages untereinander für die Informatica- und die Umgebungskomponenten kompatibel sind. Anhand der Codepages wird zwischen US-ASCII (7-Bit-ASCII-), ISO 8859-1 (8-Bit-ASCII-) und Multibyte-Zeichen unterschieden.

Damit die Daten Ihre Umgebung präzise passieren, müssen folgende Komponenten aufeinander abgestimmt sein:

- Codepage der Domänenkonfigurationsdatenbank
- Die Gebietsschema-Einstellungen und die Codepage des Administrator Tools
- Der Datenverschiebungsmodus für den PowerCenter Integration Service
- Die Codepage für jeden PowerCenter Integration Service Prozess
- Codepage des PowerCenter Client
- PowerCenter Repository Codepage
- Die Codepages der Quell- und der Target-Datenbank
- Codepage für Metadata Manager-Repository.

Sie können den PowerCenter Integration Service für RELAX-Validierung der Codepages konfigurieren. Bei Relax-Validierung sind die Einschränkungen für Quell- und Target-Codepages aufgehoben.

Unicode

Der Unicode-Standard ist die Arbeit des Unicode-Konsortiums, einem internationalen Gremium, das den Austausch von Daten in allen Sprachen fördert. Der Unicode-Standard wurde entwickelt, um jede beliebige Sprache zu unterstützen, gleich wie viele Bytes jedes Zeichen in dieser Sprache benötigen mag. Derzeit unterstützt er alle gängigen Sprachen und bietet eingeschränkte Unterstützung für andere, weniger verbreitete Sprachen. Das Unicode-Konsortium erweitert den Unicode-Standard kontinuierlich mit neuen Zeichencodierungen. Weitere Informationen zum Unicode-Standard finden Sie unter <http://www.unicode.org>.

Der Unicode-Standard umfasst mehrere Zeichensätze. Informatica nutzt die folgenden Unicode-Standards:

- UCS-2 (Universal Character Set, double-byte). Ein Zeichensatz, bei dem jedes verwendete Zeichen zwei Byte nutzt.
- UTF-16LE (Unicode Transformation Format) Ein Codierungsformat, bei dem jedes Zeichen zwischen einem und vier Byte nutzen kann.
- UTF-16 (Unicode Transformation Format) Ein Codierungsformat, bei dem jedes Zeichen zwischen zwei und vier Byte nutzen kann.
- UTF-32 (Unicode Transformation Format) Ein Codierungsformat, bei dem jedes Zeichen vier Byte verwendet.
- GB18030 Ein Unicode-Codierungsformat, das von der chinesischen Regierung definiert wurde, bei dem jedes Zeichen zwischen einem und vier Byte nutzen kann.

Informatica ist eine Unicode-Anwendung. PowerCenter Client, PowerCenter Integration Service und Data Integration Service nutzen intern UCS-2. Der PowerCenter Client konvertiert Benutzereingaben von einer beliebigen Sprache in UCS-2 und wandelt sie vor dem Schreiben in das PowerCenter-Repository von UCS-2 um. Der PowerCenter Integration Service und der Data Integration Service konvertieren die Quelldaten vor der Verarbeitung in UCS-2 und wandelt sie nach der Verarbeitung von UCS-2 um. PowerCenter Client, Model Repository, PowerCenter Integration Service und Data Integration Service unterstützen UTF-16LE. Sie können mit Informatica Daten in einer beliebigen Sprache verarbeiten.

Mit einem Unicode PowerCenter Repository arbeiten

Die PowerCenter Repository-Codepage ist die Codepage der Daten im PowerCenter Repository. Sie wählen die PowerCenter Repository-Codepage aus, wenn Sie ein PowerCenter Repository erstellen oder aktualisieren. Wenn die PowerCenter Repository-Codepage UTF-16LE ist, können Sie ein PowerCenter Repository erstellen, das die Codepage UTF-16LE verwendet.

Die Domänenkonfigurationsdatenbank verwendet die Codepage UTF-16LE. Wenn Sie Metadaten in mehreren Sprachen, wie Chinesisch, Japanisch und Arabisch speichern möchten, müssen Sie die Codepage UTF-16LE für alle Dienste in dieser Domäne verwenden.

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

Verwenden Sie die folgenden Richtlinien, wenn Sie UTF-16LE als PowerCenter Repository-Codepage benutzen:

- Die Datenbankcodepage des PowerCenter Repository muss ebenfalls UTF-16LE sein.
- Die PowerCenter Repository-Codepage muss eine Obermenge der Codepages des PowerCenter Client und des PowerCenter Integration Service-Prozesses sein.
- In den UCS-2-Zeichensatz können Sie jedes beliebige Zeichen eingeben. Zum Beispiel: Sie können deutsche, chinesische und englische Metadaten in einem UTF-16LE-fähigen PowerCenter Repository speichern.
- Installieren Sie die Sprachen und Schriftarten auf der Maschine des PowerCenter Client. Wenn Sie ein UTF-16LE PowerCenter Repository verwenden, möchten Sie die Maschinen des PowerCenter Client eventuell befähigen, mehrere Sprachen anzuzeigen. Standardmäßig zeigen die PowerCenter Clients den Text in dem Sprachsatz der Gebietsschemaeinstellungen an. Verwenden Sie in der Systemsteuerung von Windows die Einstellungen unter "Region und Sprache", um den Maschinen der PowerCenter Clients Sprachgruppen hinzuzufügen.
- Sie können den Windows Input Method Editor (IME) dazu verwenden, Multibyte-Zeichen aus jeder beliebigen Sprache einzugeben, ohne jeweils eine Windows-Version für diese spezielle Sprache ausführen zu müssen.
- Wählen Sie für den Prozess des PowerCenter Integration Service eine Codepage aus, die alle Metadaten des PowerCenter Repository korrekt verarbeiten kann. Die Codepage des Prozesses des PowerCenter Integration Service muss eine Untermenge der PowerCenter Repository-Codepage sein. Wenn der PowerCenter Integration Service mehrere Dienstprozesse hat, stellen Sie sicher, dass die Codepages für alle Prozesse des PowerCenter Integration Service eine Untermenge der PowerCenter Repository-Codepage sind. Wenn Sie den Prozess des PowerCenter Integration Service unter Windows ausführen, muss die Codepage des Prozesses des PowerCenter Integration Service dieselbe sein wie die Codepage für die Gebietsschemaeinstellungen des Systems oder des Benutzer. Wenn Sie den Prozess des PowerCenter Integration Service unter UNIX ausführen, verwenden Sie die Codepage UTF-16LE für den Prozess des PowerCenter Integration Service.

Gebietsschemata

Jede Maschine hat ein Gebietsschema. Ein Gebietsschema ist eine Zusammenfassung von Voreinstellungen, die zur Benutzerumgebung gehört, z. B. die Eingabesprache, das Tastaturlayout, die Art der Datensortierung und das Währungs- bzw. Datumsformat. Informatica verwendet auf jeder Maschine Gebietsschemaeinstellungen.

Unter Windows können Sie folgende Gebietsschemaeinstellungen vornehmen:

- Systemschema. Hierzu gehören die Sprache, die Codepages und die erforderlichen Bitmap Font-Dateien, die als Standard für das System verwendet werden.
- Benutzerschema. Hierzu gehören die Standardformate für die Anzeige des Datums, der Uhrzeit, der Währung und des Zahlenformats.

- Eingabeschema. Hierzu gehört die Eingabemethode, z. B. Tastatur, der Systemsprache.

Weitere Informationen zum Konfigurieren der Gebietsschemaeinstellungen unter Windows finden Sie in der Dokumentation zu Windows.

Systemgebietsschema

Das Systemgebietsschema wird auch als das Systemstandardgebietsschema bezeichnet. Es legt fest, welche ANSI- und OEM-Codepages sowie Bitmap-Font-Dateien als Standardwerte für das System verwendet werden. Das Systemgebietsschema enthält die Einstellung der Sprache, was auch festlegt, in welcher Sprache Text auf der Benutzeroberfläche, einschließlich in Dialogfeldern und Fehlermeldungen angezeigt wird. Eine Meldungskatalogdatei definiert die Sprache, in der Meldungen angezeigt werden. Standardmäßig verwendet das Gerät die für das Systemgebietsschema festgelegte Sprache für alle Prozesse, sofern Sie die Sprache nicht für einen bestimmten Prozess überschreiben.

Das Systemgebietsschema ist auf Ihrem System bereits festgelegt und Sie brauchen die Einstellungen eventuell nicht zu ändern, um Informatica auszuführen. Wenn Sie das Systemgebietsschema konfigurieren müssen, konfigurieren Sie das Gebietsschema auf einem Windows-Rechner im Dialogfeld "Regionale Einstellungen". Unter UNIX geben Sie das Gebietsschema in der Umgebungsvariable LANG an.

Benutzerschema

Das Benutzerschema zeigt Datum, Uhrzeit, Währung und Zahlenformate für jeden Benutzer an. Sie können verschiedene Benutzerschemata auf einer einzigen Maschine angeben. Erstellen Sie ein Benutzerschema, wenn Sie auf einer Maschine mit Daten arbeiten, die eine andere Sprache als das Betriebssystem verwenden. Zum Beispiel: Sie sind ein englischer Benutzer, der in Hongkong auf einem chinesischen Betriebssystem arbeitet. Stellen Sie Englisch als Benutzerschema ein, um englische Standards bei Ihrer Arbeit in Hongkong zu verwenden. Wenn Sie ein neues Benutzerkonto erstellen, verwendet die Maschine ein Standardbenutzerschema.. Sie können diese Standardeinstellung ändern, wenn das Konto erstellt ist.

Eingabe-Gebietsschema

Ein Eingabe-Gebietsschema gibt das Tastatur-Layout einer bestimmten Sprache an. Sie haben die Möglichkeit, auf einem Windows-Computer ein Eingabe-Gebietsschema für die Darstellung von Zeichen einer bestimmten Sprache einzustellen.

Mit dem Windows Input Method Editor (IME) können Sie Multibyte-Zeichen einer beliebigen Sprache eingeben, ohne die spezielle Windows-Version für diese Sprache ausführen zu müssen. Beispiel: Sie arbeiten auf einem englischen Betriebssystem und müssen Text in Chinesisch eingeben. In diesem Fall können Sie mit dem IME das Eingabe-Gebietsschema auf Chinesisch einstellen und brauchen die chinesische Windows-Version nicht zu installieren. Möglicherweise möchten Sie einen IME verwenden, um Multibyte-Zeichen in ein PowerCenter-Repository einzugeben, das mit UTF-16LE arbeitet.

Datenverschiebungsmodi

Der Datenverschiebungsmodus ist eine Option des PowerCenter Integration Service, die auf der Basis der Daten gewählt wird, die verschoben werden sollen: Single-Byte oder Multibyte-Daten. Welchen Datenverschiebungsmodus Sie wählen, hängt von folgenden Faktoren ab:

- Den Anforderungen, die Single-Byte oder Multibyte-Metadaten im PowerCenter Repository zu speichern.

- Den Anforderungen, auf die Quelldaten zuzugreifen, die die Single-Byte oder Multibyte-Zeichendaten enthalten.
- Künftige Notwendigkeiten für Single-Byte oder Multibyte-Daten.

Der gewählte Datenverschiebungsmodus hat darauf Einfluss, wie der PowerCenter Integration Service die Beziehungen zur Sitzungs-Codepage und die Codepage-Validierung erzwingt. Er kann auch die Performance beeinflussen. Anwendungen können Single-Byte-Zeichen schneller als Multibyte-Zeichen verarbeiten.

Zeichendatenverschiebungs-Modus

Der PowerCenter Integration Service läuft in den folgenden Modus.

- ASCII (American Standard Code for Information Interchange). Die US-ASCII Codeseite enthält einen Satz von 7-Bit-ASCII-Zeichen und ist ein Subset von anderen Zeichen-Sets. Wenn der PowerCenter Integration Service im ASCII-Datenverschiebungsmodus läuft, erfordert jedes Zeichen ein Byte.
- Unicode. Der Universal-Zeichenverschlüsselungsstandard, der alle Sprachen unterstützt. Wenn der PowerCenter Integration Service im Unicode-Datenverschiebungs-Modus läuft, ordnet er bis zu zwei Byte pro Zeichen zu. Führen Sie den PowerCenter Integration Service im Unicode-Modus aus, wenn die Quelle Multibyte-Daten enthält.

Tipp: Sie können auch den ASCII- oder den Unicode-Datenverschiebungs-Modus nutzen, wenn die Quelle 8-Bit-ASCII-Daten enthält. Beim Verarbeiten von Daten im Unicode-Datenverschiebungs-Modus ordnet der PowerCenter Integration Service ein zusätzliches Byte zu. Zur Leistungssteigerung nutzen Sie den ASCII-Datenverschiebungs-Modus. Wenn die Quelle zum Beispiel Zeichen der ISO 8859-1 Codeseite enthält, verwenden Sie die ASCII-Datenverarbeitung.

Die von Ihnen gewählte Datenverschiebung beeinflusst die Anforderungen der Codeseite. Vergewissern Sie sich, dass die Codeseiten kompatibel sind.

ASCII-Datenverschiebungsmodus

Im ASCII-Modus verarbeitet der PowerCenter Integration Service Single-Byte Zeichen und führt keine Codepage-Konvertierungen durch. Wenn Sie den PowerCenter Integration Service im ASCII-Modus ausführen, erzwingt er keine Sitzungscodepage-Beziehungen.

Unicode-Datenverschiebungsmodus

Im Unicode-Modus erkennt der PowerCenter Integration Service die Multibyte-Zeichendaten und weist jedem Zeichen bis zu zwei Bytes zu. Der PowerCenter Integration Service führt eine Codepage-Konvertierung von Quellen und Targets durch. Wenn Sie für den PowerCenter Integration Service den Unicode-Datenverschiebungsmodus einstellen, verwendet er einen Unicode-Zeichensatz, um die Zeichen in einer angegebenen Codepage zu verarbeiten, zum Beispiel Shift-JIS oder UTF-16LE.

Wenn Sie den PowerCenter Integration Service im Unicode-Modus ausführen, erzwingt er Sitzungscodepage-Beziehungen.

Ändern der Datenverschiebungsmodi

Den Datenverschiebungsmodus können Sie in den Eigenschaften des PowerCenter Integration Service im Administrator Tool ändern. Nachdem Sie den Datenverschiebungsmodus geändert haben, wird der PowerCenter Integration Service im neuen Datenverschiebungsmodus ausgeführt, wenn Sie ihn das nächste Mal starten. Ändert sich der Datenverschiebungsmodus, ändert sich auch die Bearbeitung von Zeichendaten durch den PowerCenter Integration Service. Um die Entstehung von Dateninkonsistenzen in Ihren Target-Tabellen zu vermeiden, führt der PowerCenter Integration Service zusätzliche Prüfungen auf Sitzungen durch, die Sitzungs-Cachespeicher und -Dateien wiederverwenden.

Die folgende Tabelle beschreibt, wie der PowerCenter Integration Service Sitzungsdateien und Cachespeicher behandelt, nachdem Sie den Datenverschiebungsmodus geändert haben:

Sitzungsdatei oder - Cachespeicher	Zeit der Erstellung oder Nutzung	Verhalten des PowerCenter Integration Service nach Änderung des Datenverschiebungsmodus
Sitzungs-Logdatei (*.log)	Bei jeder Sitzung.	Keine Verhaltensänderung. Erstellt ein neues Sitzungs-Log für jede Sitzung mit der Codepage des PowerCenter Integration Service Prozesses.
Arbeitsablauf-Log	Bei jedem Arbeitsablauf.	Keine Verhaltensänderung. Erstellt für jeden Arbeitsablauf anhand der Codepage des PowerCenter Integration Service Prozesses eine neue Arbeitsablauf-Logdatei.
Abgelehnte Datei (*.bad)	Bei jeder Sitzung.	Keine Verhaltensänderung. Hängt mittels der Codepage des PowerCenter Integration Service Prozesses abgelehnte Daten an die vorhandene Ablehnungsdatei an.
Ausgabedatei (*.out)	Bei Sitzungen, die in eine Einfachdatei schreiben.	Keine Verhaltensänderung. Erstellt anhand der Target-Codepage eine neue Ausgabedatei für jede Sitzung.
Indikatordatei (*.in)	Bei Sitzungen, die in eine Einfachdatei schreiben.	Keine Verhaltensänderung. Erstellt für jede Sitzung eine neue Indikatordatei.
Inkrementelle Aggregationsdateien (*.idx, *.dat)	Sitzungen, bei denen inkrementelle Aggregation aktiviert ist.	<p>Wenn Dateien entfernt oder gelöscht werden, erstellt der PowerCenter Integration Service neue Dateien.</p> <p>Werden Dateien nicht verschoben oder gelöscht, schlägt die Sitzung des PowerCenter Integration Service fehl und es wird folgende Fehlermeldung ausgegeben.</p> <pre>SM_7038 Aggregate Error: ServerMode: [server data movement mode] and CachedMode: [data movement mode that created the files] mismatch.</pre> <p>Verschieben oder Löschen von Dateien, die mit einer anderen Codepage erstellt wurden.</p>
Unbenannte persistente Lookup-Dateien (*.idx, *.dat)	Sitzungen mit einer Lookup-Umwandlung, die für einen unbenannten persistenten Lookup-Cachespeicher konfiguriert wurden.	Baut den persistenten Lookup-Cachespeicher neu auf.
Mit Namen versehene persistente Lookup-Dateien (*.idx, *.dat)	Sitzungen mit einer Lookup-Umwandlung, die für einen mit Namen versehenen persistenten Lookup-Cachespeicher konfiguriert wurden.	<p>Wenn Dateien entfernt oder gelöscht werden, erstellt der PowerCenter Integration Service neue Dateien.</p> <p>Werden keine Dateien verschoben oder gelöscht, lässt der PowerCenter Integration Service die Sitzung fehlschlagen.</p> <p>Verschieben oder Löschen von Dateien, die mit einer anderen Codepage erstellt wurden.</p>

Codepages - Übersicht

Eine Codepage enthält die Kodierung zur Angabe von Zeichen in einer oder mehreren Sprachen. Eine Kodierung ist die Zuordnung einer Zahl zu einem Zeichen im Zeichensatz. Codepages dienen der Erkennung

von Daten in unterschiedlichen Sprachen. Beispiel: Wenn Sie ein Mapping für die Verarbeitung japanischer Daten anlegen, müssen Sie eine japanische Codepage für die Quelldaten auswählen.

Wenn Sie eine Codepage auswählen, bezieht sich das Programm oder die Anwendung, für das Sie die Codepage festlegen, auf einen bestimmten Datensatz, der die von der Anwendung erkannten Zeichen beschreibt. Dies hat Auswirkungen auf die Art und Weise, in der die Anwendung Zeichendaten speichert, empfängt und sendet.

Die meisten Computer verwenden eine der folgenden Codepages:

- US-ASCII (7-Bit ASCII)
- MS Latin1 (MS 1252) für Windows-Betriebssysteme
- Latin1 (ISO 8859-1) für UNIX-Betriebssysteme
- IBM EBCDIC US English (IBM037) für Mainframe-Systeme

Die US-ASCII-Codepage enthält alle 7-Bit-ASCII-Zeichen und ist die grundlegendste aller Codepages mit Unterstützung für US-Englisch. Die US-ASCII-Codepage ist nicht mit anderen Codepages kompatibel. Wenn Sie den PowerCenter Client, den PowerCenter Integration Service oder ein PowerCenter-Repository auf einem US-ASCII-System installieren, müssen Sie alle Komponenten auf US-ASCII-Systemen installieren und den PowerCenter Integration Service im ASCII-Modus ausführen.

MS Latin1 und Latin1 unterstützen beide Englisch und die meisten westeuropäischen Sprachen und sind miteinander kompatibel. Wenn Sie den PowerCenter Client, den PowerCenter Integration Service oder ein PowerCenter-Repository auf einem System installieren, das eine dieser Codepages verwendet, können Sie die übrigen Komponenten auf einem beliebigen Computer mit MS Latin1 oder Latin1 Codepages installieren.

Die IBM EBCDIC-Codepage können Sie für den PowerCenter Integration Service Prozess verwenden, wenn Sie ihn auf einem Mainframe-System installieren. Den PowerCenter Client oder das PowerCenter-Repository können Sie nicht auf Mainframe-Systemen installieren. Daher können Sie die Codepage IBM EBCDIC nicht für Installationen mit PowerCenter Client oder PowerCenter Repository nutzen.

UNIX Codepages

In den Vereinigten Staaten haben die meisten UNIX-Betriebssystemen mehr als eine Codepage installiert und verwenden die ASCII-Codepage standardmäßig. Wenn Sie PowerCenter in einer reinen ASCII-Umgebung ausführen möchten, können Sie die ASCII-Codepage verwenden und den PowerCenter Integration Service im ASCII-Modus ausführen.

UNIX-Systeme ermöglichen es Ihnen, die Codepage zu ändern, indem Sie die LANG, LC_CTYPE oder LC_ALL Umgebungsvariable ändern. Angenommen, Sie möchten die Codepage ändern, die ein AIX-Computer benutzt. Verwenden Sie den folgenden Befehl in der C-Shell, um Ihre Umgebung anzuzeigen:

```
locale
```

Daraus ergibt sich die folgende Ausgabe, wobei "C" "ASCII" bedeutet:

```
LANG="C"
LC_CTYPE="C"
LC_NUMERIC="C"
LC_TIME="C"
LC_ALL="C"
```

Um die Sprache in Englisch zu ändern und das System die Latin1-Codepage verwenden zu lassen, können Sie den folgenden Befehl verwenden:

```
setenv LANG en_US.iso88591
```

Wenn Sie das Gebietsschema erneut überprüfen, wurde es so geändert, dass nun Latin1 (ISO 8859-1) verwendet wird:

```
LANG="en_US.iso88591"
LC_CTYPE="en_US.iso88591"
```

```
LC_NUMERIC="en_US.iso88591"  
LC_TIME="en_US.iso88591"  
LC_ALL="en_US.iso88591"
```

Weitere Informationen über das Ändern des Gebietsschemas oder der Codepage in einem UNIX-System, finden Sie in der UNIX-Dokumentation.

Windows Codepages

Das Betriebssystem Windows basiert auf Unicode, aber es zeigt nicht die Codepage an, die vom Betriebssystem in den Umgebungseinstellungen verwendet wird. Sie können jedoch eine fundierte Vermutung anstellen, denn die Codepage basiert meist auf dem Land, in dem Sie das System erworben haben und dem dort üblichen Sprachsystem.

Wenn Sie Windows in den Vereinigten Staaten erworben haben und Englisch als Eingabe- und Anzeigesprache verwenden, nutzt Ihr Betriebssystem standardmäßig die Codepage MS Latin1 (MS1252). Wenn Sie jedoch weitere Anzeige- oder Eingabesprachen von der Windows-Installations-CD installiert haben und diese Sprachen benutzen, verwendet das Betriebssystem eventuell eine andere Codepage.

Um weitere Informationen zu der Standardcodepage für Ihr Windows-Betriebssystem zu erhalten, kontaktieren Sie bitte Microsoft.

Auswählen einer Codepage

Wählen Sie die Codeseiten basierend auf den Zeichendaten, die Sie in Mappings verwenden. Zeichendaten können durch Zeichenmodi dargestellt werden, die auf der Zeichengröße basieren. Die Zeichengröße gibt den Speicherplatz an, den ein Zeichen in der Datenbank benötigt. Die verschiedenen Zeichengrößen sind folgendermaßen definiert:

- Einfaches Byte. Ein Zeichen, das als eindeutige Zahl zwischen 0 und 255 dargestellt wird. Ein Byte entspricht acht Bit. ASCII-Zeichen sind aus einem Byte bestehende Zeichen.
- Doppeltes Byte. Ein Zeichen bestehend aus zwei Byte bzw. 16 Bit, dargestellt als eine eindeutige Zahl größer als 256. Viele asiatische Sprachen, wie Chinesisch, haben Zeichen, die aus doppelten Bytes bestehen.
- Multibyte. Ein Zeichen bestehend aus zwei oder mehr Byte, dargestellt als eindeutige Zahl größer als 256. Viele asiatische Sprachen, wie Chinesisch, haben Multibyte-Zeichen.

Codepage-Kompatibilität

Die Kompatibilität der Codepage ist unabdingbar für das präzise Verschieben, wenn der PowerCenter-Integrationsdienst im Unicode-Datenverschiebungsmodus ausgeführt wird.

Eine Codepage kann mit einer anderen Codepage kompatibel oder eine Teilmenge bzw. eine einer anderen Codepage übergeordnete Menge sein:

- Kompatibel. Zwei Codepages sind kompatibel, wenn die Zeichen der beiden Codepages virtuell identisch sind. Beispiel: Die Codepages JapanEUC und JIPSE enthalten identische Zeichen und sind miteinander kompatibel. Das PowerCenter Repository und der PowerCenter-Integrationsdienst-Prozess können jeweils eine dieser Codepages nutzen und ohne Datenverlust Daten hin- und her schieben.
- Übergeordnete Menge. Eine Codepage ist eine übergeordnete Menge einer anderen Codepage, wenn Sie alle in der anderen Codepage verschlüsselten Zeichen und weitere Zeichen enthält, die nicht auf der

anderen Codepage verschlüsselt sind. Beispiel: MS Latin1 ist eine übergeordnete Menge von US-ASCII, weil es alle Zeichen der US-ASCII-Codepage enthält.

Hinweis: Bei Informatica ist eine Codepage eine sich selbst und allen anderen kompatiblen Codepages übergeordnete Menge.

- Teilmenge. Eine Codepage ist eine Teilmenge einer anderen Codepage, wenn alle Zeichen auf der Codepage ebenfalls auf der anderen Codepage verschlüsselt sind. Beispiel: US-ASCII ist eine Teilmenge von MS Latin1, weil alle Zeichen auf der US-ASCII-Codepage auch auf der MS Latin1 Codepage verschlüsselt sind.

Um die präzise Datenverschiebung zu gewährleisten, muss die Target-Codepage eine übergeordnete Menge der Quell-Codepage sein. Ist die Target-Codepage keine der Quell-Codepage übergeordnete Menge, kann der PowerCenter-Integrationsdienst möglicherweise nicht alle Zeichen verarbeiten. Dies führt zu fehlerhaften oder fehlenden Daten. Beispiel: Latin1 ist eine übergeordnete Menge von US-ASCII. Wenn Sie Latin1 als Quell-Codepage und US-ASCII als Target-Codepage auswählen, könnten Sie Zeichendaten verlieren, sofern die Quelle Zeichen enthält, die nicht in US-ASCII enthalten sind.

Beim Installieren oder Upgraden eines PowerCenter-Integrationsdienstes zum Ausführen im Unicode-Modus müssen Sie die Kompatibilität der Codepages zwischen Domänenkonfigurations-Datenbank, Administrator Tool, PowerCenter Clients, PowerCenter-Integrationsdienst-Prozessknoten, PowerCenter-Repository, Metadata Manager Repository und den Host-Computern von *pmrep* und *pmcmd* gewährleisten. Im Unicode-Modus erzwingt der PowerCenter-Integrationsdienst die Codepage-Kompatibilität zwischen PowerCenter Client und PowerCenter Repository sowie zwischen PowerCenter-Integrationsdienst-Prozess und PowerCenter-Repository. Beim Ausführen des PowerCenter-Integrationsdienstes im Unicode-Modus müssen die den Sitzungen zugeordneten Codepages außerdem die richtigen Beziehungen aufweisen:

- Für jede Quelle in der Sitzung muss die Quell-Codepage eine Teilmenge der Target-Codepage sein. Der PowerCenter-Integrationsdienst erfordert keine Codepage-Kompatibilität zwischen Quelle und PowerCenterIntegrationsdienst-Prozess oder zwischen PowerCenter-Integrationsdienst-Prozess und Target.
- Enthält die Sitzung eine Lookup- oder gespeicherte Prozedurumwandlung, muss die Datenbank oder Datei-Codepage eine Teilmenge des Target, das Daten aus der Lookup- oder gespeicherten Prozedurumwandlung aufnimmt und eine übergeordnete Menge der Quelle sein, die Daten an die Lookup- oder gespeicherte Prozedurumwandlung übergibt.
- Enthält die Sitzung eine externe Prozedur oder benutzerdefinierte Umwandlung, muss die Prozedur Daten in einer Codepage übergeben, die eine Teilmenge der Target-Codepage für Targets ist, die Daten von der externen Prozedur oder benutzerdefinierten Umwandlungen entgegennehmen.

Informatica nutzt Codepages für folgende Komponenten:

- Domänenkonfigurationsdatenbank. Die Domänenkonfigurations-Datenbank muss mit den Codepages von PowerCenter Repository und Metadata Manager Repository kompatibel sein.
- Administrator Tool. Die Dateneingabe in das Administrator Tool ist in einer beliebigen Sprache möglich.
- PowerCenter Client. Die Eingabe von Metadaten in den PowerCenter-Client ist in einer beliebigen Sprache möglich.
- PowerCenter-Integrationsdienst-Prozess. Der PowerCenter-Integrationsdienst kann Daten in ASCII-Modus oder Unicode-Modus verschieben. Als Datenverschiebungsmodus voreingestellt ist ASCII, wobei 7-Bit-ASCII- bzw. 8-Bit-ASCII-Zeichendaten übergeben werden. Zum Übergeben von Mehrbyte-Zeichendaten aus Quellen in Targets muss der Unicode-Datenverschiebungsmodus eingesetzt werden. Beim Ausführen des PowerCenter-Integrationsdienst im Unicode-Modus nutzt dieser bis zu drei Byte für jedes zu verschiebende Zeichen und führt zur Gewährleistung der Datenintegrität zusätzliche Prüfungen auf Sitzungsebene durch.

- PowerCenter Repository. Das PowerCenter Repository kann Daten in beliebigen Sprachen speichern. Zum Speichern von Mehrbyte-Daten im PowerCenter-Repository können Sie die UTF-8-Codepage nutzen. Die Codepage für das PowerCenter-Repository ist dieselbe wie die Datenbank-Codepage.
- Metadata Manager Repository. Im Metadata Manager Repository können Daten in beliebiger Sprache gespeichert werden. Zum Speichern von Mehrbyte-Daten im Repository können Sie die UTF-8-Codepage für das Metadata Manager Repository verwenden. Die Codepage für das Repository ist dieselbe wie für die Datenbank-Codepage.
- Quellen und Targets. Die Quellen und Targets speichern Daten in einer oder mehreren Sprachen. Sie benutzen die Codepages für die Angabe der Zeichenarten in den Quellen und Targets.
- PowerCenter-Befehlszeilenprogramme. Sie müssen gewährleisten, dass die Codepage für *pmrep* eine Teilmenge der PowerCenter Repository Codepage und die Codepage für *pmcmd* eine Teilmenge der PowerCenter-Integrationsdienst-Prozess Codepage ist.

Die meisten Datenbankserver nutzen zwei Codepages: eine Client-Codepage für die Aufnahme von Daten von Client-Anwendungen und eine Server-Codepage zum Speichern der Daten. Wenn der Datenbankserver läuft, konvertiert er Daten zwischen den beiden Codepages, wenn diese unterschiedlich sind. Bei dieser Datenbankkonfiguration interagiert der PowerCenter-Integrationsdienst-Prozess mit der Datenbank-Client-Codepage. Daher müssen Codepages, die der PowerCenter-Integrationsdienst-Prozess verwendet, wie die Codepages für PowerCenter-Repository, Quelle oder Target, identisch mit der Codepage des Datenbank-Client sein. Die Datenbank-Client-Codepage ist normalerweise identisch mit der Codepage des Betriebssystems, auf dem der PowerCenter-Integrationsdienst-Prozess ausgeführt wird. Die Datenbank-Client-Codepage ist eine Teilmenge der Datenbankserver-Codepage.

Ausführliche Informationen über bestimmte Datenbank-Client- und Server-Codepages finden Sie in Ihrer Datenbank-Dokumentation.

Codepage der Domänenkonfigurationsdatenbank

Die Domänen-Konfigurationsdatenbank muss mit den Codepages des PowerCenter Repository, des Metadata Manager Repository und des Model Repository, kompatibel sein.

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

Codepage des Administrator Tools

Das Administrator Tool kann auf jedem Knoten in einer Informatica-Domäne ausgeführt werden. Als Codepage für das Administrator Tool wird die Codepage des Betriebssystems des Knotens verwendet. Jeder Knoten in der Domäne muss dieselbe Codepage verwenden.

Die Codepage des Administrator Tools muss folgende Kriterien erfüllen:

- Sie muss eine Untermenge der Codepage des PowerCenter Repository sein.
- Sie muss eine Untermenge der Codepage des Metadata Manager Repository sein.
- Sie muss eine Untermenge der Codepage des Model Repository sein.

Codepage des PowerCenter Client

Die Codepage des PowerCenter Client entspricht der Codepage des Betriebssystems des PowerCenter Client. Zur Kommunikation mit dem PowerCenter Repository muss die Codepage des PowerCenter Client eine Untermenge der Codepage des PowerCenter Repository sein.

Codepage des PowerCenter Integration Service-Prozesses

Die Codepage eines PowerCenter Integration Service-Prozesses ist die Codepage des Knotens, auf dem der PowerCenter Integration Service-Prozess ausgeführt wird. Definieren Sie die Codepage für jeden PowerCenter Integration Service-Prozess im Administrator Tool auf der Registerkarte "Prozesse".

Unter UNIX können Sie jedoch die Codepage des PowerCenter Integration Service-Prozesses ändern, indem Sie die Umgebungsvariable LANG, LC_CTYPE oder LC_ALL für den Benutzer ändern, wenn der Prozess startet.

Die Codepage des PowerCenter Integration Service Prozesses muss:

- Eine Untermenge der Codepage des PowerCenter Repository sein.
- Eine Obermenge des Computers sein, der *pmcmd* hostet, oder eine Obermenge der Codepage sein, die in der Umgebungsvariablen INFA_CODEPAGENAME angegeben ist

Die Codepages aller PowerCenter Integration Service-Prozesse müssen miteinander kompatibel sein. Sie können z. B. MS Windows Latin1 für einen Knoten unter Windows und ISO-8859-1 für einen Knoten unter UNIX verwenden.

PowerCenter Integration Services, die für den Unicode-Modus konfiguriert sind, validieren Codepages beim Start einer Sitzung, um genaue Datenbewegungen zu gewährleisten. Dabei wird die Sitzungscodepage zur Konvertierung der Zeichendaten herangezogen. Wenn Sie den PowerCenter Integration Service im ASCII-Modus ausführen, validiert er die Sitzungscodepages nicht. Er liest alle Zeichendaten als ASCII-Zeichen und führt keine Codepage-Konvertierung durch.

Mit jeder Codepage ist eine Sortierreihenfolge verknüpft. Wenn Sie eine Sitzung konfigurieren, können Sie eine der Sortierreihenfolgen wählen, die mit der Codepage der PowerCenter Integration Service-Prozesses verbunden sind. Wenn Sie den PowerCenter Integration Service im Unicode-Modus ausführen, nutzt er die ausgewählte Sitzungssortierreihenfolge zur Sortierung der Zeichendaten. Wenn Sie den PowerCenter Integration Service im ASCII-Modus ausführen, sortiert er alle Zeichendaten in binärer Sortierreihenfolge.

Wenn Sie dem PowerCenter Integration Service in den Vereinigten Staaten unter Windows ausführen, sollten Sie MS Windows Latin1 (ANSI) als Codepage des PowerCenter Integration Service-Prozesses verwenden.

Wenn Sie dem PowerCenter Integration Service in den Vereinigten Staaten unter UNIX ausführen, sollten Sie ISO 8859-1 als Codepage des PowerCenter Integration Service-Prozesses verwenden.

Wenn Sie *pmcmd* für die Kommunikation mit dem PowerCenter Integration Service nutzen, muss die Codepage des Betriebssystems, das *pmcmd* hostet, mit der Codepage des PowerCenter Integration Service-Prozesses identisch sein.

Der PowerCenter Integration Service generiert die Namen der Sitzungsprotokolldateien, Ablehnungsdateien, Caches bzw. Cache-Dateien und Leistungsdetaildateien auf der Basis der Codepage des PowerCenter Integration Service-Prozesses.

PowerCenter Repository-Codepage

Die Codepage des PowerCenter-Repository ist die Codepage der Daten im Repository. Der PowerCenter Repository Service verwendet die PowerCenter Repository-Codepage, um Metadaten in der PowerCenter Repository-Datenbank zu speichern und daraus abzurufen. Wählen Sie die PowerCenter Repository-Codepage beim Erstellen oder Aktualisieren eines PowerCenter-Repository aus. Wenn die Codepage der PowerCenter Repository-Datenbank UTF-16LE ist, können Sie ein PowerCenter-Repository mit UTF-16LE als Codepage erstellen.

Die Codepage des PowerCenter-Repository muss folgende Bedingungen erfüllen:

- Mit der Codepage der Domänenkonfigurationsdatenbank kompatibel sein
- Eine Obermenge der Codepage des Administrator Tools sein

- Eine Obermenge der Codepage des PowerCenter Clients sein
- Eine Obermenge der Codepage für den PowerCenter Integration Service-Prozess sein
- Eine Obermenge des Computers sein, der *pmrep* hostet, oder eine Obermenge der Codepage sein, die in der Umgebungsvariablen INFA_CODEPAGENAME angegeben ist

Eine globale PowerCenter Repository-Codepage muss eine Teilmenge der lokalen PowerCenter Repository-Codepage sein, wenn Sie Verknüpfungen im lokalen PowerCenter-Repository erstellen möchten, die auf ein Objekt in einem globalen PowerCenter-Repository verweisen.

Wenn Sie Objekte von einem PowerCenter-Repository zu einem anderen PowerCenter-Repository kopieren, muss die Codepage für das Target-Repository eine Obermenge der Codepage des Quell-Repositorys sein.

Codepage für Metadaten Manager-Repository.

Die Codepage des Metadata Manager-Repository ist die Codepage der Daten im Repository. Der Metadata Manager Service verwendet die Metadata Manager-Repository-Codepage, um Metadaten in der Repository-Datenbank zu speichern und daraus abzurufen. Das Administrator Tool schreibt Benutzer- und Gruppen-Informationen in den Metadata Manager Service. Außerdem schreibt das Administrator Tool Domäneninformationen in die Repository-Datenbank. Der PowerCenter Repository Service-Prozess schreibt Metadaten in die Repository-Datenbank. Wählen Sie die Repository-Codepage beim Erstellen oder Aktualisieren eines Metadata Manager-Repository aus. Wenn die Codepage der Repository-Datenbank UTF-16LE ist, können Sie ein Repository mit UTF-16LE als Codepage erstellen.

Die Codepage des Metadata Manager-Repository muss folgende Bedingungen erfüllen:

- Mit der Codepage der Domänenkonfigurationsdatenbank kompatibel sein
- Eine Obermenge der Codepage des Administrator Tools sein
- Eine Untermenge der Codepage des PowerCenter Repository sein.
- Eine Obermenge der Codepage für den PowerCenter Integration Service-Prozess sein

PowerCenter-Quell-Codepage

Die Quell-Codepage ist vom Typ der Quelle abhängig:

- Flatfiles und VSAM-Dateien. Die Codepage der Daten in der Datei. Wählen Sie bei der Konfiguration der Flatfile- oder COBOL-Quelldefinition eine Codepage, die mit der Codepage der Daten in der Datei übereinstimmt.
- XML-Dateien Der PowerCenter Integration Service konvertiert XML in Unicode, wenn er eine XML-Quelle analysiert. Wenn Sie eine XML-Quelldefinition erstellen, weist der PowerCenter Designer eine Standard-Codepage zu. Sie können die Codepage nicht ändern.
- Relationale Datenbanken. Die Codepage des Datenbank-Client. Wählen Sie bei der Konfiguration der relationale Verbindung im PowerCenter Workflow Manager eine Codepage, die mit der Codepage des Datenbank-Client kompatibel ist. Wenn Sie eine Datenbank-Umgebungsvariable zur Angabe der Sprache für die Datenbank festlegen, stellen Sie sicher, dass die Codepage für die Verbindung mit der für die Variable festgelegten Sprache kompatibel ist. Zum Beispiel: Wenn Sie die Umgebungsvariable NLS_LANG für eine Oracle-Datenbank festgelegt haben, müssen Sie sicherstellen, dass die Codepage der Oracle-Verbindung mit dem festgelegten Wert in der Variable NLS_LANG identisch ist. Wenn Sie keine kompatiblen Codepages verwenden, können die Sitzungen hängen, Daten können inkonsistent werden, oder Sie können einen Datenbankfehler erhalten, wie z. B.:

```
ORA-00911: Invalid character specified.
```

Unabhängig vom Typ der Quelle muss die Quell-Codepage eine Teilmenge der Codepage der Umwandlungen und Targets sein, die Daten von der Quelle empfangen. Die Quell-Codepage braucht keine Teilmenge der Umwandlungen oder Targets zu sein, die keine Daten aus der Quelle empfangen.

Hinweis: Wählen Sie IBM EBCDIC nur dann als Codepage für Ihre Quelldatenbankverbindung, wenn Sie auf EBCDIC-Daten zugreifen, wie beispielsweise Daten aus einer extrahierten Großrechnerdatei zugreifen.

PowerCenter-Target-Codepage

Die Target-Codepage ist vom Typ des Targets abhängig:

- Einfachdateien Wählen Sie bei der Konfiguration der Einfachdatei-Target-Definition eine Codepage, die mit der Codepage der Daten in der Einfachdatei übereinstimmt.
- XML-Dateien Konfigurieren Sie die XML-Target-Codepage, nachdem Sie die XML-Target-Definition erstellt haben. Der XML-Assistent ordnet dem XML-Target eine Standard-Codepage zu. Der PowerCenter Designer wendet nicht die Codepage an, die im XML-Schema steht.
- Relationale Datenbanken. Wählen Sie bei der Konfiguration der relationale Verbindung im PowerCenter Workflow Manager eine Codepage, die mit der Codepage des Datenbank-Client kompatibel ist. Wenn Sie eine Datenbank-Umgebungsvariable zur Angabe der Sprache für die Datenbank festlegen, stellen Sie sicher, dass die Codepage für die Verbindung mit der für die Variable festgelegten Sprache kompatibel ist. Zum Beispiel: Wenn Sie die Umgebungsvariable NLS_LANG für eine Oracle-Datenbank festgelegt haben, müssen Sie sicherstellen, dass die Codepage der Oracle-Verbindung mit dem festgelegten Wert in der Variable NLS_LANG kompatibel sein. Wenn Sie keine kompatiblen Codepages verwenden, können die Sitzungen hängen oder Sie können einen Datenbankfehler erhalten, wie z. B.:

```
ORA-00911: Invalid character specified.
```

Die Target-Codepage muss eine Obermenge der Codepage der Umwandlungen und Quellen sein, die Daten an das Target liefern. Die Target-Codepage braucht keine Obermenge der Umwandlungen oder Quellen zu sein, die keine Daten an das Target liefern.

Der Integration Service erstellt Sitzungsindikatordateien, Sitzungsausgabedateien sowie Steuerungsdateien für externen Ladevorgang und Datendateien unter Verwendung der Codepage der Target-Einfachdatei.

Hinweis: Wählen Sie IBM EBCDIC nur dann als Codepage für Ihre Target-Datenbankverbindung, wenn Sie auf EBCDIC-Daten zugreifen, wie beispielsweise Daten aus einer extrahierten Großrechnerdatei zugreifen.

Befehlszeilenprogramm-Codepages

Die Befehlszeilenprogramme *pmcmd* und *pmrep* erfordern Codepage-Kompatibilität. *pmcmd* und *pmrep* nutzen Codepages zum Senden von Befehlen in Unicode. Andere Befehlszeilenprogramme erfordern keine Codepages.

Die Codepage-Kompatibilität für *pmcmd* und *pmrep* ist davon abhängig, ob Sie die Codepage-Umgebungsvariable INFA_CODEPAGENAME für *pmcmd* oder *pmrep* konfiguriert haben. Sie können diese Variable entweder für ein Befehlszeilenprogramm oder für beide angeben.

Falls Sie diese Variable für ein Befehlszeilenprogramm nicht konfiguriert haben, vergewissern Sie sich bitte, dass folgende Anforderungen erfüllt sind:

- Haben Sie die Variable nicht für *pmcmd* konfiguriert, muss die Codepage des *pmcmd* für das Computer-Hosting eine Teilmenge der Codepage für den PowerCenter Integration Service Prozess sein.
- Sollten Sie die Variable nicht für *pmrep* konfiguriert haben, muss die Codepage des *pmrep* für das Computer-Hosting eine Teilmenge der PowerCenter Repository Codepage sein.

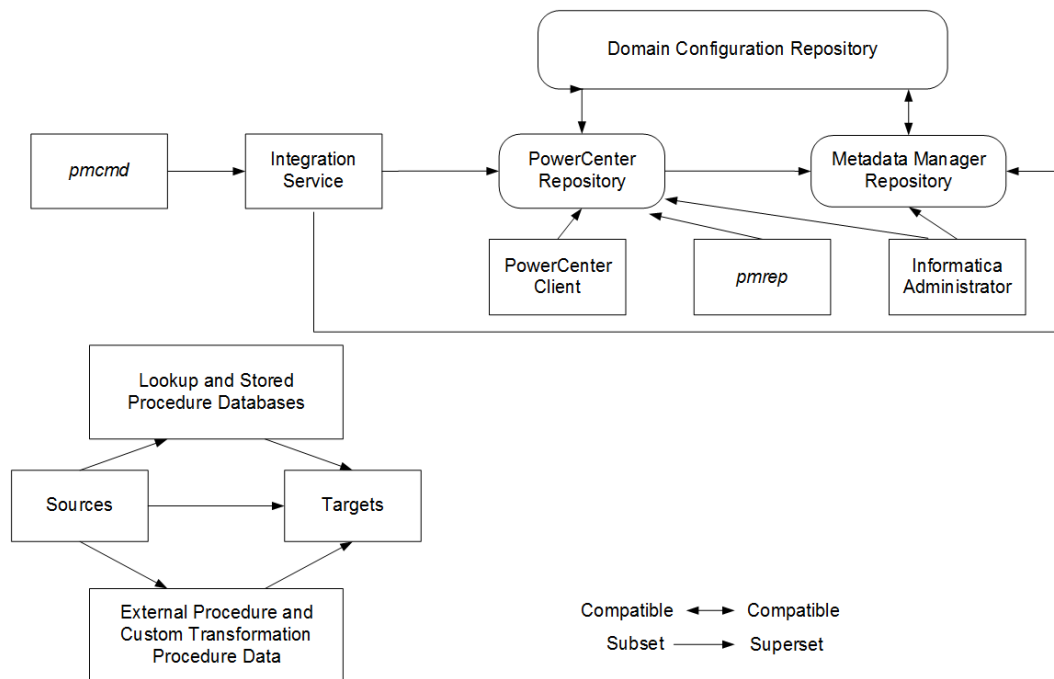
Wenn Sie die Codepage-Umgebungsvariable INFA_CODEPAGE_NAME für *pmcmd* oder *pmrep* konfigurieren, vergewissern Sie sich bitte, dass folgende Anforderungen erfüllt sind:

- Konfigurieren Sie INFA_CODEPAGE_NAME für *pmcmd*, muss die für die Variable definierte Codepage eine Teilmenge der Codepage für den PowerCenter Integration Service Prozess sein.
- Falls Sie INFA_CODEPAGE_NAME für *pmrep* konfigurieren, muss die für die Variable definierte Codepage eine Teilmenge der PowerCenter Repository Codepage sein.
- Führen Sie *pmcmd* und *pmrep* auf ein- und demselben Computer aus und konfigurieren Sie die Variable INFA_CODEPAGE_NAME, muss die für die Variable definierte Codepage Teilmengen der Codepages für den PowerCenter Integration Service Prozess und das PowerCenter Repository darstellen.

Sofern die Codepages nicht kompatibel sind, wird der PowerCenter Integration Service Prozess den Arbeitsablauf, die Sitzung oder die Task möglicherweise nicht vom PowerCenter Repository abfragen.

Codepage-Kompatibilität - Zusammenfassung

Die folgende Abbildung zeigt die Codepage-Kompatibilität in der Informatica-Umgebung:



Die folgende Tabelle enthält eine Zusammenfassung der Codepage-Kompatibilität zwischen Quellen, Zielen, Repositorys, dem Informatica Administrator, dem PowerCenter Client und dem PowerCenter-Integrationsdienst-Prozess:

Komponenten-Codepage	Codepage-Kompatibilität
Quelle (inklusive relationale, Einfachdatei und XML-Datei)	Ziel-Teilmenge. Teilmenge der Lookup-Daten. Teilmenge gespeicherter Prozeduren. Teilmenge der Codepage einer externen Prozedur oder einer benutzerdefinierten Umwandlungsprozedur.
Ziel (inklusive relationale, XML-Dateien und Einfachdateien)	Übergeordnete Menge der Quelle. Übergeordnete Menge für Lookup-Daten. Übergeordnete Menge gespeicherter Prozeduren. Übergeordnete Menge der Codepage für eine externe Prozedur oder eine benutzerdefinierte Umwandlungsprozedur. Der Integrationsdienst-Prozess erstellt mit der Codepage der Ziel-Einfachdatei externe Ladedaten und Steuerungsdateien.
Datenbank für Lookup- und gespeicherte Prozeduren	Ziel-Teilmenge. Übergeordnete Menge der Quelle.
Externe Prozedur und benutzerdefinierte Umwandlungsprozeduren	Ziel-Teilmenge. Übergeordnete Menge der Quelle.
Domänen-Konfigurationsdatenbank	Kompatibel mit dem PowerCenter-Repository-Dienst. Kompatibel mit dem Metadata Manager Repository.
PowerCenter-Integrationsdienst-Prozess	Kompatibel mit dessen Betriebssystem Teilmenge des PowerCenter-Repository. Teilmenge des Metadata Manager Repository. Übergeordnete Menge für Computer-Hosting <i>pmcmd</i> . Identisch mit anderen Knoten, auf denen die PowerCenter-Integrationsdienst-Prozesse ausgeführt werden.
PowerCenter-Repository	Kompatibel mit der Domänen-Konfigurationsdatenbank. Übergeordnete Menge des PowerCenter Client. Übergeordnete Menge der Knoten, auf denen der PowerCenter-Integrationsdienst-Prozess ausgeführt wird. Übergeordnete Menge des Metadata Manager Repository. Eine globale PowerCenter-Repository Codepage muss eine Teilmenge eines lokalen PowerCenter-Repository sein.
PowerCenter Client	Teilmenge des PowerCenter-Repository.
Computer, auf dem <i>pmcmd</i> ausgeführt wird	Teilmenge des PowerCenter-Integrationsdienst-Prozesses.
Computer, auf dem <i>pmrep</i> ausgeführt wird	Teilmenge des PowerCenter-Repository.

Komponenten-Codepage	Codepage-Kompatibilität
Administrator-Tool	Teilmenge des PowerCenter-Repository. Teilmenge des Metadata Manager Repository.
Metadata Manager Repository	Kompatibel mit der Domänen-Konfigurationsdatenbank. Teilmenge des PowerCenter-Repository. Übergeordnete Menge des Administrator-Tool. Übergeordnete Menge des PowerCenter-Integrationsdienst-Prozesses.

Codepage-Validierung

Die Computer, die den PowerCenter Client, den PowerCenter Integration Service Prozess und die PowerCenter Repository-Datenbank hosten, müssen die entsprechenden Codepages verwenden. So lassen sich Daten- oder Repository-Inkonsistenzen vermeiden. Wenn der PowerCenter Integration Service im Unicode-Datenverschiebungsmodus ausgeführt wird, erzwingt er Sitzungs-Codepage-Beziehungen. Wird der PowerCenter Integration Service im ASCII-Modus ausgeführt, erzwingt er keine Sitzungs-Codepage-Beziehungen.

Um die Kompatibilität zu gewährleisten, führen PowerCenter Client und PowerCenter Integration Service folgende Codepage-Validierungen durch:

- PowerCenter schränkt die Verwendung EBCDIC-basierter Codepages für Repositories ein. Da Sie weder den PowerCenter-Client noch das PowerCenter-Repository auf Mainframe-Systemen installieren können, ist es nicht möglich, EBCDIC-basierte Codepages wie IBM EBCDIC als PowerCenter-Repository Codepage zu wählen.
- Der PowerCenter Client kann keine Verbindung zum PowerCenter-Repository herstellen, wenn seine Codepage eine Teilmenge der PowerCenter-Repository-Codepage ist. Ist die PowerCenter-Client-Codepage keine Teilmenge der PowerCenter-Repository-Codepage, kann der PowerCenter-Client aufgrund des folgenden Fehlers keine Verbindung zur PowerCenter-Repository-Codepage herstellen:

```
REP_61082 <PowerCenter Client>'s code page <PowerCenter Client code page> is not one-way compatible to repository <PowerCenter repository name>'s code page <PowerCenter repository code page>.
```

- Nachdem Sie die PowerCenter-Repository-Codepage eingerichtet haben, können Sie sie ändern. Nachdem Sie ein PowerCenter-Repository erstellt oder geupgradet haben, dürfen Sie die PowerCenter-Repository-Codepage nicht ändern. So vermeiden Sie Datenverluste und Inkonsistenzen im PowerCenter-Repository.
- Der PowerCenter Integration Service Prozess kann starten, wenn seine Codepage eine Untermenge der PowerCenter-Repository-Codepage ist. Die Codepage des PowerCenter Integration Service Prozesses muss eine Teilmenge der PowerCenter-Repository-Codepage sein, um Datenverlust oder Inkonsistenzen zu vermeiden. Ist er keine Teilmenge der PowerCenter-Repository-Codepage, schreibt der PowerCenter Integration Service folgende Meldung in die Log-Dateien:

```
REP_61082 <PowerCenter Integration Service>'s code page <PowerCenter Integration Service code page> is not one-way compatible to repository <PowerCenter repository name>'s code page <PowerCenter repository code page>.
```

- Im Unicode-Datenverschiebungsmodus startet der PowerCenter Integration Service Arbeitsabläufe mit den entsprechenden Quell- und Target-Codepage-Beziehungen für jede Sitzung. Wird der PowerCenter Integration Service im Unicode-Modus ausgeführt, muss die Codepage für jede Quelle in einer Sitzung eine Teilmenge der Target-Codepage sein. So wird Datenverlust während einer Sitzung vermieden.

Stehen Quell- und Target-Codepage nicht im richtigen Verhältnis zueinander schlägt die PowerCenter Integration Service Sitzung fehl und ins Sitzungs-Log wird folgende Meldung geschrieben:

```
TM_6227 Error: Code page incompatible in session <session name>. <Additional details>.
```

- Der PowerCenter Workflow Manager validiert die Quell-, Target-, Lookup- und gespeicherten Prozedur-Codepage-Beziehungen für jede Sitzung. Beim Speichern der Sitzung prüft der PowerCenter Workflow Manager die Codepage-Beziehungen unabhängig vom Datenverschiebungsmodus des PowerCenter Integration Service. Konfigurieren Sie eine Sitzung mit ungültigen Quell-, Target-, Lookup- oder gespeicherten Prozedur-Codepage-Beziehungen, generiert der PowerCenter Workflow Manager beim Speichern der Sitzung eine Warnmeldung wie die folgende:

```
CMN_1933 Code page <code page name> for data from file or connection associated with transformation <name of source, target, or transformation> needs to be one-way compatible with code page <code page name> for transformation <source or target or transformation name>.
```

Wenn Sie die Sitzung im ASCII-Modus ausführen möchten, können Sie die Sitzung speichern wie konfiguriert. Um die Sitzung im Unicode-Modus auszuführen, müssen Sie die Sitzung so bearbeiten, dass sie die richtigen Codepages verwendet.

Entspannte Codepage-Validierung

In Ihrer Umgebung kann es notwendig sein, dass Sie Daten aus unterschiedlichen Quellen mit Zeichensätzen aus verschiedenen Sprachen verarbeiten. Zum Beispiel könnten Sie Daten aus englischen und japanischen Quellen unter Verwendung desselben PowerCenter-Repository verarbeiten müssen oder Quelldaten extrahieren wollen, die in einer Unicode-Codierung wie UTF-16LE codiert sind. Sie können den PowerCenter Integration Service für eine entspannte Codepage-Validierung konfigurieren. Mit der entspannten Codepage-Validierung können Sie Daten mit Quellen und Targets verarbeiten, die inkompatible Codepages haben.

Auch wenn die entspannte Codepage-Validierung Codepage-Einschränkungen bei Quellen und Targets entfernt, erzwingt sie dennoch die Codepage-Kompatibilität zwischen dem PowerCenter Integration Service und dem PowerCenter-Repository.

Hinweis: Die entspannte Codepage-Validierung ist kein Schutz vor möglichen Dateninkonsistenzen, wenn Sie Daten zwischen inkompatiblen Codepages verschieben. Sie müssen sicherstellen, dass die Zeichen, die der PowerCenter Integration Service aus der Quelle liest, in der Target-Codepage enthalten sind.

Informatica hebt die folgenden Einschränkungen auf, wenn Sie die entspannte Codepage-Validierung einsetzen:

- Quell- und Target-Codepages. Sie können jede beliebige Codepage verwenden, die von Informatica für Ihre Quell- und Targetdaten unterstützt wird.
- Sitzungs-Sortier-Reihenfolge. Sie können beim Konfigurieren von Sitzungen jede beliebige Sortierreihenfolge verwenden, die von Informatica unterstützt wird.

Wenn Sie eine Sitzung mit entspannter Codepage-Validierung starten, schreibt der PowerCenter Integration Service die folgende Meldung in das Sitzungs-Log:

```
TM_6185 WARNING! Data code page validation is disabled in this session.
```

Wenn Sie die entspannte Codepage-Validierung verwenden, schreibt der PowerCenter Integration Service Beschreibungen der Datenbankverbindungs-Codepages in das Sitzungs-Log.

Der folgende Text zeigt ein Beispiel für eine Codepage-Meldung im Sitzungs-Log:

```
TM_6187 Repository code page: [MS Windows Latin 1 (ANSI), superset of Latin 1]  
WRT_8222 Target file [$PMTTargetFileDir\passthru.out] code page: [MS Windows Traditional Chinese, superset of Big 5]
```

```
WRT_8221 Target database connection [Japanese Oracle] code page: [MS Windows Japanese,
superset of Shift-JIS]
TM_6189 Source database connection [Japanese Oracle] code page: [MS Windows Japanese,
superset of Shift-JIS]
CMN_1716 Lookup [LKP_sjis_lookup] uses database connection [Japanese Oracle] in code
page [MS Windows Japanese, superset of Shift-JIS]
CMN_1717 Stored procedure [J_SP_INCREMENT] uses database connection [Japanese Oracle] in
code page [MS Windows Japanese, superset of Shift-JIS]
```

Wenn der PowerCenter Integration Service Daten nicht richtig konvertieren kann, schreibt er eine Fehlermeldung in das Sitzungs-Log.

Konfigurieren des PowerCenter Integration Service

Um den PowerCenter Integration Service auf Codepage Relaxation zu konfigurieren, müssen folgende Tasks im Administrator Tool durchgeführt werden:

- Codepage-Validierung deaktivieren. Deaktivieren Sie die Option ValidateDataCodePages in den Eigenschaften des PowerCenter Integration Service.
- Konfigurieren Sie den PowerCenter Integration Service auf Unicode-Datenverschiebungsmodus. Wählen Sie in den Eigenschaften des PowerCenter Integration Service Unicode als Datenverschiebungsmodus.
- Konfigurieren Sie den PowerCenter Integration Service so, dass er zum Schreiben in den Logs den Zeichensatz UTF-16LE verwendet. Aktivieren Sie beim Konfigurieren von Sitzungen oder Arbeitsabläufen zum Schreiben in Log-Dateien die Option LogInUTF8 in den Eigenschaften für den PowerCenter Integration Service. Wenn Sie die Option LogInUTF8 aktivieren, schreibt der PowerCenter Integration Service alle Logs in UTF-16LE. Der PowerCenter Integration Service schreibt per Standard im Log-Manager in UTF-16LE.

Kompatible Quell- und Target-Codepages auswählen

Obwohl es das PowerCenter ermöglicht, jede unterstützte Codepage zu verwenden, gibt es Risiken mit inkompatiblen Codepages für Quellen und Targets. Wenn Ihre Target-Codepage keine Obermenge der Quell-Codepage ist, riskieren Sie Inkonsistenzen in den Target-Daten, denn die Quelldaten enthalten eventuell Zeichen, die nicht in der Target-Codepage codiert sind.

Wenn der PowerCenter Integration Service Zeichen liest, die nicht in der Target-Codepage enthalten sind, riskieren Sie Umwandlungsfehler, inkonsistente Daten oder fehlgeschlagene Sitzungen.

Hinweis: Wenn Sie die Codepage-Validierung lockern, liegt es in Ihrer Verantwortung, dass die Datenkonvertierung von der Quelle in das Target korrekt funktioniert.

Fehlerbehebung für Codepage-Lockerung

Der PowerCenter Integration Service hat einen Fehler in einer Sitzung begangen und schreibt folgende Meldung in das Sitzungs-Log:

```
TM_6188 The specified sort order is incompatible with the PowerCenter Integration
Service code page.
```

Wählen Sie zum Validieren von Codepages eine Sortierreihenfolge aus, die mit der PowerCenter Integration Service-Codepage kompatibel ist. Um die Codepage-Validierung zu lockern, legen Sie im PowerCenter Integration Service fest, dass die Codepage-Validierung im Unicode-Datenverschiebungsmodus gelockert wird.

Ich habe versucht, den Sitzungs- und Arbeitsablauf-Log anzuzeigen, aber sie enthalten nur unlesbare Zeichen.

Der PowerCenter Integration Service ist nicht für das Schreiben von Sitzungs- und Arbeitsablauf-Logs mit dem UTF-16LE Zeichensatz konfiguriert.

Aktivieren Sie die Option `LogsInUTF8` in den Eigenschaften des PowerCenter Integration Service.

PowerCenter Codepage-Umwandlung

Wenn im Datenverschiebungsmodus Unicode festgelegt ist, akzeptiert der PowerCenter-Client Eingaben in jeder Sprache und wandelt sie in UCS-2 um. Der PowerCenter Integration Service konvertiert Quelldaten vor der Verarbeitung in UCS-2 und wandelt die verarbeiteten Daten vor dem Laden von UCS-2 in die Target-Codepage um.

In einer Sitzung wandelt der PowerCenter Integration Service Quell-, Target- und Lookup-Abfragen von der PowerCenter-Repository-Codepage in die Quell-, Target- oder Lookup-Codepage um. Der PowerCenter Integration Service konvertiert auch den Namen und den Aufrufstext gespeicherter Prozeduren von der PowerCenter-Repository-Codepage in die Codepage der Datenbank der gespeicherten Prozedur um.

Zur Laufzeit überprüft der PowerCenter Integration Service, ob er die folgenden Abfragen und Prozedurentexte von der PowerCenter-Repository-Codepage ohne Datenverlust konvertieren kann:

- Quellabfrage. Muss in Quelldatenbank-Codepage konvertieren.
- Lookup-Abfrage. Muss in Lookup-Datenbank-Codepage konvertieren.
- Target-SQL-Abfrage. Muss in Target-Datenbank-Codepage konvertieren.
- Name und Aufrufstext gespeicherter Prozeduren. Muss in Codepage der Datenbank der gespeicherten Prozedur konvertieren.

Auswählen von Zeichen für PowerCenter Repository Metadaten

Bei der Eingabe von Metadaten ins PowerCenter-Repository können Sie beliebige Zeichen der PowerCenter-Repository-Codepage verwenden. Nutzt das PowerCenter-Repository UTF-16LE, können beliebige Unicode-Zeichen eingegeben werden. In einem für UTF-16LE aktivierten PowerCenter-Repository können Sie beispielsweise deutsche, japanische und englische Metadaten speichern. Es muss jedoch gewährleistet sein, dass der PowerCenter Integration Service erfolgreich SQL-Transaktionen mit Quell-, Target-, Lookup- und gespeicherten Prozedurdatenbanken abwickeln kann. Außerdem müssen Sie sicherstellen, dass der PowerCenter Integration Service aus Quell- und Lookup-Dateien lesen und in Target- und Lookup-Dateien schreiben kann. Daher müssen Sie beim Ausführen einer Sitzung darauf achten, dass die Zeichen der PowerCenter-Repository-Metadaten in den Quell-, Target-, Lookup- und gespeicherten Prozedur-Codepages kodiert sind.

Beispiel

PowerCenter Integration Service, PowerCenter-Repository und PowerCenter-Client nutzen die ISO 8859-1 Latin1 Codepage und die Quelldatenbank enthält anhand der Shift-JIS-Codepage kodierte japanische Daten. Jede Codepage enthält Zeichen, die nicht in einer anderen kodiert sind. Werden andere Zeichen als 7-Bit-

ASCII für PowerCenter-Repository und Quelldatenbank-Metadaten verwendet, kann die Sitzung in folgenden Situationen fehlschlagen oder dazu führen, dass keine Zeilen in das Target geladen werden:

- Sie erstellen ein Mapping, das ein String-Literal mit speziellen Zeichen des deutschen Sprachbereichs nach ISO 8859-1 in einer Abfrage enthält. Die Quelldatenbank kann die Abfrage zurückweisen oder inkonsistente Ergebnisse zurückgeben.
- Sie erstellen mit dem PowerCenter-Client SQL-Abfragen mit speziellen Zeichen des deutschen Sprachbereichs nach ISO 8859-1. Die Quelldatenbank kann die spezifisch deutschen Zeichen der ISO 8859-1 Codepage nicht in die Shift-JIS-Codepage konvertieren.
- Die Quelldatenbank hat einen Tabellennamen, der japanische Zeichen enthält. Der PowerCenter-Designer kann die japanischen Zeichen der Quelldatenbank-Codepage nicht in diejenigen der Codepage des PowerCenter-Client konvertieren. Stattdessen importiert der PowerCenter-Designer die japanischen Zeichen als Fragezeichen (?) und ändert so den Namen der Tabelle. Der PowerCenter Repository Service speichert den Namen der Quelltable als Fragezeichen im PowerCenter-Repository. Sendet der PowerCenter Integration Service eine Abfrage an die Quelldatenbank mit dem geänderten Tabellennamen, kann die Quelldatenbank die richtige Tabelle nicht finden und gibt keine Zeilen oder einen Fehler an den PowerCenter Integration Service zurück, so dass die Sitzung fehlschlägt.

Da die US-ASCII-Codepage eine Teilmenge der Codepages ISO 8859-1 und Shift-JIS ist, können Sie diese Dateninkonsistenzen vermeiden, indem Sie für Ihre sämtlichen Metadaten 7-Bit-ASCII-Zeichen verwenden.

Fallstudie: ISO 8859-1 Datenverarbeitung

Diese Fallstudie beschreibt, wie Sie eine Umgebung zur Verarbeitung von ISO 8859-1 Multibyte-Daten einrichten können. So können Sie Ihre Umgebung konfigurieren, wenn Sie Daten verschiedener westeuropäischer Sprachen mit Zeichensätzen der ISO 8859-1 Codepage verarbeiten müssen. Dieses Beispiel beschreibt eine Umgebung zur Verarbeitung von Daten in englischer und deutscher Sprache.

In dieser Fallstudie umfasst die ISO 8859-1 Umgebung folgende Elemente:

- PowerCenter Integration Service auf einem UNIX-System
- PowerCenter Client auf einem Windows-System, erworben in den Vereinigten Staaten
- PowerCenter Repository gespeichert in einer Oracle-Datenbank unter UNIX
- Quelldatenbank mit Daten in englischer Sprache
- Weitere Quelldatenbank mit Daten in deutscher und englischer Sprache
- Target-Datenbank mit Daten in deutscher und englischer Sprache
- Lookup-Datenbank mit englischsprachigen Daten

Die Datenumgebung muss englische und deutsche Zeichendaten verarbeiten.

ISO 8859-1 Umgebung konfigurieren

Verwenden Sie die folgenden Richtlinien, wenn Sie eine Umgebung ähnlich wie in diesem Beispiel für die ISO 8859-1 Datenverarbeitung konfigurieren möchten:

1. Stellen Sie die Codepage-Kompatibilität zwischen dem PowerCenter Repository Datenbank-Client und dem Datenbankserver sicher.
2. Stellen Sie die Codepage-Kompatibilität zwischen dem PowerCenter Client und dem PowerCenter Repository sicher sowie zwischen dem PowerCenter Integration Dienstprozess und dem PowerCenter Repository.

3. Setzen Sie den Datenverschiebungsmodus des PowerCenter Integration Service auf ASCII.
4. Überprüfen Sie die Kompatibilität der Sitzungs-Codepage.
5. Prüfen Sie die Codepage-Kompatibilität für die Lookup- und Gespeicherte-Prozeduren-Datenbank.
6. Stellen Sie die Codepage-Kompatibilität externer Prozeduren oder benutzerdefinierter Transformationsprozeduren sicher.
7. Konfigurieren Sie die Sortierreihenfolge einer Sitzung.

Schritt 1. Verifizieren der Kompatibilität von PowerCenter Repository Database Client und Server

Der Datenbank-Client und Server, die das PowerCenter Repository hosten, müssen in der Lage sein, ohne Datenverlust zu kommunizieren.

Das PowerCenter Repository befindet sich in einer Oracle-Datenbank. Benutzen Sie die Umgebungsvariable NLS_LANG, um das Gebietsschema (Sprache, Region und Zeichensatz) festzulegen, das der Datenbank-Client und -Server bei der Anmeldung verwenden sollen:

```
NLS_LANG = LANGUAGE_TERRITORY.CHARACTERSET
```

Standardmäßig konfiguriert Oracle NLS_LANG für US-Englisch, das US-Territorium, und den 7-Bit ASCII-Zeichensatz:

```
NLS_LANG = AMERICAN_AMERICA.US7ASCII
```

Ändern Sie die Standard-Konfiguration, um ISO 8859-1-Daten mit der Oracle WE8ISO8859P1 Codepage in das PowerCenter Repository zu schreiben. Beispiel:

```
NLS_LANG = AMERICAN_AMERICA.WE8ISO8859P1
```

Weitere Informationen zum Überprüfen und Ändern der PowerCenter Repository Database-Codepage finden Sie in Ihrer Datenbank-Dokumentation.

Schritt 2. Stellen Sie die PowerCenter Codepage-Kompatibilität sicher

PowerCenter Integration Service und PowerCenter-Client-Codepages müssen Teilmengen der PowerCenter Repository Codepage sein. Da der PowerCenter-Client und PowerCenter Integration Service jeweils die System-Codepages des Computers verwenden, auf denen sie installiert sind, müssen Sie überprüfen, ob die System-Codepages Teilmengen der PowerCenter Repository Codepage sind.

In diesem Fall wurde der PowerCenter-Client auf Windows-Systemen in den Vereinigten Staaten gekauft. Daher sind die System-Codepages für die PowerCenter-Client-Computer auf MS Windows Latin1 eingestellt. Um System- und Bildschirmsprachen zu überprüfen, öffnen Sie das Dialogfeld "Regionale Einstellungen" in der Windows-Systemsteuerung. Für Systeme, die in den Vereinigten Staaten erworben wurden, müssen die Ländereinstellungen und Eingabegebietsschemata für Englisch (USA) konfiguriert werden.

Der PowerCenter Integration Service ist auf einem UNIX-Rechner installiert. Die Standard-Codepage für das UNIX-Betriebssysteme ist ASCII. In dieser Umgebung ändern Sie die UNIX-System-Codepage auf ISO 8859-1 Western European, sodass sie eine Teilmenge der PowerCenter Repository-Codepage ist.

Schritt 3. Konfigurieren des PowerCenter Integration Service für den ASCII-Datenverschiebungsmodus

Konfigurieren Sie den PowerCenter Integration Service für die Verarbeitung von ISO 8859-1 Daten. Im Administrator Tool setzen Sie den Datenverschiebungsmodus für den PowerCenter Integration Service auf ASCII.

Schritt 4. Stellen Sie die Sitzungs-Codepage-Kompatibilität sicher

Wenn Sie einen Arbeitsablauf im ASCII-Datenverschiebungsmodus ausführen, erzwingt der PowerCenter Integration Service Quell- und Target-Codepage-Beziehungen. Um genaue Datenumwandlungen zu gewährleisten, muss die Quell-Codepage eine Teilmenge der Target-Codepage sein.

In diesem Fall enthält die Umgebung eine Quelldatenbank mit deutschen und englischen Daten. Wenn Sie eine Quelldatenbank-Verbindung im PowerCenter Workflow Manager konfigurieren, muss die Codepage für die Verbindung mit der Quelldatenbank-Codepage identisch und eine Teilmenge der Target-Codepage sein. Da sowohl die Codepage MS Windows Latin1 und die Codepage ISO 8859-1 Western European deutsche Umlaute enthalten, würden Sie wahrscheinlich eine dieser Codepages für die Quelldatenbank-Verbindungen verwenden.

Da die Target-Codepage eine Obermenge der Quell-Codepages sein muss, müssen Sie für die Targetdatenbank-Verbindungen entweder MS Windows Latin1, ISO-8859-1 Western European oder UTF-16LE oder flache Dateien verwenden. Um Datenkonsistenz zu gewährleisten, muss die konfigurierte Target-Codepage der Targetdatenbank oder Einfachdatei-System-Codepage entsprechen.

Wenn Sie den PowerCenter Integration Service für entspannte Codepage-Validierung konfigurieren, entfernt der PowerCenter Integration Service Einschränkungen bei der Kompatibilität von Quell- und Target-Codepages. Sie können für Quell- und Targetdaten eine beliebige unterstützte Codepage auswählen. Sie müssen jedoch sicherstellen, dass die Targets nur Zeichendaten erhalten, die in der Target-Codepage codiert wurden.

Schritt 5. Verifizieren der Codepage-Kompatibilität für Lookup-Datenbank und Datenbank der gespeicherten Prozedur

Die Codepages der Lookup-Datenbank und der Datenbank für die gespeicherten Prozeduren müssen eine Obermenge der Quell-Codepages und eine Untermenge der Target-Codepages sein. In diesem Fall müssen alle Verbindungen zu Lookup- und Gespeicherte-Prozeduren-Datenbanken eine Codepage verwenden, die mit den Codepages ISO 8859-1 Western European oder MS Windows Latin1 kompatibel ist.

Schritt 6. Kompatibilität externer Prozedur oder benutzerdefinierter Umwandlungsprozedur prüfen

Die externen Prozedur und die benutzerdefinierten Umwandlungsprozeduren müssen die Zeichendaten aus den Quell-Codepages verarbeiten können, und sie müssen die Zeichen übergeben, die in den Target-Codepages kompatibel sind. In diesem Fall müssen alle Daten, die von externen Prozeduren oder benutzerdefinierten Umwandlungsprozeduren verarbeitet werden, den Codepages ISO 8859-1 Western European oder MS Windows Latin1 entsprechen.

Schritt 7. Konfigurieren der Sitzungs-Sortierreihenfolge

Wenn Sie den PowerCenter Integration Service im ASCII-Modus ausführen, verwendet er für alle Sitzungen eine binäre Sortierreihenfolge. In den Sitzungseigenschaften listet der PowerCenter Workflow Manager alle Sortierreihenfolgen auf, die zur Codepage des PowerCenter Integration Service gehören. Sie können eine Sortierreihenfolge für die Sitzung auswählen.

Fallstudie: Verarbeiten von Unicode UTF-16LE Daten

Diese Fallstudie beschreibt, wie Sie eine Umgebung zur Verarbeitung von Unicode UTF-16LE Multibyte-Daten einrichten können. Wenn Sie Daten westeuropäischer Sprachen, Sprachen aus dem mittleren Osten oder Asien bzw. anderer im UTF-16LE Zeichensatz verschlüsselter Sprachen zu verarbeiten haben, werden Sie Ihre Umgebung möglicherweise so konfigurieren. In diesem Beispiel wird eine Umgebung beschrieben, die Daten in deutscher und japanischer Sprache verarbeitet.

In dieser Fallstudie besteht die UTF-16LE Umgebung aus folgenden Elementen:

- PowerCenter Integration Service auf einem UNIX-Computer
- PowerCenter Clients auf Windows-Systemen
- PowerCenter Repository, gespeichert in einer Oracle-Datenbank auf UNIX
- Eine Quelldatenbank mit Daten in deutscher Sprache
- Eine Quelldatenbank mit Daten in deutscher und japanischer Sprache
- Eine Target-Datenbank mit Daten in deutscher und japanischer Sprache
- Eine Lookup-Datenbank mit deutschsprachigen Daten

Die Datenumgebung muss Daten bestehend aus deutschen und japanischen Schriftzeichen verarbeiten können.

UTF-16LE Umgebung konfigurieren

Verwenden Sie die folgenden Richtlinien, wenn Sie eine Umgebung ähnlich wie in diesem Beispiel für die UTF-16LE Datenverarbeitung konfigurieren möchten:

1. Stellen Sie die Codepage-Kompatibilität zwischen dem PowerCenter Repository Datenbank-Client und dem Datenbankserver sicher.
2. Stellen Sie die Codepage-Kompatibilität zwischen dem PowerCenter Client und dem PowerCenter Repository sicher sowie zwischen dem PowerCenter Integration Service und dem PowerCenter Repository.
3. Konfigurieren Sie den PowerCenter Integration Service für Unicode-Datenverschiebungsmodus.
4. Überprüfen Sie die Kompatibilität der Sitzungs-Codepage.
5. Prüfen Sie die Codepage-Kompatibilität für die Lookup- und Gespeicherte-Prozeduren-Datenbank.
6. Stellen Sie die Codepage-Kompatibilität externer Prozeduren oder benutzerdefinierter Transformationsprozeduren sicher.
7. Konfigurieren Sie die Sortierreihenfolge einer Sitzung.

Schritt 1. Stellen Sie die Kompatibilität von PowerCenter Repository Database Client und Server sicher

Der Datenbank-Client und Server, die das PowerCenter Repository hosten, müssen in der Lage sein, ohne Datenverlust zu kommunizieren.

Das PowerCenter Repository befindet sich in einer Oracle-Datenbank. Stellen Sie die Umgebungsvariable `NLS_LANG` auf das Gebietsschema (Sprache, Region und Zeichensatz) ein, das Datenbank-Client und Server bei der Anmeldung verwenden sollen.

```
NLS_LANG = LANGUAGE_TERRITORY.CHARACTERSET
```

Standardmäßig konfiguriert Oracle NLS_LANG für US-Englisch, das US-Territorium, und den 7-Bit ASCII-Zeichensatz:

```
NLS_LANG = AMERICAN_AMERICA.US7ASCII
```

Ändern Sie die Standard-Konfiguration, um UTF-16LE Daten mit dem Oracle UTF8-Zeichensatz in das PowerCenter Repository zu schreiben. Beispiel:

```
NLS_LANG = AMERICAN_AMERICA.UTF8
```

Weitere Informationen zum Überprüfen und Ändern der PowerCenter Repository Database-Codepage finden Sie in Ihrer Datenbank-Dokumentation.

Schritt 2. Stellen Sie die PowerCenter Codepage-Kompatibilität sicher

PowerCenter Integration Service und PowerCenter-Client-Codepages müssen Teilmengen der PowerCenter Repository Codepage sein. Da der PowerCenter-Client und PowerCenter Integration Service jeweils die System-Codepages des Computers verwenden, auf denen sie installiert sind, müssen Sie überprüfen, ob die System-Codepages Teilmengen der PowerCenter Repository Codepage sind.

In diesem Fall wurden der PowerCenter-Client auf Windows-Systemen in der Schweiz gekauft. Daher sind die System-Codepages für die PowerCenter-Client-Computer auf MS Windows Latin1 eingestellt. Um System- und Bildschirmsprachen zu überprüfen, öffnen Sie das Dialogfeld "Regionale Einstellungen" in der Windows-Systemsteuerung.

Der PowerCenter Integration Service ist auf einem UNIX-Rechner installiert. Die Standard-Codepage für das UNIX-Betriebssystem ist ASCII. In dieser Umgebung muss der UNIX-System-Zeichensatz auf UTF-16LE geändert werden.

Schritt 3. Konfigurieren des PowerCenter Integration Service für den Unicode-Datenverschiebungsmodus

Sie müssen den PowerCenter Integration Service für die Verarbeitung von UTF-16LE Daten konfigurieren. Im Administrator Tool setzen Sie den Datenverschiebungsmodus für den PowerCenter Integration Service auf Unicode. Der PowerCenter Integration Service ordnet bei der Verarbeitung von Multibyte-Zeichen jedem Zeichen ein zusätzliches Byte zu.

Schritt 4. Stellen Sie die Sitzungs-Codepage-Kompatibilität sicher

Wenn Sie einen PowerCenter-Arbeitsablauf im Unicode-Datenverschiebungsmodus ausführen, erzwingt der PowerCenter Integration Service Quell- und Target-Codepage-Beziehungen. Um genaue Datenumwandlungen zu gewährleisten, muss die Quell-Codepage eine Teilmenge der Target-Codepage sein.

In diesem Fall enthält die Umgebung eine Quelldatenbank mit deutschen und japanischen Daten. Wenn Sie eine Quelldatenbank-Verbindung im PowerCenter Workflow Manager konfigurieren, muss die Codepage für die Verbindung mit der Quelldatenbank-Codepage identisch sein. Sie können jede Codepage für die Quelldatenbank verwenden.

Da die Target-Codepage eine Obermenge der Quell-Codepages sein muss, müssen Sie für die Target-Datenbank-Verbindungen UTF-16LE oder Einfachdateien verwenden. Um Datenkonsistenz zu gewährleisten, muss die konfigurierte Target-Codepage der Target-Datenbank oder Einfachdatei-Systemcodepage entsprechen.

Wenn Sie den PowerCenter Integration Service für entspannte Codepage-Validierung konfigurieren, entfernt der PowerCenter Integration Service Einschränkungen bei der Kompatibilität von Quell- und Target-Codepages. Sie können für Quell- und Targetdaten eine beliebige unterstützte Codepage auswählen. Sie müssen jedoch sicherstellen, dass die Targets nur Zeichendaten erhalten, die in der Target-Codepage codiert wurden.

Schritt 5. Verifizieren der Codepage-Kompatibilität für Lookup-Datenbank und Datenbank der gespeicherten Prozedur

Die Codepages der Lookup-Datenbank und der Datenbank für die gespeicherten Prozeduren müssen eine Obermenge der Quell-Codepages und eine Untermenge der Target-Codepages sein. In diesem Fall müssen alle Verbindungen zu Lookup- und Gespeicherte-Prozeduren-Datenbanken eine Codepage verwenden, die mit UTF-16LE kompatibel ist.

Schritt 6. Kompatibilität externer Prozedur oder benutzerdefinierter Umwandlungsprozedur prüfen

Die externen Prozedur und die benutzerdefinierten Umwandlungsprozeduren müssen die Zeichendaten aus den Quell-Codepages verarbeiten können, und sie müssen die Zeichen übergeben, die in den Target-Codepages kompatibel sind.

In diesem Fall müssen die externe Prozedur und die benutzerdefinierten Umwandlungen die deutschen und japanischen Daten aus den Quellen verarbeiten können. Der PowerCenter Integration Service übergibt die Daten an Prozeduren jedoch in UCS-2. Aus diesem Grund müssen alle Daten, die von einer externen Prozedur oder von benutzerdefinierten Umwandlungen verarbeitet werden, dem Zeichensatz UCS-2 entsprechen.

Schritt 7. Konfigurieren der Sitzungs-Sortierreihenfolge

Wenn Sie den PowerCenter Integration Service im Unicode-Modus ausführen, verwendet er für alle Sitzungen die festgelegte Sortierreihenfolge. Standardmäßig sind die Sitzungen für eine binäre Sortierreihenfolge konfiguriert.

Um deutsche und japanische Daten zu sortieren, wenn der PowerCenter Integration Service UTF-16LE verwendet, empfiehlt es sich die binäre Sortierreihenfolge beizubehalten.

KAPITEL 18

Verwalten von Verteilungspaketen

Dieses Kapitel umfasst die folgenden Themen:

- [Verwaltung von Verteilungspaketen – Übersicht, 354](#)
- [Vorbereitungen, 354](#)
- [Installieren oder Entfernen von Verteilungspaketen im Konsolenmodus, 355](#)
- [Installieren oder Entfernen von Verteilungspaketen im automatischen Modus, 356](#)
- [Nach der Installation, 357](#)

Verwaltung von Verteilungspaketen – Übersicht

Verteilungspakete können Sie mit Integration Package Manager (dem Paketmanager) auf den Informatica-Dienst- und -Clientcomputern installieren und von diesen entfernen.

Ein Verteilungspaket ist ein Satz von Verteilungsbinarydateien, die Sie innerhalb der Domäne für die folgenden Verarbeitungsanforderungen installieren:

- Die Verarbeitung soll in die Hadoop- oder Databricks-Umgebung verlagert werden.
- Es sollen komplexe Dateien innerhalb der Informatica-Domäne verarbeitet werden.
- Es soll eine Verbindung zur Hadoop- oder Databricks-Umgebung hergestellt werden, wenn die Verarbeitung innerhalb der Informatica-Domäne stattfindet.

Sie können Verteilungspakete installieren, wenn dies während des Upgrade- oder Installationsvorgangs nicht erfolgt ist oder wenn Sie ein Verteilungspaket hinzufügen möchten. Sie können ein Verteilungspaket entfernen, wenn Sie ein anderes Paket verwenden möchten oder wenn Sie ein Paket installiert haben, das Sie nicht verwenden.

Stellen Sie beim Installieren oder Entfernen von Verteilungspaketen sicher, dass Sie den Vorgang auf allen Dienst- und Clientcomputern durchführen.

Vorbereitungen

Vor der Ausführung des Integration Package Managers führen Sie einige Aufgaben durch. So legen Sie beispielsweise Umgebungsvariablen fest und laden Dateien herunter.

1. Schließen Sie die Informatica-Dienste.

2. Legen Sie eine der folgenden Umgebungsvariablen fest:

Variable	Beschreibung
INFA_JDK_HOME	Speicherort des Ordners mit dem unterstützten Java Development Kit (JDK). Legen Sie die Umgebungsvariable INFA_JDK_HOME in den folgenden Szenarien fest: <ul style="list-style-type: none">- Die Informatica-Domäne befindet sich auf einer Windows- oder Linux-Plattform- Informatica-Client
INFA_JRE_HOME	Speicherort des Ordners, der die unterstützte Java-Laufzeitumgebung (JRE) enthält. Wenn sich die Informatica-Domäne auf der AIX-Plattform befindet, legen Sie die Umgebungsvariable INFA_JRE_HOME fest.

3. Stellen Sie sicher, dass der Benutzer, der den Paketmanager ausführt, über Lese- und Schreibberechtigungen für das Informatica-Installationsverzeichnis sowie über Ausführungsberechtigungen für die ausführbare Datei verfügt.
4. Laden Sie die folgenden Dateien von der Informatica Electronic Software-Download-Site herunter:
- [Integration Package Manager](#)
 - [Distribution packages](#)
5. Extrahieren Sie die ZIP-Datei des Integration Package Managers auf ein lokales Laufwerk.
6. Kopieren Sie die ZIP-Dateien der Verteilungspakete, die Sie benötigen, an den folgenden Speicherort:
<Integration Package Manager-Verzeichnis>/source
- Hinweis:** Der Paketmanager schlägt fehl, wenn die ZIP-Dateien für Verteilungspakete nicht im Quellverzeichnis verfügbar sind.

Installieren oder Entfernen von Verteilungspaketen im Konsolenmodus

Sie können den Integration Package Manager im Konsolenmodus ausführen, um Verteilungspakete zu installieren oder zu entfernen.

1. Führen Sie im Verzeichnis des Package Manager einen der folgenden Befehle aus:
- `./Server.sh console` für Linux oder UNIX
 - `Server.bat console` für Windows
 - `Client.bat console` für Client
- Hinweis:** Verwenden Sie die Administrator-Eingabeaufforderung, um den Befehl unter Windows auszuführen.
2. Geben Sie das Installationsverzeichnis der Dienste oder des Clients ein und drücken Sie die **Eingabetaste**.
3. Wählen Sie den Vorgangstyp aus und drücken Sie die **Eingabetaste**.
- Wählen Sie 1 aus, um die vorhandenen Verteilungspakete zu entfernen.
 - Wählen Sie 2 aus, um ein oder mehrere Verteilungspakete zu installieren.
- In der Konsole werden die Verteilungspakete aufgelistet, die Sie installieren oder entfernen können.

4. Geben Sie die Verteilungspakete ein, die installiert oder entfernt werden sollen. Trennen Sie mehrere Verteilungspakete jeweils durch ein Komma und drücken Sie die **Eingabetaste**.
5. Überprüfen Sie den Installations- oder Entfernungsstatus in der Protokolldatei des Integration Package Managers.

Sie finden die Protokolldatei im folgenden Speicherort: <Verzeichnis des Integration Package Managers>/ IntegrationPackageManager_<Datum und Zeitstempel>.log

Installieren oder Entfernen von Verteilungspaketen im automatischen Modus

Sie können den Integration Package Manager im automatischen Modus ausführen, um Verteilungspakete zu installieren oder zu entfernen. Die Eigenschaftendatei für die automatische Eingabe enthält die Eigenschaften für den Paketmanager, der für Dienste und Clients im automatischen Modus ausgeführt werden soll. Legen Sie den entsprechenden Wert für jede Eigenschaft in der Datei fest.

1. Suchen Sie die Datei „IntegrationPackageManager.properties“ im folgenden Speicherort: <Integration Package Manager-Verzeichnis>/
2. Bearbeiten Sie die Eigenschaftendatei in einem Texteditor.

In der folgenden Tabelle werden die Eigenschaften beschrieben, die Sie ändern können:

Eigenschaftsname	Beschreibung
USER_INSTALL_DIR	Das Installationsverzeichnis des Diensts oder Clients.
OPERATION_TYPE	Der Vorgang, der durchgeführt werden soll: <ul style="list-style-type: none"> - Legen Sie dies auf DELETE fest, um die vorhandenen Verteilungspakete zu entfernen. - Legen Sie dies auf EXTRACT fest, um ein oder mehrere Verteilungspakete zu installieren.
SELECTED_HADOOP_LIBRARIES	Listet die Verteilungspakete und -versionen auf. Geben Sie die Verteilungspakete ein, die installiert oder entfernt werden sollen. Trennen Sie mehrere Pakete durch ein Komma.

3. Speichern Sie die Eigenschaftendatei.
4. Führen Sie im Verzeichnis des Package Manager einen der folgenden Befehle aus:
 - `./Server.sh still` für Linux oder UNIX
 - `Server.bat silent` für Windows
 - `Client.bat silent` für Client

Hinweis: Verwenden Sie die Administrator-Eingabeaufforderung, um den Befehl unter Windows auszuführen.

5. Überprüfen Sie den Installations- oder Entfernungsstatus in der Protokolldatei des Integration Package Managers.

Sie finden die Protokolldatei im folgenden Speicherort:<Integration Package Manager-Verzeichnis>/ IntegrationPackageManager_<Datum und Zeitstempel>.log

Nach der Installation

Um die Verteilungspakete zu verwenden, die mit dem Paketmanager installiert werden, konfigurieren Sie die Eigenschaft oder Umgebungsvariable auf Dienst- und Clientcomputern.

Konfigurieren Sie das Developer Tool.

Nachdem Sie die Verteilungspakete im Developer Tool installiert haben, aktualisieren Sie die Datei „developerCore.ini“ mit dem installierten Verteilungspaket.

1. Suchen Sie die Datei „developerCore.ini“ an folgendem Speicherort: <Informatica-Installationsverzeichnis>\clients\DeveloperClient
2. Bearbeiten Sie die Datei, um folgende Eigenschaft zu aktualisieren:
`-DINFA_HADOOP_DIST_DIR=hadoop\<Hadoop distribution name>_<version>`
Beispiel:
`-DINFA_HADOOP_DIST_DIR=hadoop\CDH_7.1`
3. Starten Sie das Developer Tool neu.

Konfigurieren der Umgebungsvariablen

Einige Adapter erfordern Umgebungsvariablen für den Datenintegrationsdienst und den Metadaten-Zugriffsdienst, um auf die Verteilungspakete zuzugreifen. Weitere Informationen hierzu finden Sie unter [Configure environment variables to process complex files](#).

ANHANG A

Codepages

Dieser Anhang umfasst die folgenden Themen:

- [Unterstützte Codepages für Anwendungsdienste, 358](#)
- [Unterstützte Codepages für Quellen und Ziele, 360](#)

Unterstützte Codepages für Anwendungsdienste

Informatica unterstützt die Codepages aus Gründen der Internationalisierung. Zum globalen Support verwendet Informatica die internationalen Komponenten für Unicode (ICU). Eine Liste der Codepage-Aliase in ICU finden Sie unter <http://demo.icu-project.org/icu-bin/convexp>.

Wenn Sie im Administrator-Tool eine Anwendungsdienst-Codepage zuweisen, wählen Sie die Codepage-Beschreibung aus.

Sie müssen mit UTF-8 kompatible Codepages für die Domäne, den Modellrepository-Dienst und für jeden Datenintegrationsdienst-Prozess verwenden.

Die nachstehende Tabelle gibt den Namen, eine Beschreibung und die ID für die unterstützten Codepages für PowerCenter-Repository-Dienst, Metadata Manager-Dienst und jeden PowerCenter-Integrationsdienst-Prozess an:

Name	Beschreibung	ID
IBM-037	IBM EBCDIC US Englisch	2028
IBM-1047	IBM EBCDIC US Englisch IBM1047	1047
IBM-273	IBM EBCDIC Deutsch	2030
IBM-280	IBM EBCDIC Italienisch	2035
IBM-285	IBM EBCDIC UK Englisch	2038
IBM-297	IBM EBCDIC Französisch	2040
IBM-500	IBM EBCDIC Internationales Lateinisch-1	2044
IBM-930	IBM EBCDIC Japanisch	930

Name	Beschreibung	ID
IBM-935	IBM EBCDIC Vereinfachtes Chinesisch	935
IBM-937	IBM EBCDIC Traditionelles Chinesisch	937
IBM-939	IBM EBCDIC Japanisch CP939	939
ISO-8859-10	ISO 8859-10 Lateinisch 6 (Nordisch)	13
ISO-8859-15	ISO 8859-15 Lateinisch 9 (Westeuropäisch)	201
ISO-8859-2	ISO 8859-2 Osteuropäisch	5
ISO-8859-3	ISO 8859-3 Süd-osteuropäisch	6
ISO-8859-4	ISO 8859-4 Baltisch	7
ISO-8859-5	ISO 8859-5 Kyrillisch	8
ISO-8859-6	ISO 8859-6 Arabisch	9
ISO-8859-7	ISO 8859-7 Griechisch	10
ISO-8859-8	ISO 8859-8 Hebräisch	11
ISO-8859-9	ISO 8859-9 Lateinisch 5 (Türkisch)	12
JapanEUC	Japanische erweiterte UNIX-Codierung (einschließlich JIS X 0212)	18
Latin-1	ISO 8859-1 Westeuropäisch	4
MS1250	MS Windows Lateinisch 2 (Zentraleuropa)	2250
MS1251	MS Windows Kyrillisch (Slawisch)	2251
MS1252	MS Windows Lateinisch 1 (ANSI), übergeordneter Zeichensatz von Lateinisch 1	2252
MS1253	MS Windows Griechisch	2253
MS1254	MS Windows Lateinisch 5 (Türkisch), übergeordneter Zeichensatz von ISO 8859-9	2254
MS1255	MS Windows Hebräisch	2255
MS1256	MS Windows Arabisch	2256
MS1257	MS Windows Ostseeanrainer	2257
MS1258	MS Windows Vietnamesisch	2258
MS1361	MS Windows Koreanisch (Johab)	1361
MS874	MS-DOS Thailändisch, übergeordneter Zeichensatz von TIS 620	874

Name	Beschreibung	ID
MS932	MS Windows Japanisch, Umsch-JIS	2024
MS936	MS Windows Vereinfachtes Chinesisch, übergeordneter Zeichensatz von GB 2312-80, EUC Codierung	936
MS949	MS Windows Koreanisch, übergeordneter Zeichensatz von KS C 5601-1992	949
MS950	MS Windows Traditionelles Chinesisch, übergeordneter Zeichensatz von Big 5	950
US-ASCII	7-Bit-ASCII	1
UTF-8	UTF 8-Kodierung von Unicode	106

Unterstützte Codepages für Quellen und Ziele

Informatica unterstützt die Codepages aus Gründen der Internationalisierung. Zum globalen Support verwendet Informatica die internationalen Komponenten für Unicode (ICU). Eine Liste der Codepages-Aliase in ICU finden Sie unter <http://demo.icu-project.org/icu-bin/convexp>

Wenn Sie im PowerCenter Client eine Quelle oder ein Ziel zuweisen, wählen Sie die Codepage-Beschreibung aus. Wenn Sie eine Codepage mit dem Befehl *pmrep* CreateConnection zuweisen oder die Codepage in einer Parameterdatei definieren, geben Sie den Codepage-Namen ein. Die nachstehende Tabelle gibt den Namen, eine Beschreibung und die ID für die unterstützten Codepages für Quellen und Ziele an:

Name	Beschreibung	ID
Adobe-Standard-Encoding	Adobe Standardcodierung	10073
BOCU-1	Binär geordnete Komprimierung für Unicode (BOCU-1)	10010
CESU-8	ICompatibility Codierungsschema für UTF-16 (CESU-8)	10011
cp1006	ISO Urdu	10075
cp1098	PC Farsi	10076
cp1124	ISO Kyrillisch Ukraine	10077
cp1125	PC Kyrillisch Ukraine	10078
cp1131	PC Kyrillisch Weißrussland	10080
cp1381	PC Chinesisch GB (S-Ch Mischdaten)	10082
cp850	PC Lateinisch1	10036

Name	Beschreibung	ID
cp851	PC DOS Griechisch (ohne Euro)	10037
cp856	PC Hebräisch (alt)	10040
cp857	PC Lateinisch5 (ohne Euroaktualisierung)	10041
cp858	PC Lateinisch1 (mit Euroaktualisierung)	10042
cp860	PC Portugal	10043
cp861	PC Island	10044
cp862	PC Hebräisch (ohne Euroaktualisierung)	10045
cp863	PC Kanadisches Französisch	10046
cp864	PC Arabisch (ohne Euroaktualisierung)	10047
cp865	PC Nordisch	10048
cp866	PC Russisch (ohne Euroaktualisierung)	10049
cp868	PC Urdu	10051
cp869	PC Griechisch (ohne Euroaktualisierung)	10052
cp922	IPC Estnisch (ohne Euroaktualisierung)	10056
cp949c	PC Koreanisch - KS	10028
ebcdic-xml-us	EBCDIC US (mit Euro) - Erweiterung für XML4C(Xerces)	10180
EUC-KR	EUC Koreanisch	10029
GB_2312-80	Vereinfachtes Chinesisch (GB2312-80)	10025
gb18030	GB 18030 MBCS Codepage	1392
GB2312	Chinesisches EUC	10024
HKSCS	Hongkong erweiterter Zeichensatz	9200
hp-roman8	HP Lateinisch1	10072
HZ-GB-2312	Vereinfachtes Chinesisch (HZ GB2312)	10092
IBM-037	IBM EBCDIC US Englisch	2028
IBM-1025	EBCDIC Kyrrillisch	10127
IBM-1026	EBCDIC Türkei	10128
IBM-1047	IBM EBCDIC US Englisch IBM1047	1047

Name	Beschreibung	ID
IBM-1047-s390	EBCDIC IBM-1047 für S/390 (LF und NL zwischengespeichert)	10167
IBM-1097	EBCDIC Farsi	10129
IBM-1112	EBCDIC Baltisch	10130
IBM-1122	EBCDIC Estland	10131
IBM-1123	EBCDIC Kyrillisch Ukraine	10132
IBM-1129	ISO Vietnamesisch	10079
IBM-1130	EBCDIC Vietnamesisch	10133
IBM-1132	EBCDIC Laotisch	10134
IBM-1133	ISO Laotisch	10081
IBM-1137	EBCDIC Devanagari	10163
IBM-1140	EBCDIC US (mit Euroaktualisierung)	10135
IBM-1140-s390	EBCDIC IBM-1140 für S/390 (LF und NL zwischengespeichert)	10168
IBM-1141	EBCDIC Deutschland, Österreich (mit Euroaktualisierung)	10136
IBM-1142	EBCDIC Dänemark, Norwegen (mit Euroaktualisierung)	10137
IBM-1142-s390	EBCDIC IBM-1142 für S/390 (LF und NL zwischengespeichert)	10169
IBM-1143	EBCDIC Finnland, Schweden (mit Euroaktualisierung)	10138
IBM-1143-s390	EBCDIC IBM-1143 für S/390 (LF und NL zwischengespeichert)	10170
IBM-1144	EBCDIC Italien (mit Euroaktualisierung)	10139
IBM-1144-s390	EBCDIC IBM-1144 für S/390 (LF und NL zwischengespeichert)	10171
IBM-1145	EBCDIC Spanien, Lateinamerika (mit Euroaktualisierung)	10140
IBM-1145-s390	EBCDIC IBM-1145 für S/390 (LF und NL zwischengespeichert)	10172
IBM-1146	EBCDIC Großbritannien, Irland (mit Euroaktualisierung)	10141
IBM-1146-s390	EBCDIC IBM-1146 für S/390 (LF und NL zwischengespeichert)	10173
IBM-1147	EBCDIC Frankreich (mit Euroaktualisierung)	10142
IBM-1147-s390	EBCDIC IBM-1147 für S/390 (LF und NL zwischengespeichert)	10174
IBM-1147-s390	EBCDIC IBM-1147 für S/390 (LF und NL zwischengespeichert)	10174
IBM-1148	EBCDIC Internationales Lateinisch1 (mit Euroaktualisierung)	10143

Name	Beschreibung	ID
IBM-1148-s390	EBCDIC IBM-1148 für S/390 (LF und NL zwischengespeichert)	10175
IBM-1149	EBCDIC Island (mit Euroaktualisierung)	10144
IBM-1149-s390	IEBCDIC IBM-1149 für S/390 (LF und NL zwischengespeichert)	10176
IBM-1153	EBCDIC Lateinisch2 (mit Euroaktualisierung)	10145
IBM-1153-s390	EBCDIC IBM-1153 für S/390 (LF und NL zwischengespeichert)	10177
IBM-1154	EBCDIC Mehrsprachiges Kyrillisch (mit Euroaktualisierung)	10146
IBM-1155	EBCDIC Türkei (mit Euroaktualisierung)	10147
IBM-1156	EBCDIC Mehrsprachiges Baltisch (mit Euroaktualisierung)	10148
IBM-1157	EBCDIC Estnisch (mit Euroaktualisierung)	10149
IBM-1158	EBCDIC Kyrillisch Ukraine (mit Euroaktualisierung)	10150
IBM-1159	IBM EBCDIC Taiwan, traditionelles Chinesisch	11001
IBM-1160	EBCDIC Thailändisch (mit Euroaktualisierung)	10151
IBM-1162	Thailändisch (mit Euroaktualisierung)	10033
IBM-1164	EBCDIC Vietnamesisch (mit Euroaktualisierung)	10152
IBM-1250	MS Windows Lateinisch2 (ohne Euroaktualisierung)	10058
IBM-1251	MS Windows Kyrillisch (ohne Euroaktualisierung)	10059
IBM-1255	MS Windows Hebräisch (ohne Euroaktualisierung)	10060
IBM-1256	MS Windows Arabisch (ohne Euroaktualisierung)	10062
IBM-1257	MS Windows Baltisch (ohne Euroaktualisierung)	10064
IBM-1258	MS Windows Vietnamesisch (ohne Euroaktualisierung)	10066
IBM-12712	EBCDIC Hebräisch (aktualisiert für Euro und neuen Shekel, Steuerzeichen)	10161
IBM-12712-s390	EBCDIC IBM-12712 für S/390 (LF und NL zwischengespeichert)	10178
IBM-1277	Adobe Lateinisch1-Codierung	10074
IBM-13121	IBM EBCDIC Erweitertes Koreanisch CP13121	11002
IBM-13124	IBM EBCDIC Vereinfachtes Chinesisch CP13124	11003
IBM-1363	PC Koreanisch KSC MBCS erweitert (mit \ <-> Won-Zuordnung)	10032

Name	Beschreibung	ID
IBM-1364	EBCDIC Erweitertes Koreanisch (SBCS IBM-13121 kombiniert mit DBCS IBM-4930)	10153
IBM-1371	EBCDIC Erweitertes Taiwanesisch (SBCS IBM-1159 kombiniert mit DBCS IBM-9027)	10154
IBM-1373	Taiwan Big-5 (mit Euroaktualisierung)	10019
IBM-1375	MS Taiwan Big-5 mit HKSCS-Erweiterungen	10022
IBM-1386	PC Chinesisch GBK (IBM-1386)	10023
IBM-1388	EBCDIC Chinesisch GB (S-Ch DBCS-Hostdaten)	10155
IBM-1390	EBCDIC Japanisches Katakana (mit Euroaktualisierung)	10156
IBM-1399	EBCDIC Japanisches Lateinisches-Kanji (mit Euroaktualisierung)	10157
IBM-16684	EBCDIC Erweitertes Japanisch (DBCS IBM-1390 kombiniert mit DBCS IBM-1399)	10158
IBM-16804	EBCDIC Arabisch (mit Euroaktualisierung)	10162
IBM-16804-s390	EBCDIC IBM-16804 für S/390 (LF und NL zwischengespeichert)	10179
IBM-25546	ISO-2022 Codierung für Koreanisch (Erweiterung 1)	10089
IBM-273	IBM EBCDIC Deutsch	2030
IBM-277	EBCDIC Dänemark, Norwegen	10115
IBM-278	EBCDIC Finnland, Schweden	10116
IBM-280	IBM EBCDIC Italienisch	2035
IBM-284	EBCDIC Spanien, Lateinamerika	10117
IBM-285	IBM EBCDIC UK Englisch	2038
IBM-290	EBCDIC Japanisches Katakana SBCS	10118
IBM-297	IBM EBCDIC Französisch	2040
IBM-33722	Japanisches EUC (mit \ <-> Yen-Zuordnung)	10017
IBM-367	IBM-367	10012
IBM-37-s390	EBCDIC IBM-37 für S/390 (LF und NL zwischengespeichert)	10166
IBM-420	EBCDIC Arabisch	10119
IBM-424	EBCDIC Hebräisch (aktualisiert für neuen Shekel, Steuerzeichen)	10120

Name	Beschreibung	ID
IBM-437	PC USA	10035
IBM-4899	EBCDIC Hebräisch (mit Euroaktualisierung)	10159
IBM-4909	ISO Griechisch (mit Euroaktualisierung)	10057
IBM-4933	IBM Vereinfachtes Chinesisch CP4933	11004
IBM-4971	EBCDIC Griechisch (mit Euroaktualisierung)	10160
IBM-500	IBM EBCDIC Internationales Lateinisch-1	2044
IBM-5050	Japanisches EUC (gepacktes Format)	10018
IBM-5123	EBCDIC Japanisches Lateinisch (mit Euroaktualisierung)	10164
IBM-5351	MS Windows Hebräisch (frühere Version)	10061
IBM-5352	MS Windows Arabisch (frühere Version)	10063
IBM-5353	MS Windows Baltisch (frühere Version)	10065
IBM-803	EBCDIC Hebräisch	10121
IBM-833	IBM EBCDIC Koreanisch CP833	833
IBM-834	IBM EBCDIC Koreanisch CP834	834
IBM-835	IBM Taiwan, traditionelles Chinesisch CP835	11005
IBM-836	IBM EBCDIC Vereinfachtes Chinesisch	11006
IBM-837	IBM Vereinfachtes Chinesisch CP837	11007
IBM-838	EBCDIC Thailändisch	10122
IBM-8482	EBCDIC Japanisches Katakana SBCS (mit Euroaktualisierung)	10165
IBM-852	PC Lateinisch2 (ohne Euroaktualisierung)	10038
IBM-855	PC Kyrillisch (ohne Euroaktualisierung)	10039
IBM-867	PC Hebräisch (mit Euroaktualisierung)	10050
IBM-870	EBCDIC Lateinisch2	10123
IBM-871	EBCDIC Island	10124
IBM-874	PC Thailand (ohne Euroaktualisierung)	10034
IBM-875	EBCDIC Griechisch	10125
IBM-901	PC Baltisch (mit Euroaktualisierung)	10054

Name	Beschreibung	ID
IBM-902	PC Estnisch (mit Euroaktualisierung)	10055
IBM-918	EBCDIC Urdu	10126
IBM-930	IBM EBCDIC Japanisch	930
IBM-933	IBM EBCDIC Koreanisch CP933	933
IBM-935	IBM EBCDIC Vereinfachtes Chinesisch	935
IBM-937	IBM EBCDIC Traditionelles Chinesisch	937
IBM-939	IBM EBCDIC Japanisch CP939	939
IBM-942	PC Japanisch SJIS-78 Syntax (IBM-942)	10015
IBM-943	PC Japanisch SJIS-90 (IBM-943)	10016
IBM-949	PC Koreanisch - KS (Standard)	10027
IBM-950	Taiwan Big-5 (ohne Euroaktualisierung)	10020
IBM-964	EUC Taiwan	10026
IBM-971	EUC Koreanisch (nur DBCS)	10030
IMAP-Mailboxname	IMAP-Mailboxname	10008
is-960	Israelischer Standard 960 (7-Bit Hebräisch-Codierung)	11000
ISO-2022-CN	ISO-2022 Codierung für Chinesisch	10090
ISO-2022-CN-EXT	ISO-2022 Codierung für Chinesisch (Erweiterung 1)	10091
ISO-2022-JP	ISO-2022 Codierung für Japanisch	10083
ISO-2022-JP-2	ISO-2022 Codierung für Japanisch (Erweiterung 2)	10085
ISO-2022-KR	ISO-2022 Codierung für Koreanisch	10088
ISO-8859-10	ISO 8859-10 Lateinisch 6 (Nordisch)	13
ISO-8859-13	ISO 8859-13 PC Baltisch (ohne Euroaktualisierung)	10014
ISO-8859-15	ISO 8859-15 Lateinisch 9 (Westeuropäisch)	201
ISO-8859-2	ISO 8859-2 Osteuropäisch	5
ISO-8859-3	ISO 8859-3 Süd-osteuropäisch	6
ISO-8859-4	ISO 8859-4 Baltisch	7
ISO-8859-5	ISO 8859-5 Kyrillisch	8

Name	Beschreibung	ID
ISO-8859-6	ISO 8859-6 Arabisch	9
ISO-8859-7	ISO 8859-7 Griechisch	10
ISO-8859-8	ISO 8859-8 Hebräisch	11
ISO-8859-9	ISO 8859-9 Lateinisch 5 (Türkisch)	12
JapanEUC	Japanische erweiterte UNIX-Codierung (einschließlich JIS X 0212)	18
JEF	Japanisch EBCDIC Fujitsu	9000
JEF-K	Japanisch EBCDIC-Kana Fujitsu	9005
JIPSE	NEC ACOS JIPSE Japanisch	9002
JIPSE-K	NEC ACOS JIPSE-Kana Japanisch	9007
JIS_Encoding	ISO-2022 Codierung für Japanisch (Erweiterung 1)	10084
JIS_X0201	ISO-2022 Codierung für Japanisch (JIS_X0201)	10093
JIS7	ISO-2022 Codierung für Japanisch (Erweiterung 3)	10086
JIS8	ISO-2022 Codierung für Japanisch (Erweiterung 4)	10087
JP-EBCDIC	EBCDIC Japanisch	9010
JP-EBCDIK	EBCDIK Japanisch	9011
KEIS	HITACHI KEIS Japanisch	9001
KEIS-K	HITACHI KEIS-Kana Japanisch	9006
KOI8-R	IRussisch Internet	10053
KSC_5601	PC Koreanisch KSC MBCS erweitert (KSC_5601)	10031
Latin-1	ISO 8859-1 Westeuropäisch	4
LMBCS-1	Lotus MBCS Codierung für PC Lateinisch1	10103
LMBCS-11	Lotus MBCS Codierung für MS-DOS Thailändisch	10110
LMBCS-16	Lotus MBCS Codierung für Windows Japanisch	10111
LMBCS-17	Lotus MBCS Codierung für Windows Koreanisch	10112
LMBCS-18	Lotus MBCS Codierung für Windows Chinesisch (Traditionell)	10113
LMBCS-19	Lotus MBCS Codierung für Windows Chinesisch (vereinfacht)	10114

Name	Beschreibung	ID
LMBCS-2	Lotus MBCS Codierung für PC DOS Griechisch	10104
LMBCS-3	Lotus MBCS Codierung für Windows Hebräisch	10105
LMBCS-4	Lotus MBCS Codierung für Windows Arabisch	10106
LMBCS-5	Lotus MBCS Codierung für Windows Kyrillisch	10107
LMBCS-6	Lotus MBCS Codierung für PC Lateinisch2	10108
LMBCS-8	Lotus MBCS Codierung für Windows Türkisch	10109
Macintosh	Apple Lateinisch 1	10067
MELCOM	MITSUBISHI MELCOM Japanisch	9004
MELCOM-K	MITSUBISHI MELCOM-Kana Japanisch	9009
MS1250	MS Windows Lateinisch 2 (Zentraleuropa)	2250
MS1251	MS Windows Kyrillisch (Slawisch)	2251
MS1252	MS Windows Lateinisch 1 (ANSI), übergeordneter Zeichensatz von Lateinisch 1	2252
MS1253	MS Windows Griechisch	2253
MS1254	MS Windows Lateinisch 5 (Türkisch), übergeordneter Zeichensatz von ISO 8859-9	2254
MS1255	MS Windows Hebräisch	2255
MS1256	MS Windows Arabisch	2256
MS1257	MS Windows Ostseeanrainer	2257
MS1258	MS Windows Vietnamesisch	2258
MS1361	MS Windows Koreanisch (Johab)	1361
MS874	MS-DOS Thailändisch, übergeordneter Zeichensatz von TIS 620	874
MS932	MS Windows Japanisch, Umsch-JIS	2024
MS936	MS Windows Vereinfachtes Chinesisch, übergeordneter Zeichensatz von GB 2312-80, EUC Codierung	936
MS949	MS Windows Koreanisch, übergeordneter Zeichensatz von KS C 5601-1992	949
MS950	MS Windows Traditionelles Chinesisch, übergeordneter Zeichensatz von Big 5	950
SCSU	Standardkomprimierungsschema für Unicode (SCSU)	10009

Name	Beschreibung	ID
UNISYS	UNISYS Japanisch	9003
UNISYS-K	UNISYS-Kana Japanisch	9008
US-ASCII	7-Bit-ASCII	1
UTF-16_OppositeEndian	UTF-16 Codierung von Unicode (entgegengesetztes Plattform-Endian)	10004
UTF-16_PlatformEndian	UTF-16 Codierung von Unicode (Plattform-Endian)	10003
UTF-16BE	UTF-16 Codierung von Unicode (Big Endian)	1200
UTF-16LE	UTF-16 Codierung von Unicode (Lower Endian)	1201
UTF-32_OppositeEndian	UTF-32 Codierung von Unicode (entgegengesetztes Plattform-Endian)	10006
UTF-32_PlatformEndian	UTF-32 Codierung von Unicode (Plattform-Endian)	10005
UTF-32BE	UTF-32 Codierung von Unicode (Plattform-Endian)	10001
UTF-32LE	UTF-32 Codierung von Unicode (Lower Endian)	10002
UTF-7	UTF-7-Kodierung von Unicode	10007
UTF-8	UTF 8-Kodierung von Unicode	106
windows-57002	Indischer Skriptcode zum Informationsaustausch - Devanagari	10094
windows-57003	Indischer Skriptcode zum Informationsaustausch - Bengalisch	10095
windows-57004	Indischer Skriptcode zum Informationsaustausch - Tamilisch	10099
windows-57005	Indischer Skriptcode zum Informationsaustausch - Telugu	10100
windows-57007	Indischer Skriptcode zum Informationsaustausch - Oriya	10098
windows-57008	Indischer Skriptcode zum Informationsaustausch - Kannada	10101
windows-57009	Indischer Skriptcode zum Informationsaustausch - Malayalam	10102
windows-57010	Indischer Skriptcode zum Informationsaustausch - Gujarati	10097
windows-57011	Indischer Skriptcode zum Informationsaustausch - Gurumukhi	10096
x-mac-centraleurroman	Apple Zentraleuropa	10070
x-mac-cyrillic	Apple Kyrillisch	10069

Name	Beschreibung	ID
x-mac-greek	Apple Griechisch	10068
x-mac-turkish	Apple Türkisch	10071

Einschränkungen für quell- und zielseitige Codepages

Beachten Sie bei der Zuweisung von Codepages in der Quelle oder im Ziel die folgenden Einschränkungen:

- Wählen Sie IBM EBCDIC als Code für Ihre Quelldatenbankverbindung nur dann, wenn Sie auf EBCDIC-Daten zugreifen, zum Beispiel auf Daten aus einer extrahierten Großrechnerdatei.
- Die folgenden Codepages werden nicht für Datenbank- oder relationale Verbindungen unterstützt:
 - UTF-16 Codierung von Unicode (entgegengesetztes Plattform-Endian)
 - UTF-16 Codierung von Unicode (Plattform-Endian)
 - UTF-16 Codierung von Unicode (Big Endian)
 - UTF-16 Codierung von Unicode (Lower Endian)

ANHANG B

Benutzerdefinierte Rollen

Dieser Anhang umfasst die folgenden Themen:

- [Benutzerdefinierte Rolle für den Analyst-Dienst, 371](#)
- [Benutzerdefinierte Rollen für den Metadata Manager-Dienst, 372](#)
- [Benutzerdefinierte Rolle für den Operator, 374](#)
- [PowerCenter-Repository-Dienst - Benutzerdefinierte Rollen, 375](#)
- [Benutzerdefinierte Rollen für den Test Data Manager, 376](#)

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

Konnektivität der Informatica-Plattform

Dieser Anhang umfasst die folgenden Themen:

- [Konnektivität der Informatica-Plattform - Übersicht, 380](#)
- [Domänen-Konnektivität, 381](#)
- [PowerCenter-Konnektivität, 383](#)
- [Native Konnektivität, 388](#)
- [ODBC-Konnektivität, 388](#)
- [JDBC-Konnektivität, 389](#)

Konnektivität der Informatica-Plattform - Übersicht

Die Informatica-Plattform verwendet die folgenden Konnektivitätstypen, um zwischen Clients, Diensten und anderen Komponenten in der Domäne zu kommunizieren:

TCP/IP-Netzwerkprotokoll

Anwendungsdienste und die Dienstmanager in einer Domäne verwenden TCP/IP-Netzwerkprotokoll zur Kommunikation mit anderen Knoten und Diensten. Auch die Clients verwenden TCP/IP, um mit Anwendungsdiensten zu kommunizieren. Wenn Sie Informatica-Dienste installieren, können Sie Hostnamen und Portnummer für die TCP/IP-Kommunikation auf einem Knoten konfigurieren. Sie können die Portnummern, die für Dienste auf einem Knoten verwendet werden, während der Installation oder im Informatica Administrator konfigurieren.

Native Treiber

Der Datenintegrationsdienst verwendet native Treiber, um mit Datenbanken zu kommunizieren. Der PowerCenter-Integrationsdienst und der PowerCenter-Repository-Dienst verwenden native Treiber, um mit Datenbanken zu kommunizieren. Native Treiber werden mit dem Datenbankserver und der Clientsoftware geliefert. Installieren und konfigurieren Sie die native Datenbank-Clientsoftware auf den Rechnern, auf denen die Dienste ausgeführt werden.

ODBC

Die ODBC-Treiber werden mit den Informatica-Diensten und Informatica-Clients installiert. Die Integrationsdienste verwenden ODBC-Treiber, um mit Datenbanken zu kommunizieren.

JDBC

Der Modellrepository-Dienst verwendet JDBC, um eine Verbindung mit der Modellrepository-Datenbank herzustellen. Der Metadata Manager-Dienst verwendet JDBC, um eine Verbindung mit dem Metadata Manager-Repository und Metadaten-Quellen-Repositorys herzustellen.

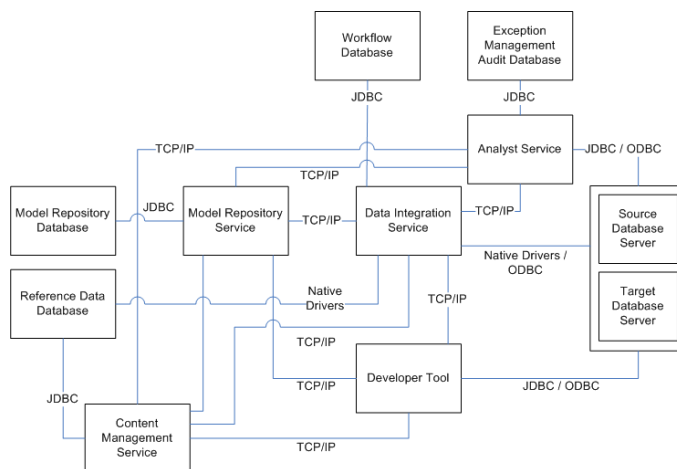
Die Gateway-Knoten in der Informatica-Domäne verwenden JDBC, um eine Verbindung mit dem Domänenkonfigurations-Repository herzustellen.

Domänen-Konnektivität

Dienste auf einem Knoten in einer Informatica-Domäne stellen mittels TCP/IP eine Verbindung zu Diensten auf anderen Knoten her. Da Dienste auf mehreren Knoten in einer Domäne ausgeführt werden können, berufen sie sich zum Weiterleiten von Anfragen auf den Dienstmanager. Der Dienstmanager auf dem Master-Gateway-Knoten wickelt Anfragen für Dienste ab und antwortet mit der Adresse des angefragten Dienstes.

Knoten kommunizieren mittels TCP/IP an dem Port, den Sie bei Installation von Informatica-Diensten für einen Knoten auswählen. Bei der Erstellung eines Knotens wählen Sie eine Portnummer für den Knoten aus. An diesem Port wartet der Dienstmanager auf eingehende TCP/IP-Verbindungen.

Die folgende Abbildung zeigt eine Übersicht der Konnektivität für Komponenten in:



Die Plattform nutzt Verbindungsobjekte, um Konnektivitätsdaten für Quell- und Zieldatenbanken zu definieren. Die Verbindungsobjekte können native oder ODBC-Konnektivität verwenden. Der Datenintegrationsdienst verwendet Verbindungsobjekte, um eine Verbindung zu Quellen und Zielen herzustellen.

Dienste und Clients stellen Verbindungen folgendermaßen her:

Modellrepository-Dienst

Der Modellrepository-Dienst verwendet JDBC zum Lesen oder Schreiben von Daten und Metadaten im Modellrepository. Er verwendet TCP/IP, um mit dem Datenintegrationsdienst und den Clients zu kommunizieren.

Datenintegrationsdienst

Der Datenintegrationsdienst verwendet ODBC oder native Treiber zum Herstellen einer Verbindung sowie zum Auslesen von Daten aus einer Quelldatenbank und Speichern der Daten in einer Zieldatenbank. Für

die Kommunikation mit dem Modellrepository-Dienst, dem Content-Managementdienst und den Client-Anwendungen wird TCP/IP genutzt.

Informatica Developer

Das Developer Tool verwendet TCP/IP, um Datenumwandlungsanfragen an den Datenintegrationsdienst zu senden. TCP/IP wird für die Kommunikation mit dem Content-Managementdienst eingesetzt, um Referenztabelle und Dateien probabilistischer Modelle zu verwalten sowie Konfigurations- und Statusinformationen für Identitätspopulationsdateien und Dateien mit Adressvalidierungsreferenzdaten abzurufen. Wenn Sie sich eine Vorschau der Mappings oder Datenobjekte im Developer Tool anzeigen lassen, verwendet es JDBC- oder ODBC-Treiber, um eine Verbindung zu der Quell- oder Zieldatenbank herzustellen und die für die Vorschau erforderlichen Metadaten abzurufen.

Informatica Analyst

Der Analyst-Dienst verwendet TCP/IP, um Anfragen an den Datenintegrationsdienst zu senden. Es nutzt TCP/IP für die Kommunikation mit dem Content-Managementdienst zum Verwalten von Referenztabelle. Wenn ein Analyst Tool-Benutzer eine Vorschau von Profilen oder Objekten anzeigt, ruft der Analyst-Dienst die für die Vorschau benötigten Metadaten aus der Quell- oder Zieldatenbank ab. Der Analyst-Dienst verwendet JDBC- oder ODBC-Treiber für die Verbindung zur Quell- oder Zieldatenbank.

Wenn Sie ODBC verwenden, um eine Verbindung zu der Quell- oder Zieldatenbank herzustellen, dann installieren Sie den ODBC-Treiber auf dem Knoten, auf dem der Analyst-Dienst läuft.

Der Analyst-Dienst kann auch eine Verbindung zu einer Ausnahmeverwaltungs-Audit-Datenbank herstellen. Die Ausnahmeverwaltungs-Audit-Datenbank ist ein zentralisierter Audit-Trail für die Arbeit, die Analyst Tool-Benutzer an Human-Task-Instanzen vornehmen. Der Analyst-Dienst verwendet JDBC-Treiber für die Verbindung zur Ausnahmeverwaltung-Audit-Datenbank.

Content-Managementdienst

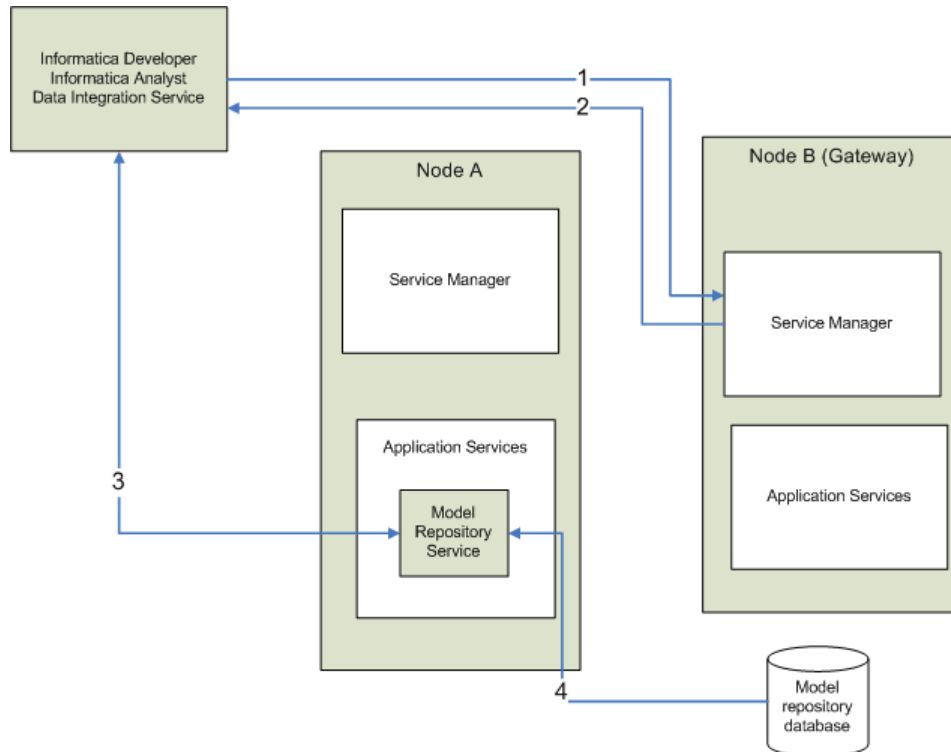
Der Content-Managementdienst verwaltet die Speicherorte und andere Eigenschaften für Referenzdaten. Der Content-Managementdienst verwendet TCP/IP zur Kommunikation mit dem Datenintegrationsdienst, um Daten in Referenztabelle zu lesen und zu schreiben. Der Content-Managementdienst verwendet JDBC zur direkten Kommunikation mit dem Referenzdaten-Warehouse beim Erstellen der Referenztabelle.

Wenn mehrere Instanzen eines Content-Managementdienst in einer Informatica-Domäne existieren, aktualisiert die Masterversion des Content Managementdienstes den Datenintegrationsdienst. Die Masterversion des Content-Managementdienst verwendet TCP/IP zur Kommunikation mit dem Domänendienst, um den zu verwendenden Modellrepository-Dienst und Datenintegrationsdienst zu ermitteln.

Model Repository-Konnektivität

Der Model Repository Service stellt mithilfe von JDBC-Treibern eine Verbindung zum Model-Repository her. Informatica Developer, Informatica Analyst, Informatica Administrator und der Data Integration Service kommunizieren über TCP/IP mit dem Model Repository Service. Informatica Developer, Informatica Analyst und Data Integration Service sind Model-Repository-Clients.

In der nachstehenden Abbildung ist dargestellt, wie ein Model-Repository-Client eine Verbindung zur Model-Repository-Datenbank herstellt:



1. Ein Model-Repository-Client sendet eine Repository-Verbindungsanfrage an den Master-Gateway-Knoten; dieser stellt den Einstiegspunkt in die Domäne dar.
2. Der Service Manager sendet den Hostnamen und die Portnummer des Knotens zurück, auf dem der Model Repository Service ausgeführt wird. Im Diagramm wird der Model Repository Service auf Knoten A ausgeführt.
3. Der Repository-Client stellt eine TCP/IP-Verbindung mit dem Model Repository Service-Prozess auf Knoten A her.
4. Der Model Repository Service-Prozess kommuniziert über JDBC mit der Model-Repository-Datenbank. Basierend auf den Anfragen vom Model Repository-Client speichert der Model Repository Service-Prozess Objekte in oder ruft Objekte aus der Model-Repository-Datenbank ab.

Hinweis: Die Tabellen im Model-Repository verfügen über eine offene Architektur. Sie können die Repository-Tabellen zwar anzeigen, dürfen Sie jedoch niemals mittels anderer Dienstprogramme manuell ändern. Informatica haftet nicht für beschädigte Daten aufgrund von an den Repository-Tabellen oder den sich darin befindlichen Daten vorgenommenen Änderungen.

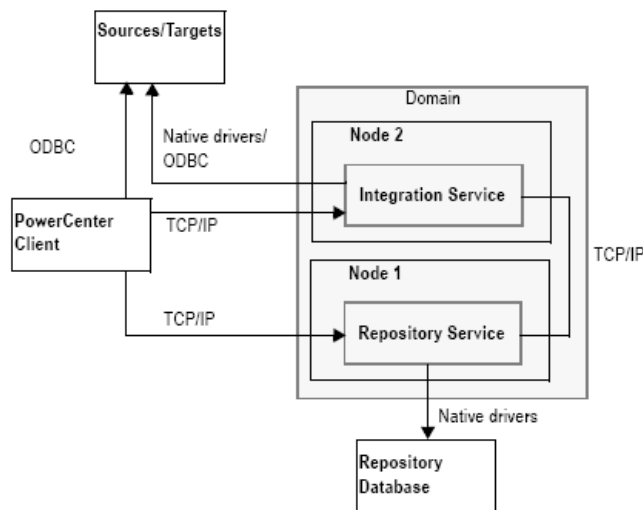
PowerCenter-Konnektivität

PowerCenter verwendet das TCP/IP-Netzwerkprotokoll, native Datenbanktreiber, ODBC und JDBC für die Kommunikation zwischen den folgenden PowerCenter-Komponenten:

- **PowerCenter-Repository-Dienst.** Der PowerCenter-Repository-Dienst verwendet native Treiber zum Kommunizieren mit dem PowerCenter-Repository. Der PowerCenter-Repository-Dienst verwendet TCP/IP zum Kommunizieren mit anderen PowerCenter-Komponenten.

- **PowerCenter-Integrationsdienst.** Der PowerCenter-Integrationsdienst verwendet die native Datenbankkonnektivität und ODBC zum Herstellen einer Verbindung zu Quell- und Zieldatenbanken. Der PowerCenter-Integrationsdienst verwendet TCP/IP zum Kommunizieren mit anderen PowerCenter-Komponenten.
- **Metadata Manager-Dienst.** Metadata Manager verwendet JDBC und ODBC für den Zugriff auf Datenquellen und Repositories.
- **PowerCenter Client.** PowerCenter Client verwendet ODBC zum Herstellen einer Verbindung zu Quell- und Zieldatenbanken. PowerCenter Client verwendet TCP/IP zur Kommunikation mit dem PowerCenter-Repository-Dienst und dem PowerCenter-Integrationsdienst.

Die nachstehende Abbildung bietet einen Überblick über die PowerCenter-Komponenten und -Konnektivität:



In der folgenden Tabelle sind die von den PowerCenter-Komponenten verwendeten Treiber aufgeführt:

Komponente	Datenbank	Treiber
PowerCenter-Repository-Dienst	PowerCenter-Repository	Nativ
PowerCenter-Integrationsdienst	Quelle Ziel Gespeicherte Prozedur Lookup	Nativ ODBC
Metadata Manager-Dienst	Metadata Manager-Repository	JDBC
PowerCenter Client	PowerCenter-Repository	Nativ
PowerCenter Client	Quelle Ziel Gespeicherte Prozedur Lookup	ODBC
Custom Metadata Configurator (Metadata Manager-Client)	Metadata Manager-Repository	JDBC

Repository Service-Konnektivität

Der PowerCenter Repository Service verwaltet die Metadaten in der PowerCenter Repository-Datenbank. Alle Anwendungen, die eine Verbindung zum Repository herstellen, müssen dies auch zum PowerCenter Repository Service tun. Der PowerCenter Repository Service verwendet native Treiber zum Kommunizieren mit der Repository-Datenbank.

In der folgenden Tabelle ist die Konnektivität beschrieben, die für die Verbindung des Repository Service mit dem Repository sowie Quell- und Target-Datenbanken erforderlich ist.

Repository Service-Konnektivität	Anforderung für die Konnektivität
PowerCenter Client	TCP/IP
PowerCenter Integration Service	TCP/IP
PowerCenter Repository-Datenbank	Native Datenbanktreiber

Der PowerCenter Integration Service stellt eine Verbindung zum Repository Service her, um bei der Ausführung von Arbeitsabläufen Metadaten abzurufen

Verbinden über den PowerCenter Client

Um über den PowerCenter Client eine Verbindung zum PowerCenter Repository Service herzustellen, fügen Sie im PowerCenter Client-Tool eine Domäne und ein Repository hinzu. Beim Herstellen einer Verbindung über das PowerCenter Client-Tool sendet dieses eine Verbindungsanfrage an den Service Manager im Gateway-Knoten. Der Service Manager gibt den Hostnamen und die Portnummer des Knotens zurück, auf dem der PowerCenter Repository Service ausgeführt wird. Der PowerCenter Client stellt die Verbindung zum PowerCenter-Repository-Dienst über TCP/IP her.

Verbinden zu Datenbanken

Zum Einrichten einer Verbindung vom PowerCenter Repository Service zur Repository-Datenbank konfigurieren Sie die Datenbankeigenschaften in Informatica Administrator. Sie müssen die nativen Datenbanktreiber für die Repository-Datenbank auf dem Rechner installieren und konfigurieren, auf dem der PowerCenter Repository Service ausgeführt wird.

Integration Service-Konnektivität

Der PowerCenter Integration Service stellt eine Verbindung zum Repository her, um Repository-Objekte zu lesen. Der PowerCenter Integration Service stellt über den PowerCenter Repository Service eine Verbindung zum Repository her. Verwenden Sie Informatica Administrator, um ein verbundenes Repository für den Integration Service zu konfigurieren.

In der folgenden Tabelle ist die Konnektivität beschrieben, die für die Verbindung des PowerCenter Integration Service mit den Plattformkomponenten sowie Quell- und Zieldatenbanken erforderlich ist:

PowerCenter Integration Service-Verbindung	Anforderung für die Konnektivität
PowerCenter-Client	TCP/IP
Andere PowerCenter Integration Service-Prozesse	TCP/IP
Repository Service	TCP/IP
Quell- und Zieldatenbanken	Native Datenbanktreiber oder ODBC Hinweis: Der PowerCenter Integration Service unter Windows und UNIX kann mithilfe von ODBC-Treibern eine Verbindung zu Datenbanken herstellen. Mit nativen Treibern kann die Leistung gesteigert werden.

Der PowerCenter Integration Service enthält ODBC-Bibliotheken, die zum Herstellen einer Verbindung zu anderen ODBC-Quellen verwendet werden kann. Die Informatica-Installation enthält ODBC-Treiber.

Bei Einfachdatei-, XML- oder COBOL-Quellen können Sie über Netzwerkverbindungen wie NFS auf Daten zugreifen oder Daten mittels FTP-Software auf den PowerCenter Integration Service-Knoten übertragen. Informationen zu Konnektivitätssoftware oder andere ODBC-Quellen finden Sie in der Dokumentation zu Ihrer Datenbank.

Verbinden über den PowerCenter Client

Der Workflow Manager kommuniziert über eine TCP/IP-Verbindung mit einem PowerCenter Integration Service-Vorgang. Der Workflow Manager kommuniziert jedes Mal, wenn Sie einen Arbeitsablauf starten oder Arbeitsablaufsdetails anzeigen, mit dem PowerCenter Integration Service.

Verbinden zum PowerCenter Repository Service

Bei Erstellung eines PowerCenter Integration Service legen Sie den PowerCenter Repository Service fest, der mit dem PowerCenter Integration Service verbunden werden soll. Wenn der PowerCenter Integration Service einen Arbeitsablauf ausführt, stellt es mittels TCP/IP eine Verbindung zum verbundenen PowerCenter Repository Service her und ruft Metadaten ab

Verbinden zu Datenbanken

Mithilfe des Workflow Manager können Sie Verbindungen zu Datenbanken erstellen. Sie können diese Verbindungen mit nativen Datenbanktreibern oder ODBC erstellen. Geben Sie bei Verwendung von nativen Treibern den Datenbankbenutzernamen, das Passwort und den nativen Verbindungs-String für jede Verbindung an. Der PowerCenter Integration Service verwendet diese Informationen zum Herstellen einer Verbindung zur Datenbank, wenn er die Sitzung ausführt

Hinweis: PowerCenter unterstützt ODBC-Treiber wie z. B. ISG Navigator, für die keine Benutzernamen und Passwörter erforderlich sind, um eine Verbindung herzustellen. Damit keine leeren Zeichenketten oder Nullen verwendet werden, verwenden Sie beim Konfigurieren einer Datenbankverbindung die reservierten Wörter PmNullUser für den Benutzernamen und PmNullPasswd für das Passwort. Der PowerCenter Integration Service behandelt PmNullUser und PmNullPasswd jeweils als keinen Benutzer und kein Passwort.

PowerCenter Client-Konnektivität

Der PowerCenter Client verwendet ODBC-Treiber und native Datenbank-Konnektivitätssoftware zur Kommunikation mit Datenbanken. Er kommuniziert über TCP/IP mit dem Integration Service und dem Repository.

In der folgenden Tabelle sind die Konnektivitätstypen beschrieben, die für die Verbindung des PowerCenter Client mit dem Integration Service, dem Repository sowie Quell- und Target-Datenbanken erforderlich sind.

PowerCenter Client-Konnektivität	Anforderung für die Konnektivität
Integration Service	TCP/IP
Repository Service	TCP/IP
Datenbank	ODBC-Verbindung für jede Datenbank

Verbinden zum Repository

Sie können mithilfe der PowerCenter Client-Tools eine Verbindung zum Repository herstellen. Alle PowerCenter Client-Tools verwenden TCP/IP zur Herstellung der Verbindung zum Repository über den Repository-Dienst, und dies jedes Mal, wenn Sie auf das Repository zugreifen, um Aufgaben wie das Herstellen einer Verbindung zum Repository, Erstellen von Repository-Objekten und Ausführen von Objektanfragen durchzuführen.

Verbinden zu Datenbanken

Zur Herstellung einer Verbindung zu Datenbanken über den Designer erstellen Sie mithilfe des Windows ODBC Data Source Administrator eine Datenquelle zu jeder Datenbank, auf die Sie zugreifen möchten. Wählen Sie die Namen der Datenquellen im Designer bei der Durchführung der folgenden Aufgaben:

- **Importieren einer Tabelle oder einer Definition einer gespeicherten Prozedur aus einer Datenbank**
Importieren einer Tabelle aus einer Datenbank mithilfe des Source Analyzer oder des Target Designer
Importieren einer gespeicherten Prozedur, einer Tabelle für eine Lookup-Umwandlung mithilfe des Transformation Developer, Mapplet Designer oder Mapping Designer

Zum Herstellen einer Verbindung zur Datenbank müssen Sie außerdem Ihren Datenbankbenutzernamen, Ihr Passwort und den Namen des Eigentümers der Tabelle bzw. der gespeicherten Prozedur angeben.
- **Vorschau von Daten** Sie können den Namen der Datenquelle bei der Vorschau von Daten im Source Analyzer oder Target Designer auswählen. Sie müssen außerdem Ihren Datenbankbenutzernamen, Ihr Passwort und Ihren Tabelleneigentümernamen angeben.

Verbindung zum Integration Service

Workflow Manager und Workflow Monitor kommunizieren jedes Mal, wenn Sie mit Sitzungen und Arbeitsabläufen verbundene Aufgaben wie z. B. das Ausführen eines Arbeitsablaufs durchführen, über TCP/IP direkt mit dem Integration Service. Wenn Sie sich über Workflow-Manager oder Workflow-Monitor bei einem Repository anmelden, werden die Integration Services aufgelistet, die für dieses Repository in Informatica Administrator konfiguriert wurden.

Metadata Manager-Dienst-Verbindung

Der Metadata Manager-Dienst benötigt zur Herstellung einer Verbindung zu einem Metadata Manager-Repository einen JDBC-Treiber. Der Custom Metadata Configurator verwendet einen JDBC-Treiber zur Herstellung einer Verbindung zum Metadata Manager-Repository.

JDBC-Treiber werden zusammen mit den Informatica-Diensten und -Clients installiert. Sie können die installierten JDBC-Treiber für die Verbindung zum Metadata Manager Repository verwenden.

Die Informatica-Installationsprogramme installieren weder ODBC-Treiber noch die JDBC-ODBC-Brücke für den Metadata Manager-Dienst.

Native Konnektivität

Zur Herstellung einer nativen Konnektivität zwischen einem Anwendungsdienst und einer Datenbank müssen Sie die Datenbank-Client-Software auf dem Rechner installieren, auf dem der Dienst ausgeführt wird.

In der nachstehenden Tabelle ist die Syntax für den nativen Verbindungs-String eines jeden unterstützten Datenbanksystems beschrieben:

Datenbank	Syntax der Verbindungszeichenfolge	Beispiel
IBM DB2	<i>dbname</i>	mydatabase
Microsoft SQL Server	<i>servername@dbname</i>	sqlserver@mydatabase
Oracle	<i>dbname.world</i> (identisch mit dem Eintrag TNSNAMES)	oracle.world
Sybase ASE	<i>servername@dbname</i>	sambrown@mydatabase Hinweis: Der Sybase ASE-Servername entspricht dem Namen des Adaptive Server aus der Schnittstellendatei.
Teradata	<i>ODBC_data_source_name</i> oder <i>ODBC_data_source_name@db_name</i> oder <i>ODBC_data_source_name@db_user_name</i>	TeradataODBC TeradataODBC@mydatabase TeradataODBC@sambrown Hinweis: Verwenden Sie Teradata-ODBC-Treiber zum Herstellen einer Verbindung zu Quell- und Target-Datenbanken.

ODBC-Konnektivität

Open Database Connectivity (ODBC) bietet eine gemeinsame Möglichkeit, mit unterschiedlichen Datenbanksystem zu kommunizieren.

Um ODBC-Konnektivität zu verwenden, müssen Sie die folgenden Komponenten auf dem Computer installieren, der den Informatica-Dienst oder das Client-Tool hostet.

- **Datenbank-Clientsoftware.** Installieren Sie die Clientsoftware für das Datenbanksystem. Damit werden die Client-Bibliotheken installiert, die zur Herstellung einer Verbindung mit der Datenbank erforderlich sind.

Hinweis: Einige ODBC-Treiber enthalten Wire Protocols und benötigen keine Datenbank-Clientsoftware.

- **ODBC-Treiber.** Die geschlossenen DataDirect 32-Bit- oder 64-Bit-ODBC-Treiber werden bei der Installation der Informatica-Dienste installiert. Die geschlossenen DataDirect 32-Bit-ODBC-Treiber werden bei der Installation der Informatica-Clients installiert. Der Datenbankserver kann auch einen ODBC-Treiber enthalten.

Nach dem Installieren der erforderlichen Komponenten, müssen Sie eine ODBC-Datenquelle für jede Datenbank konfigurieren, zu der Sie eine Verbindung herstellen möchten. Eine Datenquelle enthält Informationen, die Sie benötigen, um die Datenbank zu finden und auf sie zuzugreifen, wie zum Beispiel Datenbankname, Benutzername und Datenbank-Passwort. Unter Windows verwenden Sie den ODBC-Datenquellen-Administrator, um einen Datenquellenamen zu erstellen. Unter UNIX fügen Sie Datenquelleneinträge zu der im Systemverzeichnis \$ODBCHOME gefundenen odbc.ini-Datei hinzu.

Wenn Sie eine ODBC-Datenquelle erstellen, müssen Sie auch den Treiber festlegen, dem der ODBC-Treiber-Manager Datenbankaufrufe sendet.

Die folgende Tabelle zeigt die empfohlenen ODBC-Treiber, die mit der jeweiligen Datenbank zu verwenden sind.

Datenbank	ODBC-Treiber	Benötigt Datenbank-Clientsoftware
Informix	DataDirect Informix Wire Protocol	Nein
Microsoft Access	Microsoft Access-Treiber	Nein
Microsoft Excel	Microsoft Excel-Treiber	Nein
Microsoft SQL Server	DataDirect SQL Server Wire Protocol	Nein
Netezza	Netezza SQL	Ja
Teradata	Teradata-ODBC-Treiber	Ja
SAP HANA	SAP HANA ODBC-Treiber	Ja

JDBC-Konnektivität

JDBC (Java Database Connectivity) ist eine Java-API, die für die Konnektivität von relationalen Datenbanken sorgt. Java-basierte Anwendungen können mithilfe von JDBC-Treibern eine Verbindung zu Datenbanken herstellen.

Die folgenden Dienste und Clients stellen mithilfe von JDBC eine Verbindung zu Datenbanken her:

JDBC-Treiber werden zusammen mit den Informatica-Diensten und -Clients installiert.

Konfigurieren des Webbrowsers

- [Konfigurieren des Webbrowsers, 390](#)

Konfigurieren des Webbrowsers

Sie können das Administrator Tool in den Webbrowsern Microsoft Internet Explorer, Microsoft Edge, Google Chrome oder Safari ausführen.

Um das Administrator tool verwenden zu können, müssen Sie im Browser die folgenden Optionen konfigurieren:

Scripting und ActiveX

Aktivieren Sie die folgenden Steuerelemente in Microsoft Internet Explorer:

- Active Scripting
- Programmatischen Zugriff auf die Zwischenablage zulassen
- ActiveX-Steuerelemente und Plugins ausführen
- ActiveX-Steuerelemente ausführen, die für Scripting sicher sind

Um die Steuerelemente zu konfigurieren, klicken Sie auf **Extras > Internetoptionen > Sicherheit > Stufe anpassen**.

Vertrauenswürdige Sites

Wenn die Informatica-Domäne in einem Netzwerk mit Kerberos-Authentifizierung ausgeführt wird, müssen Sie den Browser so konfigurieren, dass der Zugriff auf die Informatica-Webanwendungen möglich ist. Fügen Sie in Microsoft Internet Explorer, Microsoft Edge und Google Chrome die URL der Informatica-Webanwendung zur Liste der vertrauenswürdigen Sites hinzu. Fügen Sie in Safari das Zertifikat der Informatica-Webanwendung zum Schlüsselbund hinzu. Wenn Sie Chrome Version 86.0.42x oder höher unter Windows verwenden, müssen Sie auch die Richtlinien `AuthServerWhitelist` und `AuthNegotiateDelegateWhitelist` festlegen.

INDEX

A

Abhängigkeiten

- Anwendungsdienste [70](#)
- Dienste und Knoten anzeigen [70](#)
- Gitter [70](#)
- Knoten [70](#)

Adabas-Verbindungen

- Eigenschaften [130](#)

Administrator Tool

- Berichte [308](#)
- Codepage [338](#)
- Fehlerprotokoll, anzeigen [300](#)
- Logs, anzeigen [295](#)

Aktivitätsdaten

- Web Services Report [316](#)

Alarme

- abonnieren [78](#)
- anzeigen [79](#)
- Benachrichtigungs-E-Mail [79](#)
- Beschreibung [19](#)
- konfigurieren [77](#)
- nachverfolgen [79](#)
- verwalten [77](#)

Alarme abonnieren

- Benutzereinstellungen [29](#)

Allgemeine Eigenschaften

- Informatica-Domäne [92](#)
- Lizenz [253](#)

Amazon Redshift-Verbindung

- Eigenschaften [132](#)

Amazon S3-Verbindung

- Eigenschaften [136](#)

Analyst Service

- Log-Ereignisse [303](#)

Analyst-Dienst

- Anwendungsdienst [41](#)
- benutzerdefinierte Rollen [371](#)

ändern

- Passwort für Benutzerkonto [29](#)

Anmeldung

- Fehlerbehebung [33](#)

Ansicht Dienste und Knoten.

- Informatica Administrator [40](#)

Anwendungen

- überwachen [269](#)

Anwendungsdienste

- Abhängigkeiten [70](#)
- aktivieren [82](#)
- Analyst-Dienst [41](#)
- Belastbarkeit, konfigurieren [116](#)
- Berichterstellungs- und Dashboard-Dienst [41](#)
- Berichterstellungsdienst [41](#)
- Beschreibung [20](#)
- Content-Managementdienst [41](#)
- Datenintegrationsdienst [41](#)

Anwendungsdienste (Fortsetzung)

- Deaktivieren [82](#)
- Entfernen [84](#)
- Lizenzen, zuweisen [250](#)
- Metadata Manager-Dienst [41](#)
- Metadaten-Zugriffsdienst [41](#)
- Modellrepository-Dienst [41](#)
- PowerCenter-Integrationsdienst [41](#)
- PowerCenter-Repository-Dienst [41](#)
- PowerExchange-Listenerdienst [41](#)
- PowerExchange-Protokollierungsdienst [41](#)
- SAP BW-Dienst [41](#)
- suchen [39](#)
- Übersicht [41](#)
- Webdienst-Hub [41](#)

Anwendungsdienste.

- Lizenzen, Aufheben der Zuordnung [251](#)

Anwendungsdienstprozess

- aktivieren [82](#)
- angehaltener Status [82](#)
- deaktivieren [82](#)
- Fehlerstatus [82](#)
- Portzuordnung [20](#)
- Standby-Status [82](#)
- Status [82](#)

Anwendungsquellen

- Codepage [340](#)

Anwendungstargets

- Codepage [341](#)

anzeigen

- Abhängigkeiten für Dienste und Knoten [70](#)

Arbeitsabläufe

- Abbrechen [283](#)
- Protokolle [285](#)
- Status [281](#)
- überwachen [278](#)
- Wiederherstellen [285](#)

Arbeitsablaufwiederherstellung

- Ausführen [285](#)
- Übersicht [284](#)

ASCII-Modus

- Übersicht [333](#)

Auditberichte

- Übersicht [63](#)

Aufgaben

- Status [282](#)

Authentifizierung

- Protokollereignisse [302](#)

Automatische Auswahl

- Netzwerk, hohe Verfügbarkeit [120](#)

Autorisierung

- Dienstmanager [19](#)
- Protokollereignisse [302](#)

B

- Backup-Verzeichnis
 - Knoteneigenschaft [103](#)
- bearbeiten
 - Verbindungen [124](#)
 - Zeitpläne [239](#)
- Befehl BackupDomain
 - Beschreibung [86](#)
- Befehlszeilenprogramme
 - Belastbarkeit, konfigurieren [118](#)
- Begrenzte Bezeichner
 - Datenbankverbindungen [233](#)
- Belastbarkeit
 - Anwendungsdienst [110](#)
 - Anwendungsdienstkonfiguration [116](#)
 - Befehlszeilenprogramm-Konfiguration [118](#)
 - im exklusiven Modus [118](#)
 - PowerCenter Client [109](#)
 - PowerCenter-Integrationsdienst [110](#)
 - PowerCenter-Repository-Dienst [110](#)
 - TCP KeepAlive-Timeout [120](#)
- Benutzer
 - Lizenzaktivität, überwachen [308](#)
 - Übersicht [61](#)
- Benutzeraktivität
 - Protokollierungsereignis-Kategorien [306](#)
- Benutzerdefinierte Eigenschaften
 - Domäne [96](#)
- Benutzerdefinierte Eigenschaften anzeigen (Eigenschaft)
 - Benutzereinstellungen [29](#)
- benutzerdefinierte Filter
 - Abgelaufene Zeit [288](#)
 - Datum und Uhrzeit [288](#)
 - Mehrfachauswahl [288](#)
- benutzerdefinierte Rollen
 - Analyst-Dienst [371](#)
 - Operator [374](#)
- Benutzerdefinierte Rollen
 - Metadata Manager-Dienst [372](#)
 - PowerCenter-Repository-Dienst [375](#)
- Benutzerdetail
 - Lizenzverwaltungsbericht [312](#)
- Benutzereinstellungen
 - Beschreibung [29](#)
- Benutzerkonten
 - Ändern des Passworts [29](#)
 - verwalten [28](#)
- Benutzerschemata
 - Beschreibung [332](#)
- Benutzerverwaltung
 - Protokollereignisse [302](#)
- Benutzerzusammenfassung
 - Lizenzverwaltungsbericht [311](#)
- Berechnungsrolle
 - Knoten [99](#)
- Bereinigen
 - Protokoll-Manager [294](#)
- Bereitgestellte Zuordnungsjobs
 - Überwachen [269](#)
- Berichte
 - Administrator Tool [308](#)
 - Domäne [308](#)
 - Lizenz [308](#)
 - überwachen [56](#)
 - Web Services [308](#)
- Berichterstellungs- und Dashboard-Dienst
 - Anwendungsdienst [41](#)

- Berichterstellungsdienst
 - Anwendungsdienst [41](#)
- Betriebsmodus
 - Auswirkungen auf die Belastbarkeit [118](#)
- Betriebssystemprofile
 - Übersicht [62](#)
- Bezeichner
 - begrenzt [233](#)
 - regulär [233](#)
- Blaze-Engine
 - Verbindungseigenschaften [154](#)
- Blockchain
 - Verbindungseigenschaften [139](#)

C

- Cassandra-Verbindungen
 - Eigenschaften [140](#)
- catalina.out
 - Fehlersuche [292](#)
- COBOL
 - Konnektivität [385](#)
- Codepage Relaxation
 - Konfigurieren des Integration Service [346](#)
- Codepage-Entspannung
 - Dateninkonsistenzen [345](#)
 - Fehlersuche [346](#)
 - Übersicht [345](#)
- Codepage-Lockerung
 - kompatible Codepages, auswählen [346](#)
- Codepage-Validierung
 - Entspannte Validierung [345](#)
 - Übersicht [344](#)
- Codepages
 - Administrator Tool [338](#)
 - Anwendungsquellen [340](#)
 - Anwendungstargets [341](#)
 - auswählen [336](#)
 - Benutzerdefinierte Umwandlung [342](#)
 - Beschreibungen [360](#)
 - Beziehungen [344](#)
 - Datenbank für gespeicherte Prozeduren [342](#)
 - Datenintegrationsdienst-Prozess [358](#)
 - Domänenkonfigurationsdatenbank [338](#)
 - Einfachdatei-Targets [341](#)
 - Entspannte Validierung für Quellen und Targets [345](#)
 - Flatfile-Quellen [340](#)
 - ID [360](#)
 - Kompatibilität - Übersicht [336](#)
 - Kompatibilitätsdiagramm [342](#)
 - Lookup-Datenbank [342](#)
 - Metadata Manager Service [340](#)
 - Namen [360](#)
 - pmcmd [339](#)
 - PowerCenter Integration Service-Prozess [339](#)
 - PowerCenter-Client [338](#)
 - PowerCenter-Integrationsdienst-Prozess [358](#)
 - Quellen [340](#), [360](#)
 - Relationale Quellen [340](#)
 - Relationale Targets [341](#)
 - Sortierreihenfolge - Übersicht [339](#)
 - Speicher [339](#), [358](#)
 - Targets [341](#)
 - Übersicht [334](#)
 - Umwandlung [347](#)
 - Umwandlung externer Verfahren [342](#)
 - UNIX [335](#)

- Codepages (*Fortsetzung*)
 - Unterstützte Codepages [358, 360](#)
 - Validierung [344](#)
 - Windows [336](#)
 - Ziele [360](#)
- Configuration Support Manager
 - zur Analyse der Knotendiagnostik verwenden [327](#)
 - zur Knotendiagnose [323](#)
- Confluent-Kafka-Verbindung
 - Allgemeine Eigenschaften [143](#)
 - Eigenschaften des Confluent-Kafka-Brokers [143](#)
 - Erstellen mit infacmd [144](#)
- Content-Managementdienst
 - Anwendungsdienst [41](#)
 - Konnektivität [381](#)
- Cosmos DB-Verbindung
 - erstellen [198](#)
- CPU-Detail
 - Lizenzverwaltungsbericht [310](#)
- CPU-Profil
 - Knoteneigenschaft [103](#)
- CPU-Zusammenfassung
 - Lizenzverwaltungsbericht [310](#)
- CPUs
 - Überschreiten des Grenzwerts [310](#)

D

- Data Analyzer
 - ODBC (Open Database Connectivity) [380](#)
- Data Integration Service
 - Protokollereignisse [303](#)
- Data Integration Services
 - Überwachung [262](#)
- Databricks-Verbindungseigenschaften [145](#)
- DataDirect ODBC-Treiber
 - plattformspezifische Treiber erforderlich [388](#)
- Dateien für die garantierte Meldungsauslieferung
 - Protokollmanager [290](#)
- Datenbank
 - Domänenkonfiguration [85](#)
- Datenbankeigenschaften
 - Informatica-Domäne [93](#)
- Datenbanktreiber
 - Integrationsdienst [380](#)
 - Repository-Dienst [380](#)
- Datenbankverbindungen
 - Aktualisierung für Domänenkonfiguration [89](#)
 - Bezeichnereigenschaften [233](#)
- Datenintegrationsdienst
 - Anwendungsdienst [41](#)
 - Konnektivität [381](#)
 - Wiederherstellung [114](#)
- Datenintegrationsdienst-Prozess
 - Status anzeigen [101](#)
 - Unterstützte Codepages [358](#)
- Datenobjekt-Zwischenspeicherung
 - mit Pass-Through-Sicherheit [125](#)
- Datenverschiebungsmodus
 - ändern [333](#)
 - ASCII [333](#)
 - Auswirkungen auf Sitzungsdateien und Cache-Speicher [333](#)
 - Beschreibung [332](#)
 - Übersicht [332](#)
 - Unicode [333](#)
- Deaktivierungsmodus
 - PowerCenter Integration Services und Dienstprozesse [82](#)

- Detaillierte Statistiken
 - Überwachen [263](#)
- Dienste
 - suchen [39](#)
- Dienste und Knoten
 - Abhängigkeiten anzeigen [70](#)
- Dienstmanager
 - Autorisierung [19](#)
 - Beschreibung [19](#)
- Dienstname
 - Protokollereignisse [301](#)
- Dienstrolle
 - Knoten [99](#)
- Domäne
 - Benutzeraktivität, überwachen [308](#)
 - Benutzersicherheit [81](#)
 - Berichte [308](#)
 - Protokollereigniskategorien [302](#)
- Domänen
 - mehrere [76](#)
- Domänen-Bericht
 - Web Services-Bericht [315](#)
- Domänen-Konfigurationsdatenbank
 - Aktualisieren [89](#)
 - Migrieren [87](#)
 - Sichere Datenbank [94](#)
 - Verbindung für Gateway-Knoten [89](#)
 - Wiederherstellen [86](#)
- Domänenberichte
 - ausführen [308](#)
 - Lizenzverwaltungsbericht [308](#)
- Domäneneigenschaften
 - Informatica-Domäne [91](#)
- Domänenkonfiguration
 - Beschreibung [85](#)
 - Migrieren [87](#)
 - Protokollereignisse [302](#)
- Domänenkonfigurationsdatenbank
 - Beschreibung [85](#)
 - Codepage [338](#)
 - sichern [86](#)
- Durchschn. Anz. der Ausführungsinstanzen (Eigenschaft)
 - Web Services Report [316](#)
- Durchschn. Anz. der Dienstpartitionen (Eigenschaft)
 - Web Services Report [316](#)
- Durchschn. DTM-Zeit (Eigenschaft)
 - Web Services Report [316](#)
- Durchschnittliche Dienstzeit (Eigenschaft)
 - Web Services Report [316](#)

E

- Einfachdateien
 - Konnektivität [385](#)
 - Logs exportieren [300](#)
 - Quell-Codepage [340](#)
 - Target-Codepage [341](#)
- Eingabe-Gebietsschemata
 - IME (Windows Input Method Editor) [332](#)
 - konfigurieren [332](#)
- Einstellungen
 - Überwachen [259](#)
- erstellen
 - Cosmos DB-Verbindung [198](#)

F

- Failover
 - Anwendungsdienst [113](#)
 - Domäne [113](#)
- Fallstudie
 - ISO 8859-1 Datenverarbeitung [348](#)
 - Verarbeiten von Unicode UTF-16LE Daten [351](#)
- Fehler protokollieren
 - Administrator Tool [300](#)
- Fehlerbehebung
 - anmelden [33](#)
 - Kerberos-Authentifizierung [33](#)
- Fehlersuche
 - catalina.out [292](#)
 - Codepage-Entspannung [346](#)
 - localhost_.txt [292](#)
 - node.log [292](#)
 - Umgebungsvariablen [84](#)
- FTP
 - Erreichen hoher Verfügbarkeit [120](#)

G

- Gateway
 - verwalten [84](#)
- Gateway-Knoten
 - Beschreibung [98](#)
 - konfigurieren [84](#)
 - Protokollieren [291](#)
 - Protokollverzeichnis [84](#)
- GB18030
 - Beschreibung [330](#)
- Gebietsschemata
 - Übersicht [331](#)
- gespeicherte Prozeduren
 - Codepages [342](#)
- Gitter
 - Abhängigkeiten [70](#)
 - Registerkarten des Informatica Administrators [47](#)
 - suchen [39](#)
- Globalisierung
 - Übersicht [329](#)
- Google Analytics-Verbindungen
 - Eigenschaften [148](#)
- Google BigQuery-Verbindung
 - Eigenschaften [149](#)
- Google BigQuery-Verbindungen
 - Verbindungsmodi [151](#)
- Google Cloud Spanner-Verbindung
 - Eigenschaften [152](#)
- Google Cloud Storage-Verbindungen
 - Eigenschaften [152](#)
- Google PubSub
 - Verbindungseigenschaften [153](#)
- Grafikanzeige-Server
 - Anforderung [308](#)
- Greenplum-Verbindungen
 - Eigenschaften [147](#)
- Gruppen
 - Übersicht [61](#)

H

- Hardwarekonfiguration
 - Lizenzverwaltungsbericht [312](#)

- HBase-Verbindungen
 - Eigenschaften [163](#)
 - MapR-DB-Eigenschaften [165](#)
- HDFS-Verbindungen
 - Eigenschaften [163](#)
- Herunterfahren
 - Informatica-Domäne [91](#)
- historische Statistik
 - Überwachen [263](#)
- Hive-Pushdown
 - Verbindungseigenschaften [154](#)
- Hive-Verbindungen
 - Eigenschaften [166](#)
- Hohe Verfügbarkeit
 - Beschreibung [26](#), [108](#)
 - Failover [112](#)
 - Neustart [112](#)
 - TCP KeepAlive-Timeout [120](#)
 - Wiederherstellung [114](#)
- HTTP-Verbindungen
 - Eigenschaften [170](#)

I

- IBM DB2
 - Verbindungszeichenfolge, Syntax [388](#)
- IBM DB2 for i5/OS-Verbindungen
 - Eigenschaften [175](#)
- IBM DB2 for z/OS-Verbindungen
 - Eigenschaften [179](#)
- IBM DB2-Verbindungen
 - Eigenschaften [172](#)
- IME (Windows Input Method Editor)
 - Eingabe-Gebietsschemata [332](#)
- IMS-Verbindungen
 - Eigenschaften [182](#)
- Informatica Administrator
 - anmelden [32](#)
 - Ansicht Dienste und Knoten. [40](#)
 - Dienste, Aktivieren und Deaktivieren [82](#)
 - Dienstprozess, Aktivieren und Deaktivieren [82](#)
 - Navigator [60](#)
 - Registerkarte "Protokolle" [59](#)
 - Registerkarte „Überwachen“ [49](#), [51](#)
 - Registerkarte „Verwalten“ [33](#), [38](#)
 - Registerkarte Berichte [59](#)
 - Registerkarten, anzeigen [31](#)
 - Sicherheitsseite [60](#)
 - Suche wird ausgeführt [60](#)
 - Übersicht [31](#), [76](#)
- Informatica Analyst
 - Konnektivität [381](#)
- Informatica Data Explorer
 - Konnektivität [381](#)
- Informatica Data Quality
 - Konnektivität [381](#)
- Informatica Data Services
 - Konnektivität [381](#)
- Informatica Developer
 - Konnektivität [381](#)
- Informatica-Domäne
 - Alarmer [77](#)
 - Allgemeine Eigenschaften [92](#)
 - Benutzersicherheit [81](#)
 - Berechtigungen [81](#)
 - Beschreibung [17](#)
 - Datenbankeigenschaften [93](#)

- Informatica-Domäne (*Fortsetzung*)
 - Domänen-Konfigurationsdatenbank [94](#)
 - Domäneneigenschaften [91](#)
 - Herunterfahren [91](#)
 - mehrere Domänen [76](#)
 - Neu starten [91](#)
 - Protokoll- und Gateway-Konfiguration [93](#)
 - Status der Operationen [114](#)
- Informatica-Netzwerk
 - anmelden [324](#)
- Information and Content Exchange (ICE)
 - Protokolldateien [300](#)
- Inkrementelle Schlüssel
 - Lizenzen [248](#)
- Innerhalb des Neustartzeitraums (Eigenschaft)
 - Informatica-Domäne [83](#)
- Integration Service
 - Konnektivität [385](#)
- Integrationsdienst
 - ODBC (Open Database Connectivity) [380](#)

J

- JD Edwards EnterpriseOne-Verbindung
 - Eigenschaften [190](#)
- JDBC (Java Database Connectivity)
 - Übersicht [389](#)
- JDBC V2-Verbindung
 - Eigenschaften [187](#)
- JDBC-Treiber
 - Data Analyzer [380](#)
 - installierte Treiber [388](#)
 - Metadata Manager [380](#)
 - Metadata Manager-Verbindung zu Datenbanken [388](#)
 - PowerCenter-Domäne [380](#)
 - Referenztabellen-Manager [380](#)
- JDBC-Verbindungen
 - Eigenschaften [185](#)
- Jobplanung
 - Übersicht [236](#)
- Jobs
 - Überwachen [263](#)
- Jobstatus
 - Domänen-Failover [286](#)

K

- Kafka-Verbindung
 - Allgemeine Eigenschaften [192](#)
 - Eigenschaften des Kafka-Brokers [192](#)
 - Erstellen mit infacmd [194](#)
- Kategorie
 - Domänenprotokollereignisse [302](#)
- Kerberos-Authentifizierung
 - Fehlerbehebung [33](#)
- Knoten
 - Abhängigkeiten [70](#)
 - Beschreibung [17](#), [98](#)
 - definieren [101](#)
 - Entfernen [107](#)
 - Gateway [84](#), [98](#)
 - Herunterfahren [106](#)
 - Host-Namen und Portnummer, Entfernen [103](#)
 - konfigurieren [103](#)
 - Neu starten [106](#)
 - Portnummer [103](#)

- Knoten (*Fortsetzung*)
 - Protokollmanager [301](#)
 - Register im Informatica Administrator [47](#)
 - Rollen [99](#)
 - Starten [106](#)
 - suchen [39](#)
 - TCP/IP-Netzwerkprotokoll [380](#)
 - Typen [98](#)
 - Worker [98](#)
 - Zu Informatica Administrator hinzufügen [101](#)
- Knotendiagnostik
 - analysieren [327](#)
 - herunterladen [326](#)
- Knotendiagnostiken [323](#)
- Knoteneigenschaften
 - Backup-Verzeichnis [103](#)
 - CPU-Profil [103](#)
 - konfigurieren [103](#)
 - Maximale Anzahl der Prozesse [103](#)
 - Maximale Länge der CPU-Ausführungswarteschlange [103](#)
 - Maximale Speichergröße in Prozent [103](#)
- Knotenkonfiguration
 - Lizenzverwaltungsbericht [313](#)
 - Protokollereignisse [302](#)
- Knotenkonfigurationsdatei
 - Speicherort [101](#)
- Knotenrollen
 - aktualisieren [100](#)
 - berechnen [99](#)
 - Dienst [99](#)
- kompatibel
 - definiert für die Codepage-Kompatibilität [336](#)
- Kompatibilität
 - zwischen Codepages [336](#)
 - zwischen Quell- und Target-Codepages [346](#)
- Konnektivität
 - COBOL [385](#)
 - Content-Managementdienst [381](#)
 - Datenintegrationsdienst [381](#)
 - Diagramm des [380](#)
 - Informatica Analyst [381](#)
 - Informatica Developer [381](#)
 - Integration Service [385](#)
 - Metadata Manager [388](#)
 - Modellrepository-Dienst [381](#)
 - PowerCenter Client [387](#)
 - PowerCenter Repository Service [385](#)
 - Übersicht [380](#)
 - Verbindungszeichenfolge, Beispiele [388](#)
- Konten
 - Ändern des Passworts [29](#)
 - verwalten [28](#)
- Kontoverwaltung
 - Übersicht [63](#)
- Kudu-Verbindung
 - Eigenschaften [194](#)

L

- LANG_C Umgebungsvariable
 - Gebietsschema unter UNIX einrichten [335](#)
- Laufzeitstatistiken
 - Web Services-Bericht [318](#)
- LC_ALL Umgebungsvariable
 - Gebietsschema unter UNIX einrichten [335](#)
- LDAP-Verbindung
 - Eigenschaften [195](#)

- Listener Service Logs
 - Log-Ereignisse [303](#)
- Lizenz
 - Aktualisieren [251](#)
 - Allgemeine Eigenschaften [253](#)
 - Aufheben der Zuordnung von einem Dienst [251](#)
 - Details, anzeigen [252](#)
 - einem Dienst zuweisen [250](#)
 - Entfernen [252](#)
 - erstellen [249](#)
 - Lizenzdatei [249](#)
 - Log-Ereignisse [304](#)
 - Protokollereignisse [302](#)
 - Register im Informatica Administrator [47](#)
 - Schlüssel [248](#)
 - Validierung [247](#)
 - verwalten [247](#)
- Lizenzierte Optionen
 - Lizenzverwaltungsbericht [313](#)
- Lizenzierung
 - Lizenzverwaltungsbericht [309](#)
 - Log-Ereignisse [304](#)
 - verwalten [247](#)
- Lizenzierungsprotokolle
 - Protokollereignisse [247](#)
- Lizenznutzung
 - Protokollereignisse [302](#)
- Lizenzschlüssel
 - Inkrementell [248](#), [251](#)
 - Ursprünglich [248](#)
- Lizenzverwaltungsbericht
 - ausführen [308](#)
 - Benutzerdetail [312](#)
 - Benutzerzusammenfassung [311](#)
 - CPU-Detail [310](#)
 - CPU-Zusammenfassung [310](#)
 - Hardwarekonfiguration [312](#)
 - Knotenkonfiguration [313](#)
 - Lizenzierte Optionen [313](#)
 - Lizenzierung [309](#)
 - Multibyte-Zeichen [314](#)
 - Per E-Mail [315](#)
 - Repository-Zusammenfassung [311](#)
 - Unicode-Schriftart [314](#)
 - wird ausgeführt [314](#)
- localhost_.txt
 - Fehlersuche [292](#)
- Log Agent
 - Beschreibung [289](#)
- Log Manager
 - catalina.out [292](#)
 - Fehlersuche [292](#)
 - konfigurieren [295](#)
 - Log-Ereignisse des PowerCenter Integration Service [304](#)
 - Log-Ereignisse des PowerCenter Repository Service [304](#)
 - Log-Ereignisse des SAP NetWeaver BI [305](#)
 - Log-Ereignisse, bereinigen [294](#)
 - Log-Ereignisse, speichern [298](#)
 - Logs, anzeigen [295](#)
 - node.log [292](#)
 - Sicherheits-Audit-Trail [304](#)
- Log-Ereignisdateien
 - Bereinigen [294](#)
- Log-Ereignisse
 - anzeigen [295](#)
 - Exportieren mit Mozilla Firefox [298](#)
 - Lizenzierung [304](#)
 - PowerCenter Repository Service [304](#)

- Log-Ereignisse (*Fortsetzung*)
 - Sicherheits-Audit-Trail [304](#)
 - speichern [298](#)
 - Speichern [298](#)
 - Web Services Hub [306](#)
 - Zeitzone [295](#)
- Logger Service Logs
 - Log-Ereignisse [303](#)
- Logische CPUs
 - Berechnung [310](#)
- Logische Datenobjekte
 - Überwachung [272](#)
- Logs
 - anzeigen [295](#)
 - Speichern [298](#)
- Lookup-Datenbanken
 - Codepages [342](#)
- löschen
 - Verbindungen [124](#)
 - Zeitpläne [240](#)

M

- Mapping-Aufgabe
 - Protokolldateien [307](#)
- Master-Gateway-Knoten
 - Beschreibung [98](#)
- Maximale Anzahl der Prozesse
 - Knoteneigenschaft [103](#)
- Maximale Anzahl Neustartversuche (Eigenschaft)
 - Informatica-Domäne [83](#)
- Maximale Länge der CPU-Ausführungswarteschlange
 - Knoteneigenschaft [103](#)
- Maximale Speichergröße in Prozent
 - Knoteneigenschaft [103](#)
- Meldungscode
 - Protokollmanager [301](#)
- Messaging-Verbindung
 - Confluent-Kafka-Verbindung [142](#)
 - Kafka-Verbindung [191](#)
- Metadata Manager
 - Konnektivität [388](#)
 - ODBC (Open Database Connectivity) [380](#)
- Metadata Manager Service
 - Codepage [340](#)
 - Log-Ereignisse [304](#)
- Metadata Manager-Dienst
 - Anwendungsdienst [41](#)
 - Benutzerdefinierte Rollen [372](#)
- Metadaten
 - Auswählen von Zeichen [347](#)
 - Zum Repository hinzufügen [347](#)
- Metadaten-Zugriffsdienst
 - Anwendungsdienst [41](#)
- Microsoft Azure Data Lake Storage Gen1-Verbindung
 - Eigenschaften [198](#)
- Microsoft Azure Data Lake Storage Gen2-Verbindung
 - Eigenschaften [200](#)
- Microsoft Azure SQL Data Warehouse-Verbindung
 - Eigenschaften [201](#)
- Microsoft SQL Server
 - Verbindungszeichenfolge, Syntax [388](#)
- migrieren
 - Domänenkonfiguration [87](#)
- Modellrepository-Dienst
 - Anwendungsdienst [41](#)
 - Konnektivität [381](#)

Modellrepository-Dienst (*Fortsetzung*)
 Protokollereignisse [304](#)
MS SQL Server-Verbindungen
 Eigenschaften [203](#)
Multibyte-Daten
 Eingeben in den PowerCenter Client [332](#)

N

Navigator
 Registerkarte „Verwalten“ [33](#), [38](#)
 Sicherheitsseite [60](#)
 suchen [39](#)
Netezza-Verbindungen
 Eigenschaften [207](#)
Netzwerk
 Hohe Verfügbarkeit [120](#)
Neustart
 Anwendungsdienst [113](#)
Neustarten
 Konfigurieren für PowerCenter -Integrationsdienst-Prozesse [83](#)
NLS_LANG
 Einstellung Gebietsschema [349](#), [351](#)
node.log
 Fehlersuche [292](#)
nodemeta.xml
 für Gateway-Knoten [84](#)
 Speicherort [101](#)

O

OData-Verbindungen
 Eigenschaften [208](#)
ODBC (Open Database Connectivity)
 Anforderung für PowerCenter Client [387](#)
 DataDirect-Treiberprobleme [388](#)
 Integrationsdienst [380](#)
 Konnektivität herstellen [388](#)
 Metadata Manager [380](#)
 PowerCenter Client [380](#)
ODBC-Verbindungen
 Eigenschaften [209](#)
Operator)
 benutzerdefinierte Rollen [374](#)
Oracle
 Einstellung Gebietsschema mit NLS_LANG [349](#), [351](#)
 Verbindungszeichenfolge, Syntax [388](#)
Oracle-Verbindungen
 Eigenschaften [211](#)
Ordner
 Administrator Tool [79](#)
 Entfernen [80](#)
 erstellen [79](#), [80](#)
 Objekte, verschieben [80](#)
 Übersicht [41](#)
 verwalten [79](#)
Originalschlüssel
 Lizenzen [248](#)

P

Pass-Through-Sicherheit
 Cache aktivieren [125](#)
 Operations-Mappings bei Web-Diensten [125](#)
 Verbindung mit einem SQL-Datendienst [125](#)

Pass-Through-Sicherheit (*Fortsetzung*)
 Verbindungen hinzufügen [126](#)
Passwort
 Ändern für ein Benutzerkonto [29](#)
pmcmd
 Codepage-Probleme [339](#)
 Kommunizieren mit dem PowerCenter Integration Service [339](#)
PmNullPasswd
 reserviertes Wort [386](#)
PmNullUser
 reserviertes Wort [386](#)
Port
 Anwendungsdienst [20](#)
 Bereich für Dienstprozesse [103](#)
 Knoten [103](#)
 Knoten-Maximalwert [103](#)
 Knoten-Minimalwert [103](#)
PowerCenter
 Konnektivität [380](#)
PowerCenter Client
 Belastbarkeit [109](#)
 Konnektivität [387](#)
 Multibyte-Zeichen, eingeben [332](#)
 ODBC (Open Database Connectivity) [380](#)
 TCP/IP-Netzwerkprotokoll [380](#)
PowerCenter Integration Service
 Aktivieren und Deaktivieren [82](#)
 Log-Ereignisse [304](#)
PowerCenter Integration Service-Prozess
 Aktivieren und Deaktivieren [82](#)
 Codepage [339](#)
PowerCenter Repository Service
 Anforderungen für die Konnektivität [385](#)
 Log-Ereignisse [304](#)
PowerCenter Sicherheit
 verwalten [60](#)
PowerCenter-Client
 Codepage [338](#)
PowerCenter-Domänen
 Konnektivität [383](#)
 TCP/IP-Netzwerkprotokoll [380](#)
PowerCenter-Integrationsdienst
 Anwendungsdienst [41](#)
 Belastbarkeit [110](#)
 Failover-Konfiguration [117](#)
 Status der Operationen [114](#)
 Tabellen zur Hochverfügbarkeits-Persistenz [117](#)
 Wiederherstellung [114](#)
 Wiederherstellungskonfiguration [117](#)
PowerCenter-Integrationsdienst-Prozess
 Neustart, konfigurieren [83](#)
 Unterstützte Codepages [358](#)
PowerCenter-Integrationsdienstprozess
 Status anzeigen [101](#)
PowerCenter-Repository-Dienst
 Anwendungsdienst [41](#)
 Belastbarkeit [110](#)
 Benutzerdefinierte Rollen [375](#)
 Status der Operationen [114](#)
 Wiederherstellung [114](#)
PowerExchange-Listenerdienst
 Anwendungsdienst [41](#)
PowerExchange-Protokollierungsdienst
 Anwendungsdienst [41](#)
ProcessID
 Meldungscode [301](#)
 Protokollmanager [301](#)

- Protokoll- und Gateway-Konfiguration
 - Informatica-Domäne [93](#)
- Protokoll-Manager
 - Bereinigen [294](#)
 - Domänenprotokollereignisse [302](#)
 - Protokollereignisse [302](#)
- Protokollagent
 - Protokollereignisse [302](#)
- Protokolldateien
 - Mapping-Aufgaben [307](#)
- Protokolle
 - Arbeitsablauf [285](#)
 - Benutzeraktivität [306](#)
 - Bereinigen [294](#)
 - Domäne [302](#)
 - Komponenten [301](#)
 - konfigurieren [292](#), [293](#)
 - PowerCenter Integration Service [304](#)
 - PowerCenter Repository Service [304](#)
 - SAP BW Service [305](#)
 - Speicherort [292](#), [293](#)
- Protokollereignisdateien
 - Beschreibung [290](#)
- Protokollereignisse
 - Arbeitsablauf [285](#)
 - Authentifizierung [302](#)
 - Autorisierung [302](#)
 - Benutzeraktivität [306](#)
 - Benutzerverwaltung [302](#)
 - Beschreibung [290](#)
 - Code [301](#)
 - Details, anzeigen [296](#)
 - Dienstname [301](#)
 - Domäne [302](#)
 - Domänenfunktionskategorien [301](#)
 - Domänenkonfiguration [302](#)
 - Knoten [301](#)
 - Knotenkonfiguration [302](#)
 - Komponenten [301](#)
 - Lizenzierung [302](#)
 - Lizenzierungsnutzung [302](#)
 - Lizenzierungsprotokolle [247](#)
 - Meldungscode [301](#)
 - message [301](#)
 - Protokoll-Manager [302](#)
 - Protokollagent [302](#)
 - Schweregradstufen [301](#)
 - Service Manager [302](#)
 - Thread [301](#)
 - Zeitstempel [301](#)
- Protokollmanager
 - Architektur [290](#)
 - Dienstname [301](#)
 - Knoten [301](#)
 - Meldungscode [301](#)
 - message [301](#)
 - ProcessID [301](#)
 - Protokollereignisse - Komponenten [301](#)
 - Protokollereignisse der Benutzeraktivität [306](#)
 - Schweregradstufen [301](#)
 - Thread [301](#)
 - verwenden [289](#)
 - Verzeichnisspeicherort, konfigurieren [292](#), [293](#)
 - Wiederherstellung [291](#)
 - Zeitstempel [301](#)
 - Zeitzone [295](#)
- Protokollverzeichnis
 - für Gateway-Knoten [84](#)

- Protokollverzeichnis (*Fortsetzung*)
 - Speicherort, konfigurieren [293](#)
 - Speicherort, Konfigurieren [292](#)
- Proz. Anteil verwendeter Partitionen (Eigenschaft)
 - Web Services Report [316](#)
- Prozessidentifikationsnummer
 - Protokollmanager [301](#)

Q

- Quelldatenbanken
 - Codepage [340](#)
- Quellen
 - Codepages [340](#), [360](#)

R

- Registerkarte "Protokolle"
 - Informatica Administrator [59](#)
- Registerkarte „Überwachen“
 - Informatica Administrator [49](#), [51](#)
- Registerkarte „Verwalten“
 - Ansicht „Pläne“ [49](#)
 - Ansicht Dienste und Knoten. [38](#)
 - Ansicht Verbindungen [48](#)
 - Informatica Administrator [33](#), [38](#)
 - Navigator [33](#), [38](#)
- Registerkarte Berichte
 - Informatica Administrator [59](#)
- Reguläre Bezeichner
 - Datenbankverbindungen [233](#)
- Repository-Metadaten
 - Auswählen von Zeichen [347](#)
- Repository-Zusammenfassung
 - Lizenzverwaltungsbericht [311](#)
- Repositorys
 - Backup-Verzeichnis [103](#)
 - Codepages [339](#)
 - Unicode [330](#)
 - Unterstützte Codepages [358](#)
 - UTF-16LE [330](#)
- Ressourcenmanager-Dienst
 - Protokollereignisse [305](#)
 - Systemdienste [45](#)
- Rollen
 - Knoten [99](#)
 - Übersicht [62](#)

S

- SAP BW Service
 - Log-Ereignisse [305](#)
- SAP BW-Dienst
 - Anwendungsdienst [41](#)
- SAP-Verbindungen
 - Eigenschaften [217](#)
- Scheduler-Dienst
 - Protokollereignisse [305](#)
- Schwellenwert für die Ressourcenbereitstellung
 - Einstellung für Knoten [103](#)
- Sequenzielle Verbindungen
 - Eigenschaften [219](#)
- Service Manager
 - Protokollereignisse [302](#)

- Severity levels
 - Protokollereignisse [301](#)
- Sicherheit
 - Audit Trail [304](#)
 - Berechtigungen [81](#)
- Sicherheitsseite
 - Informatica Administrator [60](#)
 - Navigator [60](#)
- sichern
 - Domänenkonfigurationsdatenbank [86](#)
- Sitzungen
 - Sortierreihenfolge [339](#)
- SMTP-Konfiguration
 - Alarmer [77](#)
- Snowflake-Verbindung
 - Eigenschaften [222](#)
- Sortierreihenfolge
 - Codepage [339](#)
- Spark HDFS-Staging-Verzeichnis
 - Hadoop-Verbindungseigenschaften [154](#)
- Spark-Ausführungsparameter
 - Hadoop-Verbindungseigenschaften [154](#)
- Spark-Bereitstellungsmodus
 - Hadoop-Verbindungseigenschaften [154](#)
- Spark-Engine
 - Verbindungseigenschaften [154](#)
- SQL-Datendienste
 - Überwachung [273](#)
- Stacktraces
 - anzeigen [296](#)
- Statistik
 - zum Überwachen [55](#)
- Statistiken
 - Web Services Hub [315](#)
- Status der Operationen
 - Domäne [114](#)
 - PowerCenter-Integrationsdienst [114](#)
 - PowerCenter-Repository-Dienst [114](#)
- Stoppen
 - Informatica-Domäne [91](#)
- Suchbereich
 - Informatica Administrator [60](#)
- Sybase ASE
 - Verbindungszeichenfolge, Syntax [388](#)
- Systemdienste
 - Ressourcenmanager-Dienst [45](#)
- Systemgebietsschemata
 - Beschreibung [332](#)

T

- Tabellen zur Hochverfügbarkeits-Persistenz
 - PowerCenter-Integrationsdienst [117](#)
- Tableau V3-Verbindung
 - Eigenschaften [226](#)
- Target-Datenbanken
 - Codepage [341](#)
- Targets
 - Codepages [341](#)
- TCP KeepAlive-Timeout
 - Hohe Verfügbarkeit [120](#)
- TCP/IP-Netzwerkprotokoll
 - Anforderung für Integration Service [387](#)
 - Knoten [380](#)
 - PowerCenter Client [380](#)
 - PowerCenter-Domänen [380](#)

- Teilmenge
 - definiert für die Codepage-Kompatibilität [336](#)
- Teradata
 - Verbindungszeichenfolge, Syntax [388](#)
- testen
 - Datenbankverbindungen [124](#)
- Thread-Identifizierung
 - Registerkarte "Protokolle" [301](#)
- Threads
 - Protokollmanager [301](#)
- Twitter-Streaming-Verbindungen
 - Eigenschaften [228](#)

U

- Übergeordnete Menge
 - definiert für die Codepage-Kompatibilität [336](#)
- Übersicht
 - Verbindungen [121](#)
- Übersichtsstatistik
 - Überwachen [261](#)
- überwachen
 - Anwendungen [269](#)
 - Arbeitsabläufe [278](#)
 - Berichte [56](#)
 - Statistik [55](#)
- Überwachen
 - Bereitgestellte Zuordnungsjobs [269](#)
 - Beschreibung [256](#)
 - Detaillierte Statistiken [263](#)
 - Einstellungen, konfigurieren [259](#)
 - Exportieren der Übersichtsstatistik [262](#)
 - historische Statistik [263](#)
 - Jobs [263](#)
 - Konfigurieren [258](#)
 - Setup [257](#)
 - Übersichtsstatistik [261](#), [263](#)
 - Übersichtsstatistik anzeigen [262](#)
- Überwachung
 - Data Integration Services [262](#)
 - Logische Datenobjekte [272](#)
 - SQL-Datendienste [273](#)
 - Web-Dienste [276](#)
- Überwachungsmodellrepository-Dienst
 - Anwendungsdienst [41](#)
- UCS-2
 - Beschreibung [330](#)
- Umgebungsvariablen
 - Fehlersuche [84](#)
 - LANG_C [335](#)
 - LC_ALL [335](#)
 - LC_CTYPE [335](#)
 - NLS_LANG [349](#), [351](#)
- Unicode
 - GB18030 [330](#)
 - Repositorys [330](#)
 - UCS-2 [330](#)
 - UTF-16 [330](#)
 - UTF-16LE [330](#)
 - UTF-32 [330](#)
- Unicode-Modus
 - Übersicht [333](#)
- UNIX
 - Codepages [335](#)
- UNIX-Umgebungsvariablen
 - LANG_C [335](#)
 - LC_ALL [335](#)

UNIX-Umgebungsvariablen (*Fortsetzung*)

LC_CTYPE [335](#)

UTF-16

Beschreibung [330](#)

UTF-16LE

Beschreibung [330](#)

Speicher [339](#)

UTF-32

Beschreibung [330](#)

V

validieren

Codepages [344](#)

Lizenzen [247](#)

Verbinden von

SQL-Datendienst [125](#)

Verbindung

Details [196](#)

Eigenschaften [196](#)

Verbindungen

Eigenschaften [154](#)

Salesforce Marketing Cloud [215](#)

aktualisieren [123](#)

bearbeiten [124](#)

Datenbankbezeichnereigenschaften [233](#)

Erstellen von Datenbankverbindungen [122](#)

Google PubSub [153](#)

löschen [124](#)

Pass-Through-Sicherheit [125](#)

Pass-Through-Sicherheit hinzufügen [126](#)

testen [124](#)

Übersicht [121](#)

Web Services-Eigenschaften [231](#)

Verbindungen für Teradata Parallel Transporter

Eigenschaften [223](#)

Verbindungs-Strings

native Konnektivität [388](#)

Verbindungseigenschaften

Databricks [145](#)

Blockchain [139](#)

Verbindungspooling

Eigenschaften [126](#)

Verbindungszeichenfolge

Beispiele [388](#)

Syntax [388](#)

Verknüpfte Domäne

Mehrere Domänen [76](#)

verwalten

Benutzerkonten [28](#)

Konten [28](#)

Verzeichnis des Spark-Ereignisprotokolls

Hadoop-Verbindungseigenschaften [154](#)

Vollständige Historienstatistik

Web Services-Bericht [320](#)

VSAM-Verbindungen

Eigenschaften [229](#)

W

Web Services Hub

Anwendungsdienst [26](#)

Web Services Hub (*Fortsetzung*)

Log-Ereignisse [306](#)

Statistiken [315](#)

Web Services Report

Aktivitätsdaten [316](#)

Durchschn. Anz. der Ausführungsinstanzen (Eigenschaft) [316](#)

Durchschn. Anz. der Dienstpartitionen (Eigenschaft) [316](#)

Durchschn. DTM-Zeit (Eigenschaft) [316](#)

Durchschnittliche Dienstzeit (Eigenschaft) [316](#)

Inhalt [316](#)

Proz. Anteil verwendeter Partitionen (Eigenschaft) [316](#)

Web Services-Bericht

Laufzeitstatistiken [318](#)

Vollständige Historienstatistik [320](#)

Web-Dienste

Überwachung [276](#)

Web-Verbindungen

Eigenschaften [170](#)

Webdienst-Hub

Anwendungsdienst [41](#)

Wiederherstellen

Domänen-Konfigurationsdatenbank [86](#)

Wiederherstellung

Datenintegrationsdienst [114](#)

Hohe Verfügbarkeit [114](#)

Integration Service [114](#)

PowerCenter-Repository-Dienst [114](#)

Worker-Knoten

Beschreibung [98](#)

Konfigurieren als Gateway [84](#)

X

X Virtual Frame Buffer

für Lizenzbericht [308](#)

für Web-Dienste-Bericht [308](#)

XML

Logs exportieren in [299](#)

Z

Zeichengrößen

Doppeltes Byte [336](#)

Einfaches Byte [336](#)

Multibyte [336](#)

Zeitpläne

Bearbeiten [239](#)

löschen [240](#)

Übersicht [236](#)

Zeitpläne erstellen [237](#)

Zeitstempel

Protokollmanager [301](#)

Zeitzone

Protokollmanager [295](#)

Ziele

Codepages [360](#)

zu Datenbanken verbinden

JDBC [388](#)