opentext™

OpenText™ Identity Manager CE 24.4 (v4.10)

Installations- und Upgrade-Anleitung für Windows

Januar 2025

Rechtliche Hinweise

Copyright 2009–2024 Open Text Alle Rechte vorbehalten.

Für Produkte und Services von Open Text oder seinen verbundenen Unternehmen und Lizenznehmern („Open Text“) gelten nur die Gewährleistungen, die in den Gewährleistungserklärungen, die solchen Produkten beiliegen, ausdrücklich beschrieben sind. Aus den in dieser Publikation enthaltenen Informationen ergibt sich keine zusätzliche Gewährleistung. Open Text haftet nicht für technische oder redaktionelle Fehler oder Auslassungen in diesem Dokument. Die in diesem Dokument enthaltenen Informationen sind vorbehaltlich etwaiger Änderungen.

Inhalt

Info zu diesem Handbuch und zur Bibliothek **11**

Teil I Überblick über die Umgebung von OpenText Identity Manager **13**

1 Kurze Einführung zu den Komponenten von OpenText Identity Manager **15**

Komponenten des OpenText Identity Manager-Servers 16
OpenText Identity Manager Server 17
Remote Loader 18
Fan-out-Agent 18
OpenText Identity Console 18
Identity Applications-Komponenten 19
Benutzeranwendung 19
Authentifizierungsservice 19
Self-Service Password Reset 20
Web-Anwendungsserver 20
Datenbank der Identity Applications 20
Treiber für Identity Applications 21
Komponenten von Identity Reporting 21
Identity Reporting 22
Authentifizierungsservice 22
Self-Service Password Reset 22
Identity Reporting-Datenbank 22
Web-Anwendungsserver 23
Treiber für Identity Reporting 23
Sentinel for Log Management für Identity Governance and Administration 24
OpenText Identity Manager-Werkzeuge 24
Designer für OpenText Identity Manager 25
Analyzer für OpenText Identity Manager 25
Funktionelle Architektur 26
Bereitstellungsoptionen für OpenText Identity Manager 27
Beispiele für OpenText Identity Manager-Bereitstellungen 28
Beispiel für die Bereitstellung einer Advanced Edition 30
Beispiel für die Bereitstellung einer Standard Edition 32

Teil II Planen der Installation von OpenText Identity Manager **35**

2 Planen der Installation **37**

Festlegen der Hardwareanforderungen 37
Arbeitsblatt zur Bereitstellungsplanung 38
Arbeitsblatt zur Architektur 38
Arbeitsblatt zu den Systemanforderungen 39
Überprüfen der Ports für die OpenText Identity Manager-Komponenten 39

Teil III Installieren und Konfigurieren der OpenText Identity Manager-Komponenten 41

3 Überblick über den Installations- und Konfigurationsvorgang 43

Installationsreihenfolge . . . 43
Erläuterungen zum Installations- und Konfigurationsvorgang für die Komponenten OpenText Identity Manager Server, Identity Applications und Identity Reporting . . . 43
Installationsmethoden . . . 44
Installationsoptionen . . . 44
Konfigurationsmodi . . . 45
Verwenden von nicht intuitiven Passwörtern bei der Konfiguration . . . 45
Erläuterungen zum Installationsvorgang für Designer und Analyzer . . . 45
Installationsverfahren . . . 46
Installationsverfahren für OpenText Identity Manager Server, Identity Applications und Identity Reporting . . . 46
Installation des Remote Loader . . . 48
Installieren des Java Remote Loader . . . 49
Installieren des .NET Remote Loader . . . 51
Installieren von SSPR . . . 51
Konfigurationseinstellungen in . . . 52
Arbeitsblatt für die Konfiguration der OpenText Identity Manager-Engine . . . 52
Arbeitsblatt zur Konfiguration von Identity Applications . . . 54
Arbeitsblatt zur Konfiguration von Identity Reporting . . . 57
Konfiguration des Arbeitsblatts für Self-Service Password Reset . . . 59
Schritte nach der Installation . . . 60
Übergeben der preferIPv4Stack-Eigenschaft an die JVM . . . 61
Prüfen des Serverzustands . . . 61
Überwachen der Zustandsstatistiken . . . 61
Erstellen von Verbundindizes . . . 62
Konfigurieren der Identity-Anwendung für das Ablehnen einer vom Client initiierten erneuten SSL-Aushandlung . . . 63

4 Abschließende Konfigurationsschritte 65

Das Konfigurieren des Identitätsdepots . . . 65
Manuelles Importieren der Identity Applications- und Identity Reporting-Zertifikate im Identitätsdepot . . . 65
Konfigurieren des Remote Loader und der Treiber . . . 66
Konfigurieren der „Passwort vergessen“-Verwaltung . . . 66
Verwenden der Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung für die „Passwort vergessen“-Verwaltung . . . 66
Verwenden eines externen Systems für die „Passwort vergessen“-Verwaltung . . . 69
Aktualisieren der SSPR-Links im Dashboard für eine dezentrale Umgebung oder eine Cluster-Umgebung . . . 71
Konfigurieren der Datenbank für Identity Applications . . . 71
Konfigurieren einer Oracle-Datenbank . . . 71
Konfigurieren einer SQL Server-Datenbank . . . 73
Konfigurieren von Identity Applications . . . 74
Konfigurieren der Einstellungen für Identity Applications . . . 74
Bereitstellen von REST-APIs für Identity Applications . . . 98
Zugreifen auf die Oracle-Datenbank anhand des Oracle-Service-Namens . . . 99
Manuelles Erstellen der Datenbank . . . 99
Konfigurieren der Single Sign-on-Einstellungen für Identity Applications . . . 101

Starten der Identity Applications 102
Überlegungen zur Konfiguration und Nutzung der Identity Applications 102
Konfigurieren der Laufzeitumgebung für die Datenerfassung 102
Konfigurieren des DCS-Treibers für das Erfassen von Daten aus den Identity Applications 103
Migrieren des DCS-Treibers. 104
Zusätzliche Unterstützung für benutzerdefinierte Attribute und Objekte 106
Zusätzliche Unterstützung für mehrere Treibersätze 109
Konfigurieren der Treiber für die Ausführung im Remote-Modus mit SSL 110
Konfigurieren von Identity Reporting 112
Manuelles Hinzufügen der Datenquelle auf der Seite der Identity-Datenerfassungsdienste 112
Ausführen von Berichten über eine Oracle-Datenbank 113
Manuelles Erstellen des Datenbankschemas 113
Bereitstellen von REST-APIs für Identity Reporting 117
Verbinden mit einer entfernten PostgreSQL-Datenbank 117
Schritte nach der Installation für Identity Reporting 118
OpenText Identity Manager aktivieren 119

Teil IV Konfigurieren von OpenText Identity Manager im FIPS-Modus 121

5 Konfigurieren von JRE für FIPS 123

6 Konfigurieren von OpenText Identity Manager Engine im FIPS-Modus 125

7 Konfigurieren von Remote Loader im FIPS-Modus 127

8 Konfigurieren des Fan-out-Agenten im FIPS-Modus 129

Prozedur. 129

9 Konfigurieren von Identity Applications und Identity Reporting im FIPS-Modus 131

Prozedur. 131

Teil V Installation von Designer 135

10 Planen der Installation von Designer 137

Checkliste für die Installation von Designer 137

11 Installation von Designer 139

Ausführen der ausführbaren Windows-Datei. 139
Verwenden der automatischen Installation 139
Installieren von Designer in einem anderen Gebietsschema als dem Systemgebietsschema 140
Bearbeiten eines Installationspfads mit Leerzeichen. 141

Teil VI Installation von Analyzer 143

12 Planen der Installation von Analyzer 145

Checkliste für die Installation von Analyzer 145

13 Installation von Analyzer 147

Ausführen der ausführbaren Windows-Datei 147
Verwenden der automatischen Installation 147

14 Aufgaben nach Abschluss der Installation 149

Konfigurieren eines verbundenen Systems 149
Erstellen und Konfigurieren eines Treibersatzes 149
Erstellen von Treibersätzen 150
Zuweisen der Standardpasswortrichtlinie zu Treibersätzen 150
Erstellen des Passwortrichtlinienobjekts im Identitätsdepot 150
Erstellen einer benutzerdefinierten Passwortrichtlinie 151
Erstellen des Standard-Benachrichtigungssammlungs-Objekts im Identitätsdepot 152
Erstellen eines Driver 152
Definieren von Richtlinien 153
Verwalten von Treiberaktivitäten 153

Teil VII Aufrüsten von OpenText Identity Manager 155

15 Vorbereiten der Aufrüstung von OpenText Identity Manager 157

Checkliste für die Aufrüstung von OpenText Identity Manager 157
Erläuterungen zur Aufrüstung und zur Migration 159
Unterstützte Aufrüstungspfade 160
Aufrüsten von Identity Manager 4.7.5 160
Aufrüsten von Identity Manager 4.8.x 162
Sichern der aktuellen Konfiguration 164
Exportieren des Designer-Projekts 164
Exportieren der Treiberkonfiguration 166

16 Aufrüsten der OpenText Identity Manager-Komponenten 167

Überlegungen für das Upgrade 167
Upgrade-Reihenfolge 168
Upgrade von Designer 168
Aufrüsten der OpenText Identity Manager-Engine-Komponenten 169
Upgrade des Identitätsdepots 169
Upgrade der OpenText Identity Manager-Engine 170
Aufrüstung von Remote Loader 172
Aufrüstung des Java Remote Loader 174
Aufrüsten des Fan-out-Agent 175
Aufrüsten von Identity Applications 175
Erläuterungen zum Aufrüstungsprogramm 176
Voraussetzungen für die Aufrüstung 176
Systemanforderungen 176

Aufrüsten der PostgreSQL-Datenbank 176
Upgrade der Treiberpakete für Identity Applications 179
Aufrüsten von Identity Applications 179
Aufgaben nach der Aufrüstung für Identity Applications 180
Aufrüsten von Identity Reporting 184
Voraussetzungen für die Aufrüstung 184
Aufrüsten von Identity Reporting 185
Schritte nach der Aufrüstung für Reporting 185
Ändern der Verweise auf reportRunner in der Datenbank 187
Überprüfen der Aufrüstung für Identity Reporting 187
Aufrüsten von Analyzer 188
Arbeitsschritte nach der Aktualisierung 188
Konfigurieren von TLSv1.3 für Tomcat-Dienste 188
Aufgaben nach dem Upgrade im FIPS-aktivierten Modus 189
Anhalten und Starten der OpenText Identity Manager-Treiber 190
Anhalten der Treiber 190
Starten der Treiber 191
Aufrüsten der OpenText Identity Manager-Treiber 192
Einen neuen Treiber erstellen 192
Vorhandene Inhalte durch Inhalte aus Paketen ersetzen 192
Aktuelle Inhalte beibehalten und neue Inhalte über Pakete hinzufügen 193
Hinzufügen von neuen Servern zum Treibersatz 194
Hinzufügen des neuen Servers zum Treibersatz 194
Entfernen des alten Servers aus dem Treibersatz 194
Wiederherstellen der benutzerdefinierten Richtlinien und Regeln für den Treiber 195
Wiederherstellen benutzerdefinierter Richtlinien und Regeln für den Treiber mithilfe von Designer 196
Wiederherstellen benutzerdefinierter Richtlinien und Regeln für den Treiber mit der OpenText Identity Console 196

17 Wechseln von der Advanced Edition zur Standard Edition 199

Teil VIII Migrieren der OpenText Identity Manager-Daten in eine neue Installation 201

18 Vorbereiten der Migration von OpenText Identity Manager 203

Checkliste für die Migration 203

19 Migrieren von OpenText Identity Manager auf einen neuen Server 205

Checkliste für die Migration von OpenText Identity Manager 205
Vorbereiten des Designer-Projekts auf die Migration 206
Kopieren von serverspezifischen Informationen für den Treibersatz 207
Kopieren der serverspezifischen Informationen in Designer 207
Ändern der serverspezifischen Informationen in der OpenText Identity Console 208
Ändern der serverspezifischen Informationen für die Benutzeranwendung 209
Migrieren der OpenText Identity Manager-Engine auf einen neuen Server 209
Migrieren des Benutzeranwendungstreibers 209
Importieren eines neuen Basispakets 209
Aufrüsten eines vorhandenen Basispakets 210
Bereitstellen des migrierten Treibers 210
Aufrüsten der Identity Applications 211

Migrieren von Identity Applications 211
Migrieren der Datenbank zum neuen Server 212
Installieren von Identity Applications auf dem neuen Server 213
Abschließen der Migration der Identity Applications 213
Vorbereiten einer Oracle-Datenbank für die SQL-Datei 213
Leeren des Browsercache 214
Aktualisieren der Einstellung für die maximale Zeitüberschreitung für das SharedPagePortlet 215
Deaktivieren der Einstellung für automatische Abfragen für Gruppen 215

Teil IX Bereitstellen von OpenText Identity Manager in Microsoft Azure 217

20 Planung und Implementierung von OpenText Identity Manager in Microsoft Azure 219

Voraussetzungen 219
Bereitstellungsverfahren 219
Erstellen einer Ressourcengruppe 221
Erstellen eines virtuellen Netzwerks und Teilnetzes 221
Erstellen eines Anwendungs-Gateways 222
Erstellen einer VM-Instanz 224
Aktualisieren von Host-Einträgen in der VM 225
Einrichten von Designer 226
Konfigurieren des Anwendungs-Gateways 226

21 Beispielszenarien für Hybrid OpenText Identity Manager 231

Verwenden der Treibersatzverbindung mehrerer Server 231
Verwenden der OpenText eDirectory-Treiberverbindung 232

Teil X Bereitstellen von OpenText Identity Manager für Hochverfügbarkeit 233

22 Vorbereiten der Installation von OpenText Identity Manager in einer Clusterumgebung 235

Voraussetzungen 235
Identitätsdepot 235
Identity Applications 236
Datenbank für Identity Applications 236
Vorbereiten eines Clusters für Identity Applications 237
Erläuterungen zu Clustergruppen in Tomcat-Umgebungen 237
Festlegen der Systemeigenschaften für Workflow-Engine-IDs 237
Verwenden eines einzigen Master-Schlüssels für alle Benutzeranwendungen im Cluster 238

23 Beispiellösung für eine Identity Manager-Clusterbereitstellung 239

Voraussetzungen 239
Konfigurieren von OpenText Identity Manager in einem OpenText eDirectory-Cluster 239
Clustering für Remote Loader 240

24 Beispiellösung für eine Identity Applications-Clusterbereitstellung 241

Voraussetzungen 242

Installationsvorgang 243
Aktivieren des Berechtigungsindex für das Clustering 249

25 Deinstallieren der OpenText Identity Manager-Komponenten 251

Deinstallieren von Identity Reporting 251
Entfernen von Objekten aus dem Identitätsdepot 252
Deinstallieren der OpenText Identity Manager-Engine 253
Deinstallieren von Remote Loader 253
Deinstallieren der Identity Applications 253
Löschen der Treiber für das rollenbasierte Bereitstellungsmodul 253
Deinstallieren der Identity Applications 254
Deinstallieren der Identity Reporting-Komponenten 254
Löschen der Berichterstellungstreiber 255
Deinstallieren von Identity Reporting 255
Deinstallation von Analyzer 256
Deinstallation von Designer 256

26 Fehlerbehebung 257

Fehlersuche bei der OpenText Identity Manager-Engine 257
Fehlersuche bei Identity Applications und der RBPM-Installation 258
Fehlersuche bei der Installation und Deinstallation 262
Fehlersuche bei der Anmeldung 266
Behebung des SSPR-Seitenanforderungsfehlers 269
Fehlersuche zu dem Problem ".NET Remote Loader startet nicht" unter Windows 2016 269
Fehlerbehebung 502 Fehlerhaftes Gateway beim Laden der Formulare in der Azure-Bereitstellung 270

Info zu diesem Handbuch und zur Bibliothek

Die *Installations- und Upgrade-Anleitung* bietet Anweisungen zum Installieren oder Aktualisieren von OpenText™ Identity Manager CE 24.4 (v4.10) (OpenText Identity Manager). In diesem Handbuch werden die Installation und die Konfiguration einzelner Komponenten in einer dezentralen Umgebung beschrieben.

Zielgruppe

Dieses Handbuch richtet sich an Identitätsarchitekten und Identitätsadministratoren, die für die Installation der erforderlichen Komponenten einer Identitätsmanagement-Lösung in ihrer Organisation zuständig sind.

Weitere Informationen in der Bibliothek

Weitere Informationen zur OpenText Identity Manager-Bibliothek finden Sie auf der Website der OpenText Identity Manager-Dokumentation (https://www.netiq.com/documentation/identity-manager-4.10/).

Überblick über die Umgebung von OpenText Identity Manager

Dieses Handbuch konzentriert sich auf die Aufgaben, die Sie zur Installation und Konfiguration von OpenText Identity Manager ausführen müssen.

Wenn OpenText Identity Manager neu für Sie ist, machen Sie die folgenden Abschnitte mit der Lösung und den enthaltenen Komponenten des Programms vertraut. Die Komponenten, die Sie herunterladen und installieren können, werden von Ihrer OpenText Identity Manager-Edition bestimmt.

- Kurze Einführung zu den Komponenten von OpenText Identity Manager
- Funktionelle Architektur

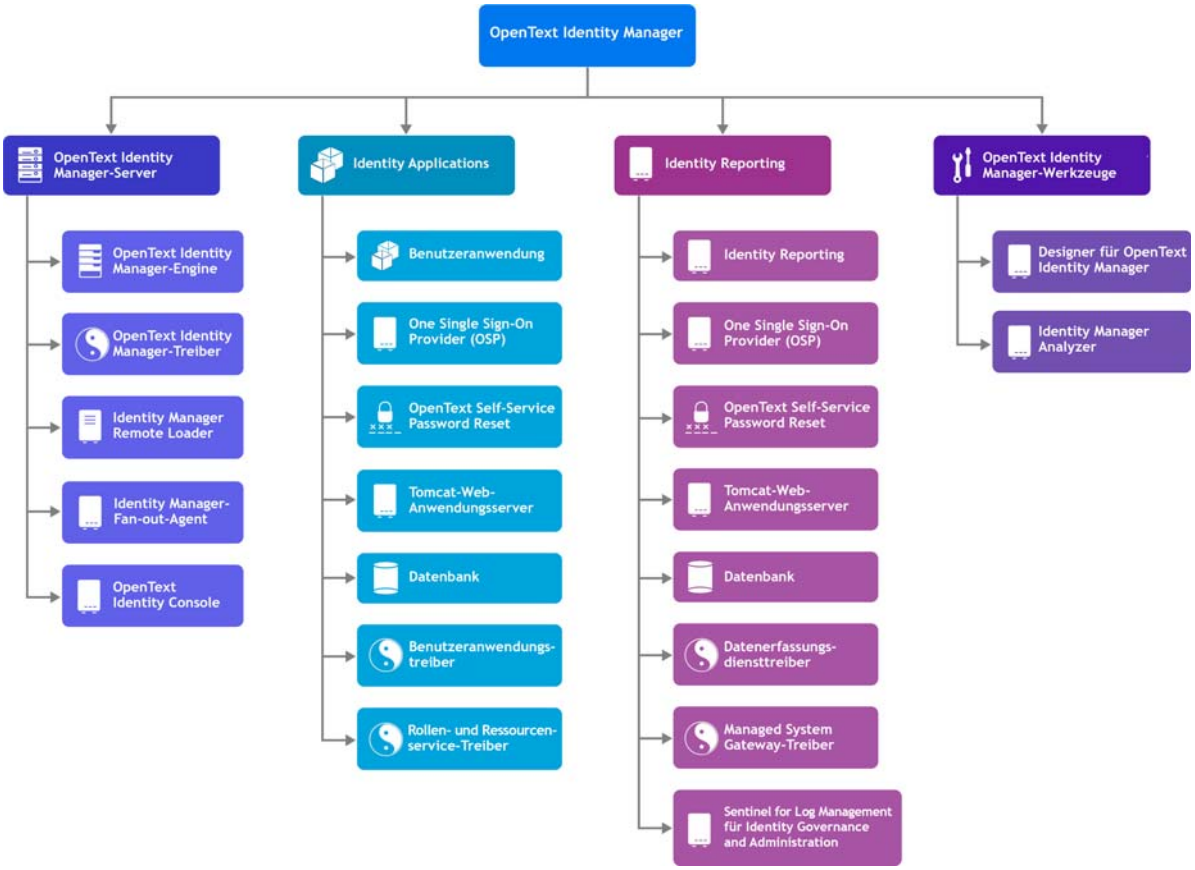
1 Kurze Einführung zu den Komponenten von OpenText Identity Manager

Um die unterschiedlichen Bedürfnisse der Kunden zu erfüllen, ist OpenText Identity Manager in den Advanced und Standard Editions erhältlich. Jede Edition umfasst mehrere Funktionen und jede Funktion wird von mehreren Komponenten verarbeitet. Daher kann Ihre OpenText Identity Manager-Implementierung je nach Ihren Anforderungen eine oder alle der folgenden Komponenten umfassen:

- Identity Manager Server
- Identity Applications
- Identity Reporting
- OpenText Identity Manager-Werkzeuge

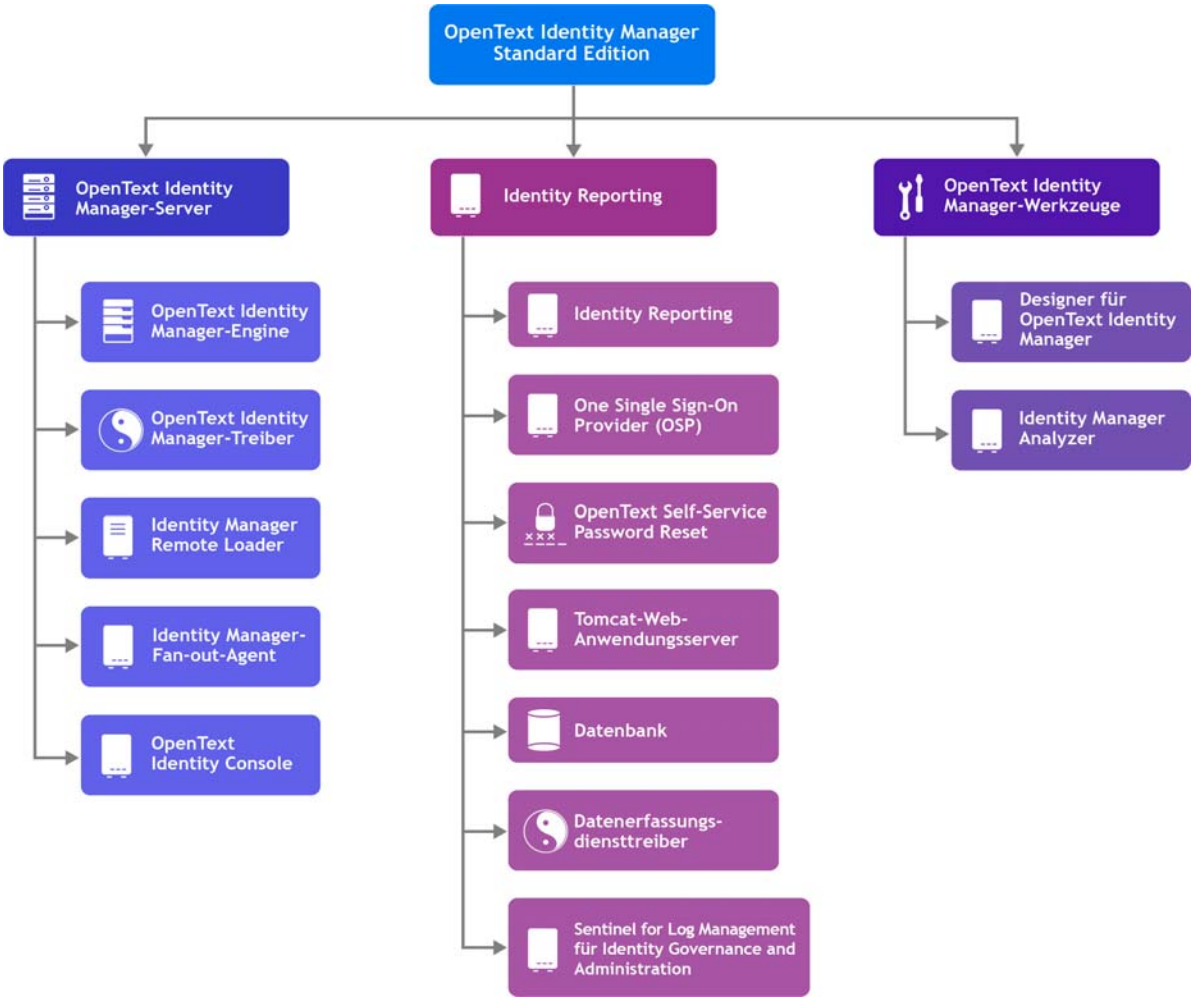
In Abbildung 1-1 sind die Komponenten aufgeführt, die in der Umgebung der OpenText Identity Manager Advanced Edition bereitgestellt werden.

Abbildung 1-1 *Komponenten für OpenText Identity Manager Advanced Edition*



In Abbildung 1-2 sind die Komponenten aufgeführt, die in der Umgebung der OpenText Identity Manager Standard Edition bereitgestellt werden.

Abbildung 1-2 *Komponenten für OpenText Identity Manager Standard Edition*



Je nachdem, wie die Komponenten miteinander interagieren, werden einige Komponenten logisch als eine Gruppe von Komponenten installiert. Einige Komponenten werden als eigenständige Komponenten installiert, um die Installation zu erleichtern. Informationen zur Interaktion der Komponenten finden Sie im Überblick und Planungshandbuch zu OpenText™ Identity Manager CE 24.4 (v4.10).

Lesen Sie die Informationen in den folgenden Abschnitten, um zu verstehen, wie die Komponenten gruppiert sind und wie jede Komponente oder eine Gruppe von Komponenten installiert wird.

Komponenten des OpenText Identity Manager-Servers

Erforderlich für alle Installationen

Eine Installation des OpenText Identity Manager Server setzt sich aus den folgenden Komponenten zusammen.

OpenText Identity Manager Server

Der OpenText Identity Manager Server führt Aufgaben in OpenText Identity Manager aus. Er umfasst ein Identitätsdepot, die Identity Manager-Engine und OpenText Identity Manager-Treiber.

Zur Unterstützung der Vorgänge des OpenText Identity Manager Servers installiert das Installationsprogramm eine unterstützte Version der Oracle Java-Laufzeitumgebung (Java Runtime Environment, JRE). Installieren Sie die Komponenten des OpenText Identity Manager Servers über die **OpenText Identity Manager-Engine**-Installationsoption des Installationsprogramms.

Identitätsdepot

Bei der Installation der OpenText Identity Manager-Engine wird eine Verbindung zum Identitätsdepot hergestellt und konfiguriert. OpenText Identity Manager nutzt das Identitätsdepot als das Standard-Repository für alle Identitätsdaten. Die Identitätsdaten enthalten den aktuellen Status der verwalteten Identitäten, einschließlich Benutzerkonto und Organisationsdaten.

OpenText Identity Manager-Engine

Die OpenText Identity Manager-Engine verarbeitet die Datenänderungen, die im Identitätsdepot oder in einer verbundenen Anwendung vorgenommen werden. Der Server, auf dem die OpenText Identity Manager-Engine ausgeführt wird, wird als OpenText Identity Manager-Server bezeichnet.

OpenText Identity Manager-Treiber

Der OpenText Identity Manager Server verarbeitet die Bereitstellung der Benutzer und verwaltet verbundene Systemkonten und -gruppen über Treiber. Ein Treiber ist die Softwareschnittstelle zu einem verbundenen System.

OpenText Identity Manager-Treiber werden als Teil der OpenText Identity Manager Serverarchitektur ausgeführt. Ein Treiber fungiert als Gateway zu einer nativen Systemtechnologie vom Endpunkttyp. Beispielsweise können Computer, auf denen Active Directory-Services ausgeführt werden, nur verwaltet werden, wenn der Active Directory-Treiber entweder auf dem OpenText Identity Manager Server installiert ist oder auf dem Server der Zielanwendung, mit dem der OpenText Identity Manager Server kommunizieren kann. Treiber verwalten die Objekte, die sich auf dem verbundenen System befinden. Verwaltete Objekte sind Konten, Gruppen und (optional) bestimmte Objekte vom Endpunkttyp.

Ein Treiber übersetzt die Aktionen der OpenText Identity Manager-Engine in Änderungen am verbundenen System, wie "Ein neues Email-Konto auf einem verbundenen Microsoft Exchange-System erstellen". Mit jedem in OpenText Identity Manager konfigurierten Treiber ist eine Ereigniscachedatei (TAO-Datei) verknüpft. Ereignisse werden im Cache der TAO-Datei gespeichert, bevor sie vom Treiber verarbeitet werden. Die Cache-Dateien befinden sich standardmäßig im DIB-Verzeichnis (Informationsdatenbank) des Identitätsdepots.

OpenText Identity Manager bietet einige integrierte Treiber (Java, nativ, .NET) für die Verwaltung von Verbindungen mit verschiedenen Typen des verbundenen Systems. Mit OpenText Identity Manager kann auch ein benutzerdefinierter Treiber entwickelt werden, um die Datensynchronisierung mit einer Vielzahl von anderen Systemen zu ermöglichen. Dazu zählen eine selbst entwickelte Anwendung oder ein Repository ohne Technologieschnittstelle, das keine Standardtreiber nutzen kann.

Remote Loader

Treiber können lokal am OpenText Identity Manager Server oder mit einem Remote Loader installiert werden. Ein Remote Loader lädt die Treiber, die auf den Remote-Servern installiert sind, und kommuniziert an deren Stelle mit der OpenText Identity Manager-Engine. Wenn die Anwendung auf demselben Server wie die OpenText Identity Manager-Engine ausgeführt wird, können Sie den Treiber auf diesem Server installieren. Wird die Anwendung dagegen nicht auf demselben Server wie die OpenText Identity Manager-Engine ausgeführt, müssen Sie den Treiber auf dem Anwendungsserver installieren. Zur Erleichterung der Auslastung und der Konfiguration der Umgebung können Sie den Remote Loader auf einem separaten Server installieren, also nicht auf demselben Server wie Tomcat und den OpenText Identity Manager-Server. Weitere Informationen zu Remote Loader finden Sie unter Bestimmen, wann Remote Loader verwendet werden soll im Verwaltungshandbuch zu OpenText™ Identity Manager CE 24.4 (v4.10)-Treiber.

Installieren Sie den Remote Loader-Service und die Treiberinstanzen im Remote Loader über die Option **Identity Manager Remote Loader-Server**.

Fan-out-Agent

Der Fan-out-Agent von Identity Manager ist eine Installationskomponente, die vom JDBC(Java Database Connectivity)-Fan-out-Treiber genutzt wird, um mehrere JDBC-Fan-out-Treiberinstanzen zu erstellen. Der Fan-out-Treiber stellt mit minimalem Aufwand für mehrere Datenbanken Benutzer, Gruppen und Passwörter bereit. Der OpenText Identity Manager-Administrator ist dadurch nicht mehr gezwungen, mehrere JDBC-Treiber mit denselben Richtlinien wie für die Bereitstellung mehrerer Datenbanken desselben Typs zu konfigurieren. Sie können Benutzerkonten zentral verwalten und sie gegebenenfalls automatisch erstellen, konfigurieren, pflegen und entfernen lassen. Weitere Informationen finden Sie im *NetIQ Identity Manager-Treiber für JDBC-Fan-out – Implementierungshandbuch (https://www.netiq.com/documentation/identity-manager-4.10-drivers/jdbc_fanout/data/netiq-identity-manager-for-jdbc-fan-out-driver-implementation-guide.html)*.

Installieren Sie den Fan-out-Agent über die Installationsoption **Identity Manager Fan-out-Agent** des Installationsprogramms.

OpenText Identity Console

Die OpenText Identity Console ersetzt iManager.

OpenText Identity Console ist eine webbasierte Administrationskonsole, mit der Sie über das Internet und einen Webbrowser von einem beliebigen Standort aus auf virtuelle, sichere und benutzerdefinierte Weise auf Netzwerkadministrationsprogramme zugreifen können. Das Programm erleichtert die dezentrale Bearbeitung von Administrationsaufgaben.

Mit der OpenText Identity Console können Sie ähnliche Funktionen wie mit Designer ausführen und außerdem den Zustand des Systems überwachen. Es empfiehlt sich, die Administration mit der OpenText Identity Console vorzunehmen. Designer eignet sich dagegen für Konfigurationsaufgaben, die Änderungen an Paketen, Modellierung und Tests vor der Bereitstellung erfordern.

Weitere Informationen finden Sie im OpenText™ Identity Console-Administrationshandbuch.

Identity Applications-Komponenten

Erforderlich für die Installation der Advanced Edition

Identity Applications besteht aus einer Reihe miteinander verbundener browsergestützter Webanwendungen. Ihre Organisation verwaltet hiermit die Benutzerkonten und Berechtigungen für die zahlreichen verschiedenen Rollen und Ressourcen, die den Benutzern zur Verfügung stehen. Sie können Identity Applications mit Selbstbedienungssupport für Ihre Benutzer einrichten, z. B. zum Anfordern von Rollen oder zum Ändern der Passwörter. Außerdem können Sie Workflows einrichten, mit denen sich die Rollen und Ressourcen noch effizienter verwalten und zuweisen lassen. Identity Applications besteht aus einer Verwaltungskonsole (für Verwaltungsaufgaben), der Benutzerkonsole (Dashboard) und REST-Services, mit denen Sie diese Aufgaben ausführen.

HINWEIS: Vor der Installation von Identity Applications muss die OpenText Identity Manager-Engine installiert sein.

Installieren Sie Identity Applications-Komponenten über die Installationsoption **Identity Applications** des Installationsprogramms.

Eine Identity Applications-Installation setzt sich aus den folgenden Komponenten zusammen:

Benutzeranwendung

In der browsergestützten Benutzeranwendung erledigen die Benutzer verschiedene Identitäts-Self-Service-Aufgaben und Rollenbereitstellungsaufgaben. Einige der Aufgaben, die in früheren Versionen des Produkts auf der Oberfläche der Benutzeranwendung ausgeführt wurden, befinden sich nun auf der neuen Benutzeroberfläche mit einer Verwaltungskonsole und einer Benutzerkonsole. Die Benutzeranwendung stellt weiterhin einige Funktionen zur Verfügung, die noch nicht auf der neuen Benutzeroberfläche vorhanden sind. Weitere Informationen finden Sie im OpenText™ Identity Manager CE 24.4 (v4.10) – Administratorhandbuch zu Identity Applications.

Authentifizierungsservice

Der Authentifizierungsservice gewährt Zugriff auf die Funktionen von Identity Applications. Weitere Informationen über den Single Sign-on-Zugriff in OpenText Identity Manager finden Sie im OpenText™ Identity Manager CE 24.4 (v4.10) – Administratorhandbuch zu Identity Applications.

Der Authentifizierungsservice ist in der OSP-Komponente (One Single Sign-On Provider) enthalten. Für Identity Applications ist eine lokale Installation von OSP erforderlich. OSP wird automatisch mit Identity Applications installiert.

Self-Service Password Reset

Der Self-Service-Passwortverwaltungsservice ermöglicht den Zugriff auf die Self-Service-Passwortverwaltung. Identity Applications umfasst die Komponente Self Service Password Reset (SSPR), mit der Benutzer, die Zugriff auf Identity Applications besitzen, ihr Passwort ohne Administratoreingriff zurücksetzen können.

Im Installationsvorgang von Identity Applications wird SSPR standardmäßig aktiviert. SSPR kann jedoch auch auf einem separaten Computer installiert werden, falls er für Ihre Bereitstellung erforderlich ist oder falls Sie die Standard Edition installieren. Wenn Sie SSPR in der Advanced Edition auf einem separaten Computer installieren, müssen Sie die Passwortverwaltungseinstellungen in der Identity Applications-Konfigurationsdatei (`ism-configuration.properties`) nach der Installation der beiden Komponenten definieren, entweder manuell oder mit dem ConfigUpdate-Dienstprogramm.

Web-Anwendungsserver

Der Anwendungsserver stellt das Laufzeit-Framework zur Verfügung, in dem die Komponenten der Identity Applications ausgeführt werden. Identity Applications sind als WAR-Dateien (Webanwendungsressource oder Webanwendungsarchiv) gepackt. Bei der Installation werden die WAR-Dateien auf dem Anwendungsserver bereitgestellt. Auf dem Anwendungsserver wird die Java Virtual Machine (JVM) ausgeführt. Sie stellt die Laufzeitumgebung für den Anwendungscode zur Verfügung. Die folgenden WAR-Dateien gelten für die URL für eine Komponente der Identity Applications:

- **IDMProv** für die Benutzeranwendungsoberfläche
- **idmdash** für das Dashboard
- **idmadmin** für die Identity Applications-Verwaltungsoberfläche

Wenn ein Benutzer mit `idmdash`- oder `idmadmin`-Anwendungen interagiert, fragen diese Anwendungen die zugrundeliegende Datei `IDMProv.war` ab und rufen die Informationen für den Benutzer ab. `IDMProv.war` stellt die REST- und SOAP-APIs zur Verfügung, wobei `idmdash` und `idmadmin` die Informationen für die Benutzeroberfläche enthalten.

Identity Applications werden auf dem Apache Tomcat-Anwendungsserver ausgeführt, der im Installationskit enthalten ist. Zur Unterstützung des Tomcat-Anwendungsservers installiert das Installationsprogramm die unterstützten Versionen von JRE und Apache ActiveMQ.

Datenbank der Identity Applications

Die Identity Applications-Datenbank enthält Konfigurationsdaten für Identity Applications wie lokalisierte Bezeichnungen, Berechtigungswerte und Email-Serverkonfiguration. In ihr sind auch Workflow-Statusdaten gespeichert, die für die Workflow-Engine erforderlich sind. Für Identity Applications werden die Datenbanken PostgreSQL, Oracle und Microsoft SQL Server unterstützt.

Das Installationsprogramm für Identity Applications installiert automatisch die unterstützte Version der PostgreSQL-Datenbank, die als Standarddatenbank für Identity Applications fungiert. Wenn Sie PostgreSQL nicht als Datenbank nutzen möchten, können Sie eine unterstützte Version der Oracle- oder MS SQL-Datenbank mit Identity Applications konfigurieren. Für Identity Applications ist zur Kommunikation mit der Datenbank ein Java Database Connectivity-Treiber (JDBC-Treiber Typ 4)

erforderlich. Das Installationsprogramm fordert zur Eingabe des Speicherorts und Namens des JDBC-Treibers für die Datenbank auf. Daher müssen Sie diesen JDBC-Treiber von der Datenbank des Installationsverzeichnisses abrufen, bevor Sie die Installation von Identity Applications starten.

- Für die PostgreSQL-Datenbank ist der Treiber im Paket des OpenText Identity Manager-Installationsprogramms enthalten.
- Für die Oracle-Datenbank können Sie den Treiber von der Oracle-Website herunterladen.
- Laden Sie den Treiber für die Microsoft SQL Server-Datenbank von der Microsoft-Website herunter.

Die Datenbank kann sich lokal auf dem Identity Applications-Server oder auf einem Remote-Computer befinden. Wenn Sie eine Remote-Datenbank verwenden, müssen Sie eine Verbindung zur Datenbank konfigurieren.

Treiber für Identity Applications

Für Identity Applications-Komponenten sind die folgenden Treiber erforderlich:

Benutzeranwendungstreiber

Speichert Konfigurationsinformationen und benachrichtigt Identity Applications über Änderungen im Identitätsdepot. Sie können den Treiber so konfigurieren, dass Ereignisse im Identitätsdepot bestimmte Workflows auslösen. Der Treiber kann außerdem der Benutzeranwendung den Erfolg oder das Fehlschlagen der Bereitstellungsaktivität eines Workflows melden, sodass Benutzer den endgültigen Status ihrer Anforderungen sehen können.

Rollen- und Ressourcenservice-Treiber

Er verwaltet alle Rollenzuweisungen, startet Workflows für Rollenzuweisungsanforderungen, die eine Genehmigung erfordern, und verwaltet indirekte Rollenzuweisungen nach Gruppen- und Containermitgliedschaften. Der Treiber erteilt und entzieht Berechtigungen für Benutzer basierend auf ihren Rollenmitgliedschaften und führt Bereinigungsvorgänge für abgeschlossene Anforderungen durch. Der Treiber verwaltet Ressourcenanforderungen zusätzlich zu Rollenanforderungen.

Die Installationsoption **Identity Applications** des Installationsprogramms stellt dem Identitätsdepot den Benutzeranwendungstreiber und den Rollen- und Ressourcenservice-Treiber bereit.

Komponenten von Identity Reporting

(Optional) Installieren Sie diese Komponente nur, wenn Sie die Berichterstellungsfunktion implementieren möchten

Identity Reporting gibt Ihnen einen Gesamtüberblick über die Berechtigungen Ihrer Benutzer sowie Aufschluss darüber, welche Autorisierungen und Berechtigungen den Identitäten in Ihrer Organisation in der Vergangenheit und gegenwärtig erteilt wurden. OpenText Identity Manager stellt vordefinierte Berichte zur Verfügung, mit denen Sie den Status einer OpenText Identity Manager-Umgebung überwachen können, einschließlich der von Identitätsdepots und den verbundenen Systemen erfassten Informationen. Installieren Sie Identity Reporting, das im Lieferumfang von OpenText Identity Manager enthalten ist, um die in OpenText Identity Manager verfügbaren Berichte zu verwenden. Identity Reporting enthält auch ein Werkzeug zum Packen von Berichten,

das den Vorgang der Erstellung benutzerdefinierter Berichte erleichtert. Über die Benutzeroberfläche des Berichterstellungsmoduls können Sie schnell und einfach festlegen, dass die Berichtgenerierung außerhalb der Hauptgeschäftszeit erfolgt und somit die Systemleistung nicht beeinträchtigt wird. Weitere Informationen über Identity Reporting finden Sie im OpenText™ Identity Manager CE 24.4 (v4.10) – Administratorhandbuch zu Identity Reporting.

HINWEIS: Vor der Installation von Identity Reporting in einer Advanced Edition müssen Sie Identity Applications installieren.

Eine Identity Reporting-Installation setzt sich aus den folgenden Komponenten zusammen:

Identity Reporting

Browserbasierte Anwendung, die durch Aufrufen des Berichterstellungsservice Berichte generiert. Der Berichterstellungsservice ruft die zum Generieren von Berichten erforderlichen Daten vom Identity Reporting-Repository (Identity Information Warehouse) ab. Es enthält alle Information zur Berichtverwaltung (wie Berichtdefinitionen und -zeitpläne), Datenbankansichten und für die Berichterstellung erforderliche Konfigurationsinformationen.

Authentifizierungsservice

Der Authentifizierungsservice wird von der OSP-Komponente bereitgestellt. Weitere Informationen finden Sie unter „Authentifizierungsservice“, auf Seite 19.

HINWEIS: OSP wird automatisch mit Identity Reporting installiert. In einer Installation einer Advanced Edition kann Identity Reporting jedoch den mit Identity Applications installierten Authentifizierungsservice nutzen. Wenn Sie denselben Authentifizierungsservice nutzen, müssen Sie bei der Konfiguration von Identity Reporting die Authentifizierungseinstellungen angeben.

Self-Service Password Reset

Der Self-Service-Passwortverwaltungsservice ermöglicht den Zugriff auf die Self-Service-Passwortverwaltung. Weitere Informationen finden Sie unter „Self-Service Password Reset“, auf Seite 20.

Identity Reporting-Datenbank

Die Identity Reporting-Datenbank (Identity Information Warehouse) speichert Informationen über den tatsächlichen und gewünschten Zustand des Identitätsdepots und der verbundenen Systeme in Ihrer Organisation. Sie können aus diesen Informationen Berichte generieren, um die Beziehung zwischen Objekten, wie Benutzer und Rollen, anzuzeigen. Die Datenbank kann sich lokal auf dem Identity Reporting-Server oder auf einem Remote-Computer befinden. OpenText Identity Manager verwendet Datenquellen für die Verbindung zur Datenbank. Für Identity Reporting ist zur Kommunikation mit der Datenbank ein Java Database Connectivity-Treiber (JDBC-Treiber Typ 4)

erforderlich. Ein JDBC-Treiber ermöglicht einem Identity Reporting-Server die Kommunikation mit der Datenquelle. Für Identity Reporting werden die Datenbanken PostgreSQL, Oracle und Microsoft SQL unterstützt.

- Für die PostgreSQL-Datenbank ist der Treiber im Paket des OpenText Identity Manager-Installationsprogramms enthalten.
- Für die Oracle-Datenbank können Sie den Treiber von der Oracle-Website herunterladen.
- Laden Sie den Treiber für die Microsoft SQL Server-Datenbank von der Microsoft-Website herunter.

HINWEIS: Vor der Installation der Identity Reporting-Komponenten muss der OpenText Identity Manager Server installiert sein.

Web-Anwendungsserver

Der Anwendungsserver stellt das Laufzeit-Framework zur Verfügung, in dem die Komponenten für Identity Reporting ausgeführt werden. Die folgenden WAR-Dateien gelten für die URL für eine Komponente von Identity Reporting:

- **IDMRPT** für die Identity Reporting-Anwendung/Oberfläche
- **idmdcs** für den OpenText Identity Manager-Datenerfassungsdienst

Wenn ein Benutzer mit `IDMRPT`- oder `idmdcs`-Anwendungen interagiert, fragen diese Anwendungen den Berichterstellungsservice ab und rufen die Informationen für den Benutzer ab. Der Berichterstellungsservice stellt die REST-APIs zur Verfügung, wobei `IDMRPT` und `idmdcs` die Informationen für die Benutzeroberfläche enthalten.

Weitere Informationen zum Web-Anwendungsserver finden Sie im „Web-Anwendungsserver“, auf Seite 20.

Treiber für Identity Reporting

Für die Identity Reporting-Komponenten sind die folgenden Treiber erforderlich:

Managed System Gateway-Treiber

Fragt das Identitätsdepot ab, um die folgende Art von Informationen von verwalteten Systemen zu erfassen:

- Liste aller verwalteten Systeme
- Liste mit allen Konten für die verwalteten Systeme
- Berechtigungstypen, Werte und Zuweisungen sowie Benutzerkontenprofile für die verwalteten Systeme

Datenerfassungsdiensttreiber

Der Datenerfassungsdienst erfasst mithilfe des DCS-Treibers Änderungen an Objekten, die in einem Identitätsdepot gespeichert sind, z. B. Konten, Rolle, Ressourcen, Gruppen und Teammitgliedschaften. Der Treiber registriert sich beim Dienst und gibt Änderungsereignisse (z. B. Datensynchronisierung sowie Hinzufügungs-, Änderungs- und Löschungsereignisse) an den Dienst weiter.

Der Dienst ist in drei Unterdienste unterteilt:

- **Berichtdatensammler:** Verwendet ein Pull-Modell zum Abrufen von Daten aus einer oder mehreren Identitätsdepot-Datenquellen. Die Sammlung der Daten wird regelmäßig auf Grundlage der festgelegten Konfigurationsparameter durchgeführt. Der Sammler ruft zum Abrufen der Daten den Managed System Gateway-Treiber (MSGW-Treiber) auf.
- **Ereignisgesteuerter Datensammler:** Verwendet ein Push-Modell zum Sammeln von Ereignisdaten, die vom Datenerfassungsdiensttreiber erfasst wurden.
- **Datensammler für nicht verwaltete Anwendungen:** Ruft Daten von einer oder mehreren nicht verwalteten Anwendungen ab, indem er einen speziell für jede Anwendung geschriebenen REST-Endpunkt aufruft. Nicht verwaltete Anwendungen sind Anwendungen in Ihrem Unternehmen, die nicht mit dem Identitätsdepot verbunden sind.

Die **Identity Reporting**-Installationsoption des Installationsvorgangs stellt dem Identitätsdepot den MSGW-Treiber und den Datenerfassungsdiensttreiber bereit.

Sentinel for Log Management für Identity Governance and Administration

Sentinel Log Management für Identity Governance and Administration (IGA) ist ein Sicherheitsinformations- und Ereignisverwaltungssystem (SIEM-System), das Informationen aus vielen Quellen in einem Unternehmen erhält. Es standardisiert diese Informationen, setzt Prioritäten und stellt Ihnen diese Informationen zur Verfügung, damit Sie Entscheidungen hinsichtlich Bedrohungen, Risiken und Richtlinien treffen können. Sentinel Log Management für IGA erfasst Protokollereignisse, die mit Aktionen verknüpft sind, die in verschiedenen OpenText-Produkten durchgeführt werden. Dazu zählen Identity Reporting, Identity Applications und das Identitätsdepot. Diese Ereignisse werden im öffentlichen Schema im Identity Reporting-Repository (Identity Information Warehouse) gespeichert.

OpenText Identity Manager stellt für Sentinel Log Management für IGA ein separates Installationsprogramm (`SentinelLogManagementForIGA8.7.0.0.tar.gz`) zur Verfügung.

OpenText Identity Manager-Werkzeuge

Erforderlich für alle Installationen

OpenText Identity Manager enthält eine Reihe von Verwaltungswerkzeugen, die die Implementierung, Anpassung und Pflege der Lösung erleichtern. Einige dieser Werkzeuge werden mit OpenText Identity Manager installiert, einige müssen separat installiert werden.

Designer für OpenText Identity Manager

Designer für OpenText Identity Manager (Designer) hilft beim Konzipieren, Testen, Dokumentieren und Bereitstellen von OpenText Identity Manager-Lösungen in einer Netzwerk- oder Testumgebung. Sie können das OpenText Identity Manager-System zunächst in einer Offline-Umgebung erstellen und konfigurieren und später dann in das Live-System übertragen. Beim Gestalten hilft Designer wie folgt:

- Alle Komponenten in der OpenText Identity Manager-Lösung werden grafisch dargestellt, und ihre Zusammenarbeit wird überwacht.
- Ändern und testen Sie Ihre OpenText Identity Manager-Umgebung, damit ihre Funktionsfähigkeit gewährleistet ist, wenn Sie die Testlösung ganz oder teilweise in der Produktionsumgebung bereitstellen.

Mithilfe von Designer behalten Sie den Überblick über Ihre Design- und Layoutdaten. Per Mausklick können Sie diese Daten in verschiedenen Formaten ausgeben. Mit Designer sind Teams außerdem in der Lage, gemeinsam an unternehmensweiten Projekten zu arbeiten.

OpenText Identity Manager enthält ein separates Installationsprogramm für Designer.

Analyzer für OpenText Identity Manager

Analyzer für OpenText Identity Manager ermöglicht die Analyse, die Bereinigung, den Abgleich und die Berichterstellung für Daten gemäß den internen Datenqualitätsrichtlinien. Mit Analyzer können Sie alle Datenspeicher des Unternehmens analysieren, verbessern und kontrollieren. Analyzer umfasst die folgenden Funktionen:

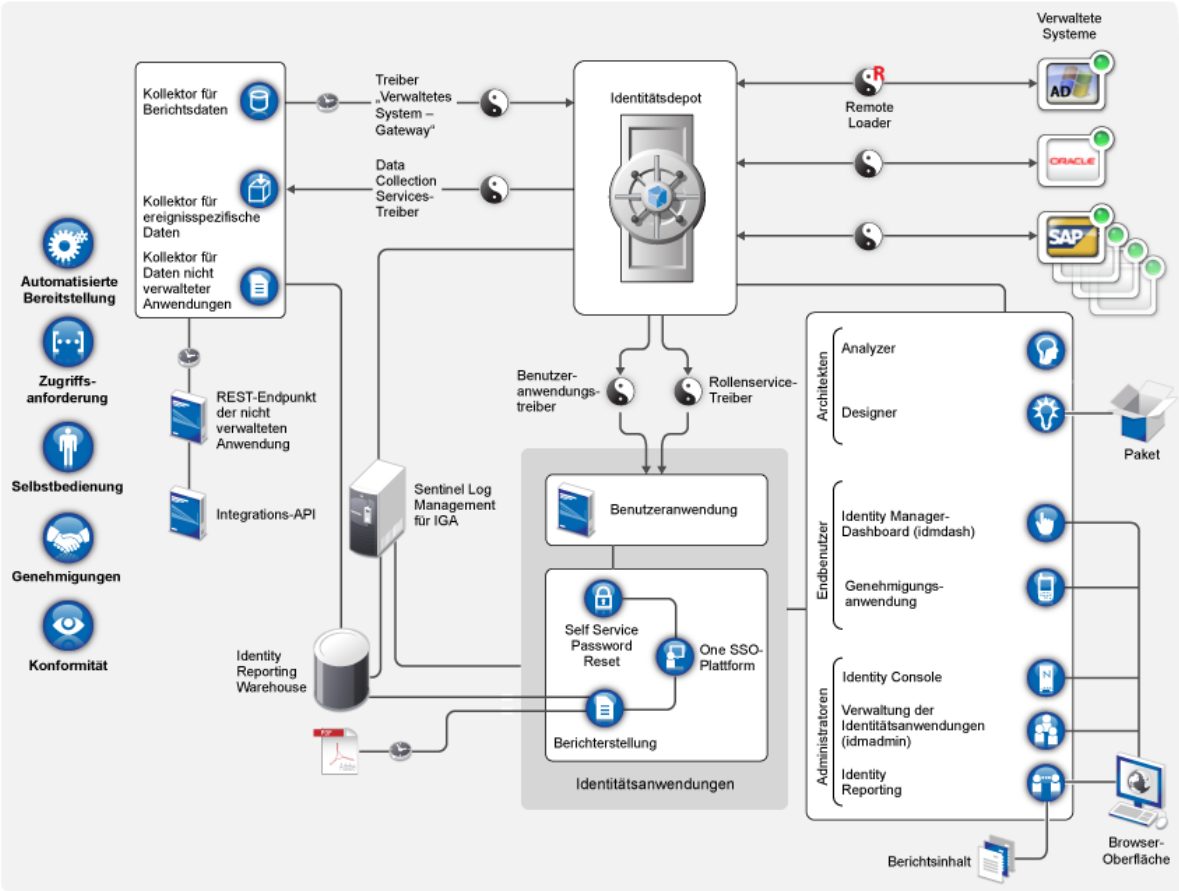
- Die Analyzer-Schemazuordnung weist die Schemaattribute einer Anwendung den entsprechenden Schemaattributen im Basisschema von Analyzer zu. Damit ist gewährleistet, dass ähnliche Werte in den verschiedenartigen Systemen beim Analysieren und Bereinigen der Daten fehlerfrei in Verbindung gebracht werden. Hierzu greift Analyzer auf die Schemazuordnungsfunktionen in Designer zurück.
- Im Analyseprofil-Editor konfigurieren Sie ein Profil, mit dem eine oder mehrere Datengruppeninstanzen analysiert werden. Die einzelnen Analyseprofile enthalten jeweils mindestens eine Metrik zur Bewertung der Attributwerte, wodurch festgestellt wird, inwieweit die Daten den definierten Datenformatstandards entsprechen.
- Im Übereinstimmungsprofil-Editor vergleichen Sie Werte in einer oder mehreren Datengruppen. Hierbei können Sie nach doppelten Werten innerhalb einer Datengruppe sowie nach übereinstimmenden Werten in zwei verschiedenen Datengruppen suchen.

OpenText Identity Manager stellt ein separates Installationsprogramm für Analyzer zur Verfügung.

WICHTIG: Das Analyzer-Tool ist nicht in der ISO für OpenText Identity Manager 4.10 enthalten. Wenn Analyzer bereits installiert ist, aktualisieren Sie ihn auf Version 4.8.5 und verwenden Sie ihn mit OpenText Identity Manager 4.10.

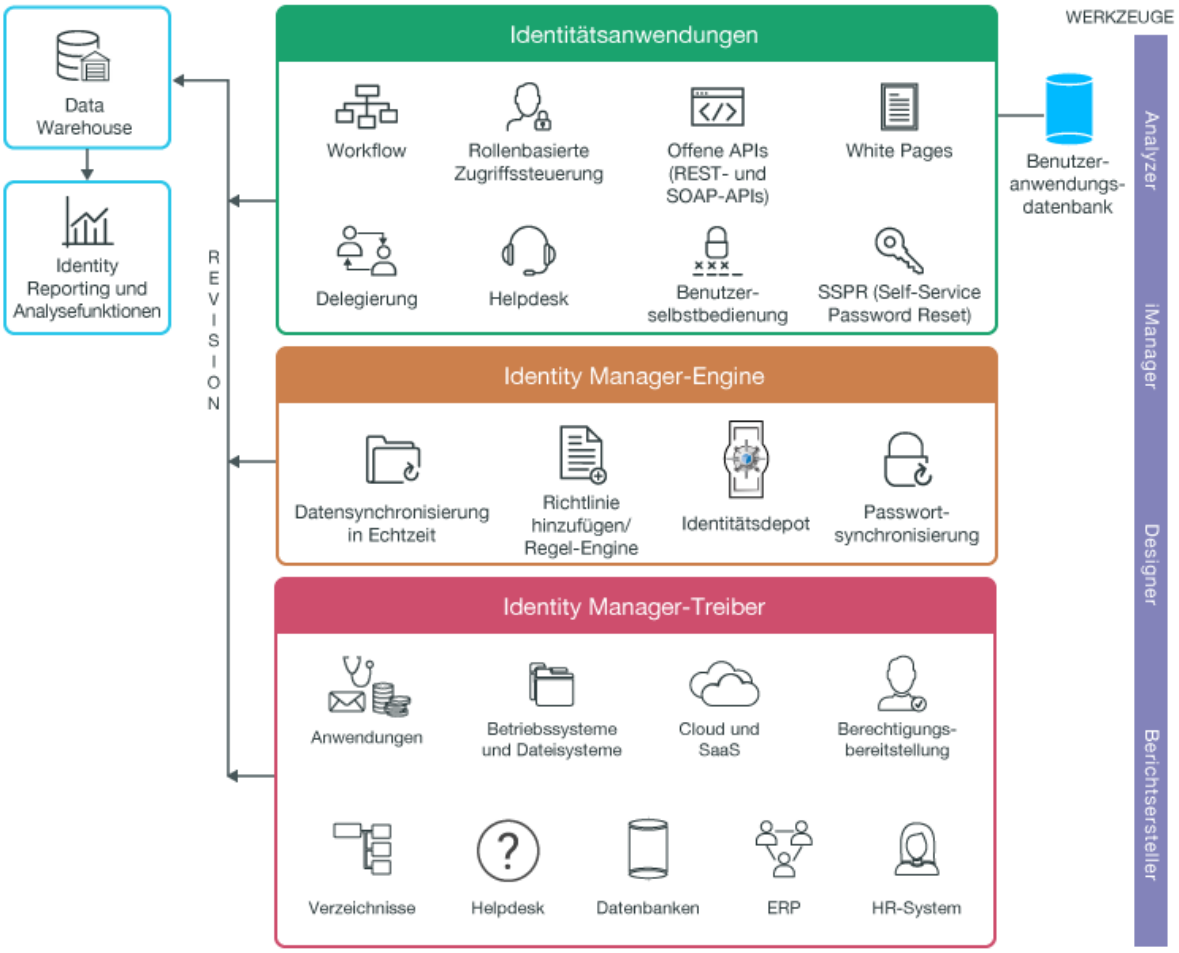
Wenn Sie den Zweck der verschiedenen OpenText Identity Manager-Komponenten und die Methoden zu deren Installation verstanden haben, sehen Sie sich Abbildung 1-3 an, um zu verstehen, wie die Komponenten miteinander interagieren.

Abbildung 1-3 *Interaktion zwischen OpenText Identity Manager-Komponenten*



Funktionelle Architektur

Die folgende Darstellung veranschaulicht die grundlegende funktionelle Architektur für OpenText Identity Manager-Komponenten. In dieser Darstellung sind nicht alle möglichen Integrationen abgedeckt.



Informationen über mögliche Bereitstellungsszenarien finden Sie unter Bereitstellungsoptionen für OpenText Identity Manager.

Bereitstellungsoptionen für OpenText Identity Manager

In der folgenden Tabelle erhalten Sie Informationen zur Planung der physischen Umgebung für Ihre Identity Management-Lösung. Diese Bereitstellungsanwendungsfälle geben Ihnen einen Überblick über die physische Architektur des Identity Management. Sie erfahren, wie die Komponentenprodukte verbunden sind und untereinander sowie mit anderen Produkten kommunizieren. Einen ersten Überblick über die funktionelle Architektur und die Komponenten von Identity Management finden Sie unter „Funktionelle Architektur“, auf Seite 26.

Bereitstellungsoption	Zusammenfassung
Einzelserverkonfiguration auf einem Computer	Die einfachste Bereitstellungskonfiguration umfasst den OpenText Identity Manager Server und andere erforderliche Anwendungen auf einem Computer. Sie müssen sicherstellen, dass der Computer über den Arbeitsspeicher, die Geschwindigkeit und den verfügbaren Festplattenspeicherplatz verfügt, die für den Workload erforderlich sind. Es handelt sich hierbei um einen einfachen Bereitstellungsanwendungsfall. Er eignet sich weitgehend nur für einen Proof of Concept (POC) und zu Demonstrationszwecken. Für eine Produktionsumgebung ist er möglicherweise nicht geeignet.
Verteilte Serverkonfiguration	Bei dieser Bereitstellung befindet sich der OpenText Identity Manager Server auf einem Computer und alle anderen erforderlichen Anwendungen auf einem oder mehreren weiteren Computern. Beispielsweise können Komponenten wie Identity Applications, OSP und SSPR auf einem separaten Computer ausgeführt werden. Ein weiterer Computer kann zum Hosten der Komponenten für den Berichterstellungsservice vorgesehen werden, um die Systemanforderungen zur Ausführung der Komponente Sentinel Log Management für IGA zu erfüllen.
Hochverfügbarkeits-Bereitstellung	Hochverfügbarkeit ist ein Redundanzvorgang, der automatisch zu einem Standby-Server umschaltet, wenn der Primärserver ausfällt oder vorübergehend für Wartungszwecke heruntergefahren wurde. OpenText Identity Manager unterstützt die Installation der folgenden Komponenten in einer Hochverfügbarkeitsumgebung: ◆ Identitätsdepot ◆ OpenText Identity Manager-Engine ◆ Remote Loader ◆ Identity Applications mit Ausnahme von Identity Reporting Eine typische Clusterkonfiguration umfasst Tomcat-Anwendungsserver-Knoten, auf denen Identity Applications für Lastausgleich und Fehlertoleranz gehostet wird. Die gesamte Kommunikation wird über das Lastausgleichprogramm weitergeleitet. Alle Knoten kommunizieren mit derselben Instanz des Identitätsdepots und der Identity Applications-Datenbank. Diese Konfiguration ist skalierbar.

Beispiele für OpenText Identity Manager-Bereitstellungen

Mit OpenText Identity Manager steuern Sie die Benutzeridentitäten und deren Zugriff auf Anwendungen und Konten auf verbundenen Systemen. Wählen Sie die zu installierende OpenText Identity Manager-Edition entsprechend der benötigten Funktion aus. Diese bestimmt dann die zu installierenden Komponenten. In der folgenden Tabelle sind die Funktionen der OpenText Identity Manager Advanced Edition und der OpenText Identity Manager Standard Edition aufgeführt.

Funktion	Advanced Edition	Standard Edition	Zu installierende Komponenten
Automatische regelbasierte Benutzerbereitstellung	✓	✓	OpenText Identity Manager-Engine und Designer
Identitätssynchronisierung in Echtzeit	✓	✓	OpenText Identity Manager-Engine und Designer
Passwortverwaltung und Passwortselbstbedienung	✓	✓	OpenText Identity Manager-Engine und SSPR
Einheitliches Identitätsinformations-Tool (Analyzer)	✓	✓	Analyzer
REST APIs und Single Sign-on-Support	✓	✓ (nur eingeschränkte Unterstützung)	OpenText Identity Manager-Engine, OSP und Identity Reporting
Berichterstellung über den aktuellen Zustand	✓	✓	OpenText Identity Manager-Engine und Identity Reporting
Rollenbasierte unternehmensgerechte Bereitstellung	✓	✗	OpenText Identity Manager-Engine und Identity Applications
Automatische Genehmigungs-Workflows für die Durchsetzung von Geschäftsrichtlinien	✓	✗	OpenText Identity Manager-Engine, Designer und Identity Applications
Erweiterte Selbstbedienung in den Identity Applications	✓	✗	OpenText Identity Manager-Engine und Identity Applications
Ressourcenmodell und Katalog für die einfache Ressourcenbereitstellung	✓	✗	OpenText Identity Manager-Engine und Identity Applications
Berichterstellung über den Zustandsverlauf	✓	✗	OpenText Identity Manager-Engine und Identity Reporting
Berichterstellung über verbundene Systeme	✓	✗	OpenText Identity Manager-Engine und Identity Reporting
Rollen- und Ressourcenverwaltung	✓	✗	OpenText Identity Manager-Engine und Identity Applications

HINWEIS: In allen OpenText Identity Manager-Installationen ist der OpenText Identity Manager Server die zentrale Komponente. Abhängig von der OpenText Identity Manager-Edition wird auf einem Tomcat-Anwendungsserver nur Identity Reporting installiert bzw. sowohl Identity Reporting als auch Identity Applications. Installieren Sie nach Bedarf andere Komponenten mit dem für die OpenText Identity Manager-Komponenten spezifischen Installationsprogramm. Installieren Sie beispielsweise Designer, Analyzer oder Sentinel Log Management für IGA.

Prüfen Sie vor der Installation von OpenText Identity Manager zudem die Ziele für Ihre Implementierung und achten sie auf die Optionen für die physische Topologie, wie Hochverfügbarkeit und Skalierbarkeit. Dadurch ermitteln Sie die Konfiguration, die zu den Anforderungen Ihrer Organisation passt.

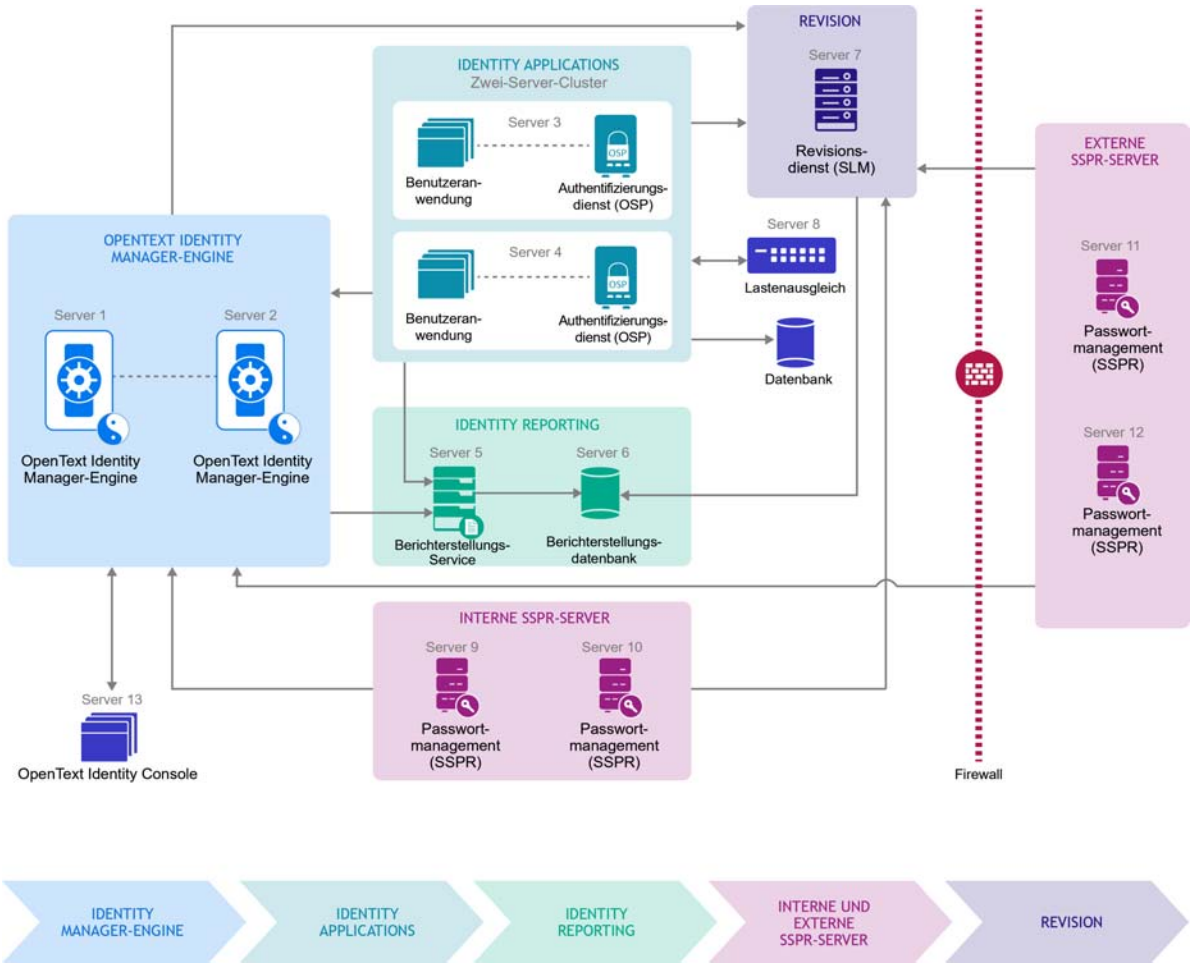
Durch die Hochverfügbarkeit lassen sich wichtige Netzwerkressourcen wie Daten, Anwendungen und Dienste effizient verwalten. Hochverfügbarkeit wird durch Reduzierung der einzelnen Fehlerquellen und Nutzung redundanter Komponenten implementiert. Auf ähnliche Weise lässt sich durch die Verbindung mehrerer Instanzen von Identity Management-Komponenten mit einem Lastausgleichprogramm eine Hochverfügbarkeitsumgebung bereitstellen.

In diesem Abschnitt werden zwei Beispiele beschrieben, die die Implementierung der Advanced Edition und Standard Edition auf hohem Niveau beschreibt. Sie dienen Ihnen als Referenz für die Erstellung eines Bereitstellungsdiagramms für Ihre Implementierung.

Beispiel für die Bereitstellung einer Advanced Edition

Abbildung 1-4 zeigt eine anspruchsvolle Bereitstellungstopologie einer Installation der OpenText Identity Manager Advanced Edition.

Abbildung 1-4 *Beispiel für die Bereitstellung einer Advanced Edition*



- Die Komponenten des OpenText Identity Manager Servers, sein zugrundeliegendes Repository (Identitätsdepot) und die webfähigen Komponenten (Identity Applications und Identity Reporting) werden in der Intranetzone installiert. Das Lastausgleichprogramm leitet dann den Datenverkehr an die Komponenten von Identity Applications weiter. Diese Bereitstellung schafft mehr Sicherheit, weil diese Komponenten durch Firewalls vom Intranet-Datenverkehr getrennt sind.
- Die Komponenten des OpenText Identity Manager Servers werden zur Verwendung einer Zwei-Server-Konfiguration (Primär- und Sekundärserver) konfiguriert. Eine virtuelle logische IP-Adresse ist auf dem Primärserver aktiv. Er fungiert als (aktiver) Primärknoten, ein weiterer Server als Sekundärknoten. Fällt der Primärserver aus, wird die logische IP-Adresse an den Sekundärserver verschoben. Alle Prozesse werden dann am Sekundärserver gestartet. Die Anwendungsvorgänge für den Zugriff auf den Sekundärserver erfahren möglicherweise einen vorübergehenden Serviceausfall, wenn die logische IP-Adresse verschoben wird. Alle anderen Vorgänge werden gestartet. Alle Komponenten nutzen zu jedem Zeitpunkt denselben Identitätsdepot-Server.
- SSPR-Services sind innerhalb und außerhalb der Firewall für die Passwortverwaltungsanforderungen lokaler und mobiler Benutzer der Organisation verfügbar. Die innerhalb der Firewall installierten Services sind für die lokalen Passwortverwaltungsanforderungen zuständig. Falls sie das Passwort vergessen, können mobile

Mitarbeiter nicht mehr auf das VPN zugreifen und daher auch nicht mehr auf die intern vorhandenen SSPR-Services. Sie können zur Verwaltung ihrer Passwörter direkt auf die SSPR-Services zugreifen, die sich außerhalb der Firewall befinden.

- Die Benutzeranwendung und der Authentifizierungsservice (OSP) werden in einem Cluster bereitgestellt. Sie unterstützen den Ausfallsicherungsvorgang (Failover) für Identity Applications. Die Clusterknoten werden der Identity Applications-Datenbank hinzugefügt, die auf einem separaten Computer installiert ist. Mit dieser Bereitstellung können Sie dem Cluster weitere Knoten hinzufügen. Die Clusterkonfiguration wird sofort an die neu hinzugefügten Knoten gesendet. Das Lastausgleichprogramm ist normalerweise Teil des Clusters. Es versteht sowohl die Clusterkonfiguration als auch die Failover-Richtlinien. In dieser Konfiguration ist immer nur ein Clusterknoten aktiv, während sich die verbleibenden Knoten im passiven oder Standby-Modus befinden. Wenn ein Knoten ausfällt, werden die Anforderungen an diesen Knoten an die noch aktiven Knoten im Cluster verteilt. Da diese Installation eine interne, hochverfügbare Lösung ist, schützt sie vor Ausfällen der lokalen Hardware und Software. Sie nutzt einen hardwarebasierten Cluster aus zwei Knoten, um Hochverfügbarkeit für Identity Applications-Komponenten zu erzielen.

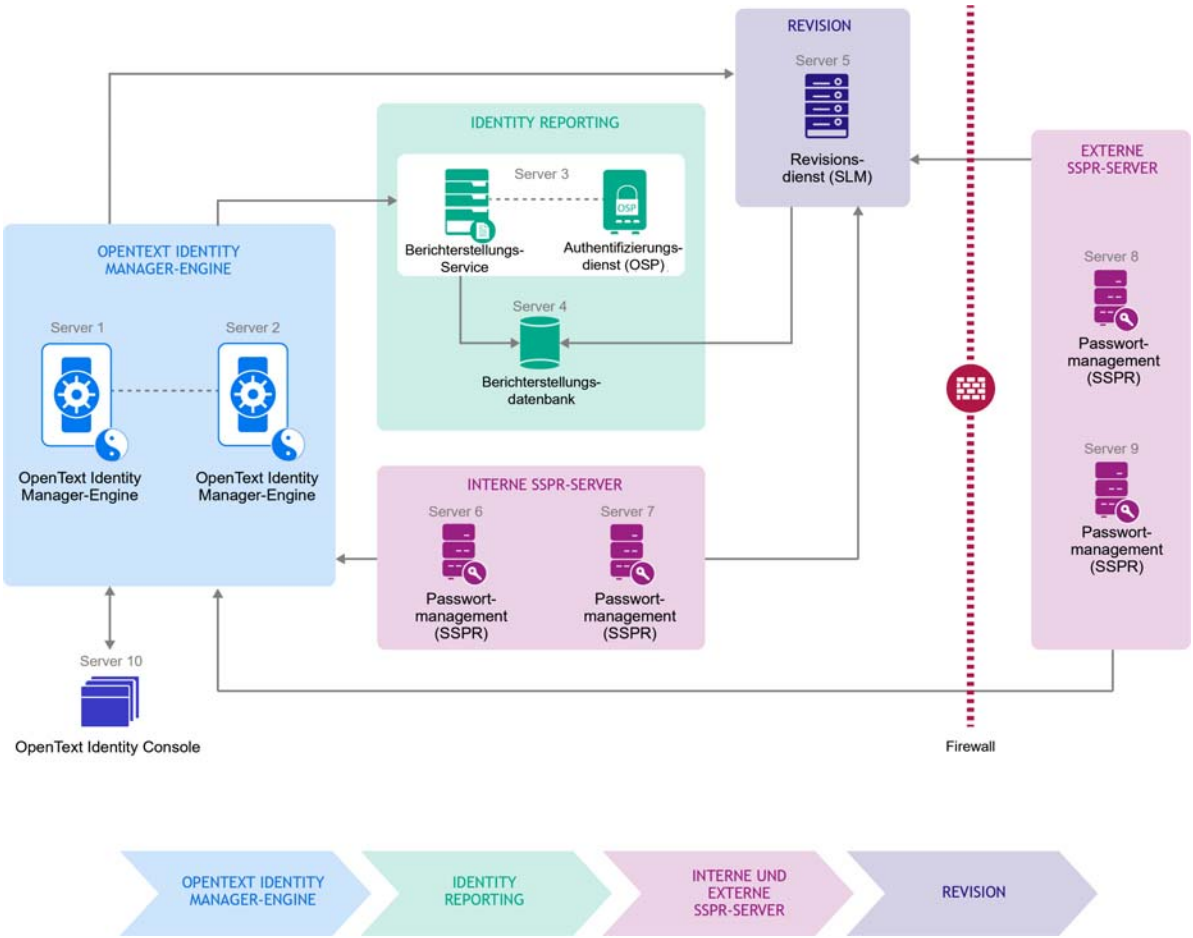
Wir haben diese Konfiguration getestet und empfehlen sie.

HINWEIS: OpenText Identity Manager unterstützt kein Clustering der Identity Reporting-Komponenten.

Beispiel für die Bereitstellung einer Standard Edition

In Produktionsbereitstellungen spezifizieren die Sicherheitsrichtlinien möglicherweise, dass der Authentifizierungsservice für erweiterte Authentifizierung und Schutz Ihrer Umgebung nicht dem öffentlichen Netzwerk gezeigt werden darf. Abbildung 1-5 zeigt eine anspruchsvolle Bereitstellungstopologie einer Installation der OpenText Identity Manager Standard Edition.

Abbildung 1-5 *Beispiel für die Bereitstellung einer Standard Edition*



- Die Komponenten des OpenText Identity Manager Servers, sein zugrundeliegendes Repository (Identitätsdepot) und die Identity Reporting-Komponenten werden in der Intranetzone installiert. Der Internetdatenverkehr wird über die Webserver an die Identity Reporting-Komponenten geroutet, die für zusätzlichen Schutz hinter der Firewall installiert sind. Diese Bereitstellung schafft mehr Sicherheit, weil diese Komponenten durch Firewalls vom Intranet-Datenverkehr getrennt sind.
- Die Komponenten des OpenText Identity Manager Servers werden zur Verwendung einer Zwei-Server-Konfiguration (Primär- und Sekundärserver) konfiguriert. Eine virtuelle logische IP-Adresse ist auf dem Primärserver aktiv. Er fungiert als (aktiver) Knoten, ein weiterer Server als Sekundärknoten. Fällt der Primärserver aus, wird die logische IP-Adresse an den Sekundärserver verschoben. Alle Prozesse werden dann am Sekundärserver gestartet. Die Anwendungsvorgänge für den Zugriff auf den Sekundärserver erfahren möglicherweise einen vorübergehenden Serviceausfall, wenn die logische IP-Adresse verschoben wird. Alle anderen Vorgänge werden gestartet. Alle Komponenten nutzen zu jedem Zeitpunkt denselben Identitätsdepot-Server.
- SSPR-Services sind innerhalb und außerhalb der Firewall für die Passwortverwaltungsanforderungen lokaler und mobiler Benutzer der Organisation verfügbar. Die innerhalb der Firewall installierten Services sind für die lokalen Passwortverwaltungsanforderungen zuständig. Falls sie das Passwort vergessen, können mobile

Mitarbeiter nicht mehr auf das VPN zugreifen und daher auch nicht mehr auf die intern vorhandenen SSPR-Services. Sie können zur Verwaltung ihrer Passwörter direkt auf die SSPR-Services zugreifen, die sich außerhalb der Firewall befinden.

Wir haben diese Konfiguration getestet und empfehlen sie.

HINWEIS: OpenText Identity Manager unterstützt kein Clustering der Identity Reporting-Komponenten.

II Planen der Installation von OpenText Identity Manager

Die Planung Ihrer OpenText Identity Manager-Implementierung hängt davon ab, wie OpenText Identity Manager die Benutzer verwalten soll und welche Funktionen Sie benötigen, um Ihre Geschäftsziele zu erreichen. Denken Sie über folgende Fragen nach, die Ihnen bei der Entscheidungsfindung helfen:

- Wie verwalte ich Identitäten?
- Ist eine automatische Bereitstellung erforderlich?
- Welche Geschäftsanforderungen sollte ich mit dem Workflow implementieren?

Ihre Entscheidungen sollen die beste Methode zur Implementierung von OpenText Identity Manager für Ihre Anforderungen darstellen.

Vor der Bereitstellung von OpenText Identity Manager in einem großen Unternehmen müssen zusätzliche Aufgaben geplant werden. Weitere Informationen finden Sie im Abschnitt Planung im *Überblick und Planungshandbuch zu OpenText™ Identity Manager CE 24.4 (v4.10)*.

2 Planen der Installation

In der folgenden Tabelle sind die Komponenten aufgeführt, die zur Unterstützung der zu implementierenden Funktionen installiert werden müssen. Im Abschnitt "Installation" finden Sie Anweisungen zur Installation dieser Komponenten.

Funktionalität	Zu installierende Komponente
Verwalten der Benutzeridentitäten in einem Unternehmensverzeichnis	OpenText Identity Manager Server
Bereitstellung von Konten in verbundenen Systemen	OpenText Identity Manager Server
	Identity Applications
	Benutzeranwendungstreiber
	Rollen- und Ressourcenservice-Treiber
	Designer
	HINWEIS: Anweisungen zur Installation der OpenText Identity Manager-Treiber finden Sie im Treiberimplementierungshandbuch für den zu installierenden Treibertyp auf der Website Dokumentation zu den OpenText Identity Manager-Treibern (https://www.netiq.com/documentation/identity-manager-4.10-drivers/).
Authentifizierung	OpenText Identity Manager Server
	One Single Sign-On Provider (OSP)
Passwortverwaltung	OpenText Identity Manager Server
	Self-Service-Passwortverwaltung
Generieren von Berichten zu OpenText Identity Manager-Aktivitäten	OpenText Identity Manager Server
	Identity Reporting
	One Single Sign-On Provider (OSP)

Festlegen der Hardwareanforderungen

Die für Ihre OpenText Identity Manager-Installation erforderliche Hardware wird durch zwei Faktoren bestimmt:

- Die zu implementierenden Funktionen
- Den Umfang Ihrer Bereitstellung

Die folgenden Bereitstellungstypen können Ihnen dabei helfen, den Umfang der Bereitstellung abzuschätzen.

Bereitstellungstyp	Hardwareanforderungen
Proof of Concept (Demonstration)	Eine Einzelserverbereitstellung für Demonstrationszwecke oder Basistests in einer Entwicklungsumgebung.
Einfaches Beispiel	Eine Implementierung mit mehreren Servern, die sich für kleine bis mittelgroße Implementierungen eignet. Für diese Art von Implementierung ist ein Server zur Ausführung des OpenText Identity Manager Servers und dessen Komponenten erforderlich sowie zwei weitere Server zur Ausführung der Identity Applications- und Identity Reporting-Komponenten.
Zwischenstation	Eine Hochverfügbarkeitsimplementierung, die sich für Implementierungen mittleren Umfangs eignet.
Große Unternehmen	Eine Hochverfügbarkeitsimplementierung mit einem OpenText Identity Manager-Engine-Cluster für die Ausfallsicherung (Failover) sowie einen weiteren Cluster für Identity Applications und den Authentifizierungsservice zur Unterstützung des Single Sign-on-Zugriffs (OSP unter Windows) und Fehlertoleranz.

Arbeitsblatt zur Bereitstellungsplanung

Die Informationen in diesem Thema helfen Ihnen, die Details der neuen Implementierung von OpenText Identity Manager zu verstehen.

Tabelle 2-1 *Arbeitsblatt zur Planung*

Planungsaktivität	Arbeitsblatt
Entwickeln Sie Ihre Bereitstellungsarchitektur. Führen Sie die Anzahl der physischen Computer/Server auf sowie die anderen Systeme, die Sie zur Unterstützung Ihrer Umgebung benötigen.	Arbeitsblatt zur Architektur
Stellen Sie sicher, dass Ihr System die Systemanforderungen erfüllt.	Arbeitsblatt zu den Systemanforderungen
Prüfen Sie die Netzwerkports, um herauszufinden, ob die Standardports einen Konflikt mit den verwendeten Ports verursachen.	Überprüfen der Ports für die OpenText Identity Manager-Komponenten

Arbeitsblatt zur Architektur

Wählen Sie nach Ermittlung des Bereitstellungsumfangs die entsprechende Bereitstellung aus und geben Sie die Anzahl der physischen Computer/Server an, die zur Unterstützung der Bereitstellung erforderlich sind.

Tabelle 2-2 *Arbeitsblatt zur Architektur*

Bereitstellungsanwendungsfall
Failover-Bereitstellung für OpenText Identity Manager Server mit allen Treibern
Anzahl der laufenden Treiber
Hochverfügbarkeitsbereitstellung mit Identity Applications

Arbeitsblatt zu den Systemanforderungen

Informationen über empfohlene Hardware, unterstützte Betriebssysteme und unterstützte virtuelle Umgebungen finden Sie im Dokument Systemanforderungen für OpenText™ Identity Manager CE 24.4 (v4.10).

Informationen zu den Systemanforderungen für eine bestimmte Version finden Sie in den jeweiligen Versionshinweisen, zu finden auf der Website für die OpenText Identity Manager-Dokumentation (https://www.netiq.com/documentation/identity-manager-4.10/). Eine OpenText Identity Manager-Implementierung kann je nach den Anforderungen Ihrer IT-Umgebung variieren. Daher sollten Sie vor Abschluss der OpenText Identity Manager-Architektur für Ihre Umgebung die Consulting Services oder einen OpenText Identity Manager-Partner kontaktieren.

Überprüfen der Ports für die OpenText Identity Manager-Komponenten

OpenText Identity Manager-Komponenten nutzen verschiedene Ports für die ordnungsgemäße Kommunikation der OpenText Identity Manager-Komponenten untereinander.

HINWEIS: Wenn ein Standardport bereits verwendet wird, muss ein anderer Port für die entsprechende OpenText Identity Manager-Komponente angegeben werden.

Anschlussnummer	**Komponente**	**Verwendung durch den Port**
389	Identitätsdepot	Für die LDAP-Kommunikation in Klartext mit OpenText Identity Manager-Komponenten
465	Identity Reporting	Für die Kommunikation mit dem SMTP-Mailserver
524	Identitätsdepot	Für die Kommunikation mit dem NetWare-Kernprotokoll (NCP)

Anschlussnummer	Komponente	Verwendung durch den Port
636	Identitätsdepot	Für die LDAP-TLS/SSL-Kommunikation mit OpenText Identity Manager-Komponenten
5432	Identity Applications	Für die Kommunikation mit der Datenbank der Identity Applications
7707	Identity Reporting	Wird vom Treiber des Gateways im verwalteten System für die Kommunikation mit dem Identitätsdepot verwendet
8000	Remote Loader	Wird von der Treiberinstanz für die TCP/IP-Kommunikation verwendet **HINWEIS:** Jeder Instanz des Remote Loader muss ein eindeutiger Port zugewiesen werden.
8005	Identity Applications	Wird von Tomcat für den Empfang von Befehlen zum Herunterfahren verwendet
8009	Identity Applications	Wird von Tomcat für die Kommunikation mit einem Web-Connector über das AJP-Protokoll anstatt über HTTP verwendet
8028	Identitätsdepot	Für die HTTP-Kommunikation in Klartext mit der NCP-Kommunikation
8030	Identitätsdepot	Für die HTTPs-Kommunikation mit der NCP-Kommunikation
8080	Identity Applications	Wird von Tomcat für die HTTP-Klartextkommunikation verwendet
8090	Remote Loader	Wird vom Remote Loader zum Empfangen von TCP/IP-Verbindungen mit dem Remote-Schnittstellenmodul verwendet **HINWEIS:** Jeder Instanz des Remote Loader muss ein eindeutiger Port zugewiesen werden.
8109	Identity Applications	Nur bei Verwendung der integrierten Installation Wird von Tomcat für die Kommunikation mit einem Web-Connector über das AJP-Protokoll anstatt über HTTP verwendet
8180	Identity Applications	Wird vom Tomcat-Anwendungsserver, auf dem Identity Applications ausgeführt werden, für die HTTP-Kommunikation verwendet
8443	Identity Applications	Wird von Tomcat für die HTTPS-Kommunikation (SSL-Kommunikation) oder zum Umleiten von Anforderungen für die SSL-Kommunikation verwendet
8543	Identity Applications	*Standardmäßig keine Überwachung* Wird von Tomcat zum Umleiten von Anforderungen verwendet, für die der SSL-Transport erforderlich ist, wenn Sie das TLS/SSL-Protokoll nicht nutzen
5432	Identity Reporting	Wird für PostgreSQL-Datenbank-Sentinel verwendet
45654	Benutzeranwendung	Wird vom Server, auf dem die Datenbank für Identity Applications installiert ist, zum Empfang der Kommunikation verwendet, wenn Tomcat mit einer Clustergruppe ausgeführt wird

III Installieren und Konfigurieren der OpenText Identity Manager-Komponenten

In diesem Abschnitt finden Sie die Schritte für die Installation und Konfiguration der OpenText Identity Manager-Komponenten. Die Installationsanweisungen finden Sie unter „Installationsverfahren“, auf Seite 46.

Nach der Installation der OpenText Identity Manager-Komponenten und nach Abschluss der Basiskonfiguration müssen Sie einige weitere Konfigurationsschritte für die Komponenten ausführen, um den vollen Funktionsumfang zu erhalten. Weitere Informationen finden Sie unter Kapitel 4, „Abschließende Konfigurationsschritte“, auf Seite 65.

3 Überblick über den Installations- und Konfigurationsvorgang

In diesem Abschnitt wird die Vorgehensweise bei der Installation und Konfiguration der OpenText Identity Manager-Komponenten beschrieben. Informieren Sie sich vor Beginn des Konfigurationsvorgangs über die Konfigurationsoptionen der einzelnen Komponenten. Weitere Informationen finden Sie unter Konfigurationseinstellungen in.

Bei einigen Komponenten wie Designer oder Analyzer ist keine Konfiguration erforderlich.

Installationsreihenfolge

Die Komponenten müssen in der folgenden Reihenfolge installiert werden, da die Installationsprogramme für einige Komponenten die Informationen über vorher installierte Komponenten benötigen:

- Sentinel Log Management für Identity Governance and Administration (IGA) (Installation wird nur auf Linux-Rechnern unterstützt)
- Komponenten des OpenText Identity Manager-Servers
- Komponenten von Identity Applications (nur für die Advanced Edition)
- Komponenten von Identity Reporting
- Designer für OpenText Identity Manager
- Analyzer für OpenText Identity Manager

Vor der Installation der Komponenten müssen Sie die Voraussetzungen und Überlegungen für die Installation der einzelnen Komponenten genau lesen.

Erläuterungen zum Installations- und Konfigurationsvorgang für die Komponenten OpenText Identity Manager Server, Identity Applications und Identity Reporting

OpenText Identity Manager stellt eine assistentenbasierte Installationsmethode zum Installieren und Konfigurieren der folgenden OpenText Identity Manager-Komponenten zur Verfügung:

- OpenText Identity Manager Server
- Identity Applications
- Identity Reporting

Das Installationsprogramm ermöglicht Ihnen die interaktive oder automatische Installation und Konfiguration. Während der Installation können Sie die Werte für die installierten Komponenten angeben.

Bei der Installation wird auch in Ihrem Dateisystem ein Repository mit abhängigen Komponenten wie JRE, Apache Tomcat, PostgreSQl, ActiveMQ und OpenSSL erstellt. Wenn Sie mehrere OpenText Identity Manager-Komponenten auf demselben Computer installieren, wird im Installationsvorgang auf dieses Repository verwiesen statt mehrere Kopien dieser Komponenten für jede OpenText Identity Manager-Komponente zu erstellen, die diese benötigt. Beispielsweise verwenden Identity Applications und Identity Reporting denselben Tomcat, wenn sie auf demselben Computer installiert sind.

Installationsmethoden

OpenText Identity Manager unterstützt die interaktive und automatische Installation. Bei der automatischen (nicht interaktiven) Installation wird keine Benutzeroberfläche angezeigt, und der Benutzer muss keinerlei Fragen beantworten.

Interaktive Methode

Bei dieser Methode müssen Sie die zu installierenden Komponenten auswählen. Die Komponenten werden entsprechend Ihrer Auswahl installiert.

Automatische Methode

Bei dieser Methode müssen Sie die Werte für die zu installierenden Komponenten in der Eigenschaftendatei angeben. Wenn das Installationsprogramm aufgerufen wird, werden diese Werte aus der Eigenschaftendatei gelesen. Sie können dieselbe Eigenschaftendatei für die automatische Installation auf verschiedenen Computern in Ihrer Umgebung verwenden.

Installationsoptionen

In der folgenden Tabelle sind die zu installierenden Komponenten beschrieben und die Installationsoptionen des Installationsprogramms angegeben.

Tabelle 3-1 *Installationsoptionen*

Installationsoption	Installierte Komponenten
OpenText Identity Manager-Engine	Installiert das Identitätsdepot, die OpenText Identity Manager-Engine, den Remote Loader-Service-Webadministrator sowie die OpenText Identity Manager-Plugins, den Fan-out-Agent und die Treiber.
Identity Applications	Installiert Identity Applications, den One SSO Provider (OSP), den Benutzeranwendungstreiber, den Rollen- und Ressourcenservice-Treiber (RRSD), PostgreSQL sowie Self Service Password Reset (SSPR). **HINWEIS:** Wenn Sie SSPR auf einem anderen Server als Identity Applications installieren möchten, verwenden Sie die install.exe im Verzeichnis <Speicherort der eingehängten ISO-Datei>\common\sspr\.
Identity Reporting	Installiert Identity Reporting, OSP, PostgreSQL, den Treiber für den Datenerfassungsdienst (DCS) sowie den Managed System Gateway (MSGW)-Treiber.

Konfigurationsmodi

Zur Konfiguration der OpenText Identity Manager-Komponenten wählen Sie zwischen folgenden Methoden:

- Typisch
- Benutzerdefiniert

Bei einer typischen Konfiguration werden Standardeinstellungen für die meisten Konfigurationsoptionen herangezogen. In einer benutzerdefinierten Konfiguration können Sie individuelle Werte je nach Ihren besonderen Anforderungen festlegen. Mit dieser Option werden die meisten Einstellungen konfiguriert.

Verwenden von nicht intuitiven Passwörtern bei der Konfiguration

Während der Konfiguration müssen Sie für zahlreiche OpenText Identity Manager-Komponenten ein Passwort angeben. Um die Konfiguration schneller auszuführen, können Sie festlegen, dass ein einziges Passwort für alle Konfigurationsparameter verwendet werden soll.

Das Passwort muss mindestens sechs Zeichen umfassen. Verwenden Sie keine Wörter, die im Wörterbuch zu finden sind. Wörter aus dem Wörterbuch sind Schwachstellen für frei erhältliche Tools, die Passwörter knacken, weil diese oft Wörterbuchlisten enthalten. Falls Sie Wörter aus dem Wörterbuch verwenden müssen, versuchen Sie, diese mit Zahlen und Satzzeichen zu kombinieren.

Erläuterungen zum Installationsvorgang für Designer und Analyzer

OpenText Identity Manager stellt für Designer und Analyzer verschiedene Windows-Installationsprogramme zur Verfügung. Die Installationsprogramme für Designer und Analyzer sind auf der Produkt-Download-Website verfügbar.

Designer

Designer wird mit der Datei `Identity_Manager_4.10.0_Designer_Windows.zip` installiert. Geben Sie bei der automatischen Installation die Werte für die Installation in der Datei `designerInstaller.properties` an. Andernfalls nimmt das Installationsprogramm die Standardparameterwerte für die Installation an.

Designer benötigt keine Konfiguration.

Analyzer

WICHTIG: Das Analyzer-Tool ist nicht in der ISO für OpenText Identity Manager 4.10 enthalten. Wenn Analyzer bereits installiert ist, aktualisieren Sie ihn auf Version 4.8.5 und verwenden Sie ihn mit OpenText Identity Manager 4.10.

Analyzer wird mit der Datei `Identity_Manager_4.8.5_Windows_Analyzer.zip` installiert. Geben Sie bei der automatischen Installation die Werte für die Installation in der Datei `designerInstaller.properties` an. Andernfalls nimmt das Installationsprogramm die Standardparameterwerte für die Installation an.

Analyzer benötigt keine Konfiguration.

Installationsverfahren

In diesem Kapitel lernen Sie die Installationsmethoden für die OpenText Identity Manager-Komponenten kennen.

Installationsverfahren für OpenText Identity Manager Server, Identity Applications und Identity Reporting

In diesem Abschnitt werden Sie durch das Installationsverfahren für die OpenText Identity Manager Server-, Identity Applications- und Identity Reporting-Komponenten per interaktiver oder automatischer Methode geführt. Die Option **OpenText Identity Manager Server** im Installationsprogramm ermöglicht Ihnen die Installation des 32-Bit-, des 64-Bit- und des .NET Remote Loader.

HINWEIS: Bevor Sie die OpenText Identity Manager-Engine installieren, müssen Sie sicherstellen, dass der Windows-Server mit dem neuesten Windows-Patch aktualisiert wurde und der Windows-Server neu gestartet wird.

HINWEIS: Wenn Sie einen sekundären Server in einer Umgebung mit mehreren Servern bereitstellen, müssen Sie die IP-Adresse des Identitätsdepots des primären Servers angeben.

Interaktive Installation

1. Laden Sie die Datei `Identity_Manager_4.10.0_Windows.iso` von der Seite Software und Lizenz (https://sld.microfocus.com/) herunter.
2. Stellen Sie die heruntergeladene .iso-Datei bereit.
3. Führen Sie entsprechend der zu installierenden Komponente die `install.exe` aus, die an den folgenden Speicherorten verfügbar ist:
   - **OpenText Identity Manager Server:** `<Speicherort der eingehängten ISO-Datei>\IdentityManagerServer`
   - **Identity Applications:** `<Speicherort der eingehängten ISO-Datei>\IdentityApplications`
   - **Identity Reporting:** `<Speicherort der eingehängten ISO-Datei>\IdentityReporting`
4. Wählen Sie die Sprache für die Installation aus und klicken Sie auf **OK**.

   Auf dem Bildschirm **Einführung** werden die für die Installation verfügbaren Komponenten angezeigt.
5. Klicken Sie auf **Weiter**.

6 Lesen Sie die Lizenzvereinbarung durch und bestätigen Sie Ihr Einverständnis.

7 Wählen Sie die zu installierenden Komponenten aus und klicken Sie auf **Weiter**.

8 Geben Sie den Installationsorder an und klicken Sie dann auf **Weiter**.

HINWEIS: Der benutzerdefinierte Installationsordner sollte keine Sonderzeichen wie "." und "_" enthalten.

---

9 Wählen Sie die Installationsart aus:

- Standardinstallation
- Angepasste Installation

10 Die Installationsparameter unterscheiden sich entsprechend des ausgewählten Installationsmodus. Geben Sie die erforderlichen Details an. Informationen zu den Konfigurationsparametern finden Sie in den folgenden Tabellen:

- Einstellungen für die Identity Manager-Engine
- Einstellungen für Identity Applications
- Einstellungen für Identity Reporting

11 Lesen Sie die Details auf der Seite mit der Zusammenfassung vor der Installation und klicken Sie auf **Installieren**.

Automatische Installation

Für die automatische Installation der OpenText Identity Manager-Komponenten stehen Ihnen die Eigenschaftendateien in der jeweiligen `.iso`-Datei zur Verfügung. Das OpenText Identity Manager-Medium enthält ein Beispiel einer Eigenschaftendatei am Speicherort `<Speicherort_der_heruntergeladenen_ISO-Datei>\`*`Identity Manager-Komponente`*`>\response-files`.

Gehen Sie für die automatische Installation der Komponente folgendermaßen vor:

1 Laden Sie die Datei `Identity_Manager_4.10.0_Windows.iso` von der OpenText-Downloads-Website herunter.

2 Stellen Sie die heruntergeladene `.iso`-Datei bereit.

3 Verwenden Sie entsprechend der gewünschten Installationsmethode für die Komponenten die Dateien `typical_install.properties` bzw. `custom_install.properties`, die an den folgenden Speicherorten zur Verfügung stehen:

- **OpenText Identity Manager Server:** `<Speicherort der eingehängten ISO-Datei>\IdentityManagerServer\response-files`
- **Identity Applications:** `<Speicherort der eingehängten ISO-Datei>\IdentityApplications\response-files`
- **Identity Reporting:** `<Speicherort der eingehängten ISO-Datei>\IdentityReporting\response-files`

4 Bearbeiten Sie die Installationsparameter nach Bedarf. Informationen zu den Konfigurationsparametern finden Sie in den folgenden Tabellen:

- Einstellungen für die Identity Manager-Engine

- Einstellungen für Identity Applications
- Einstellungen für Identity Reporting

5 Führen Sie zur automatischen Installation folgenden Befehl im Verzeichnis mit der zu installierenden Komponente aus:

```
.\install.exe -i silent -f <Pfad zur typischen oder benutzerdefinierten Installationseigenschaftsdatei>
```

Beispiel:

```
.\install.exe -i silent -f C:\Users\Administrator\Desktop typical_install_idmengine.properties
```

6 (Optional) Die Standardinstallationsverzeichnisse sind im Installationsprotokoll aufgeführt. Sehen Sie sich beispielsweise folgende Dateien an:

```
C:\Programme\NetIQ\IDM\Installieren\Protokolle
```

Installation des Remote Loader

OpenText Identity Manager enthält eine Option zur Installation von Remote Loader auf einem eigenständigen Server. Verwenden Sie diese Option, wenn Sie OpenText Identity Manager-Engine und Remote Loader auf separaten Computern installieren möchten.

HINWEIS: Mit dieser Option können der 64-Bit-Remote Loader und der .NET-Remote Loader installiert werden. Informationen zur Installation eines 32-Bit-Remote Loader finden Sie unter Installationsverfahren für OpenText Identity Manager Server, Identity Applications und Identity Reporting.

Interaktive Installation

1 Laden Sie die Datei `Identity_Manager_4.10.0_RL_Windows.iso` von der OpenText-Downloads-Website herunter.

2 Hängen Sie die heruntergeladene `.iso`-Datei ein.

3 Führen Sie am Speicherplatz der Bereitstellung die Datei `install.exe` aus.

4 Wählen Sie die Sprache für die Installation aus und klicken Sie auf **OK**.

5 Klicken Sie auf **Weiter**.

6 Lesen Sie die Lizenzvereinbarung durch und bestätigen Sie Ihr Einverständnis.

7 Klicken Sie auf **Weiter**.

8 Geben Sie den Installationsordner an und klicken Sie auf **Weiter**.

9 Klicken Sie auf **Installieren**.

Automatische Installation

1 Laden Sie die Datei `Identity_Manager_4.10.0_RL_Windows.iso` von der OpenText-Downloads-Website herunter.

2 Hängen Sie die heruntergeladene `.iso`-Datei ein.

3 Navigieren Sie zu `<Speicherort der eingehängten ISO-Datei>\response-files`.

4 Führen Sie zur Ausführung der automatischen Installation folgenden Befehl im Verzeichnis mit der Eigenschaftendatei aus:

```
install.exe -i silent -f install.properties
```

Installieren des Java Remote Loader

Der Java Remote Loader dient in Identity Manager zum Datenaustausch zwischen der aktiven Identity Manager-Engine auf einem Server und den Identity Manager-Treibern an anderen Speicherorten, an denen `rdxml` nicht aktiviert ist. Installieren Sie den Java Remote Loader (dirxml_jremote) auf einer beliebigen unterstützten Windows-Plattform mit einer kompatiblen JRE und Java-Sockets.

1 Kopieren Sie auf dem Server, der die Identity Manager-Engine hostet, die ISO- und JAR-Dateien des Anwendungsschnittstellenmoduls an den Standardspeicherort. Beispiel: Verzeichnis `C:\NetIQ\idm\NDS\lib`.

2 Melden Sie sich an dem Computer an, auf dem der Java Remote Loader installiert werden soll (Zielcomputer).

3 Überprüfen Sie, ob eine unterstützte Version der JRE auf dem Zielcomputer vorliegt.

4 Laden Sie die Datei `Identity_Manager_4.10.0_Windows.iso` von der OpenText-Downloads-Website herunter.

5 Stellen Sie die heruntergeladene `.iso`-Datei bereit.

6 Navigieren Sie zum Verzeichnis `<Speicherort der installierten ISO-Datei>\IdentityManagerServer\products\IDM\java_remoteloader`.

7 Kopieren Sie die Datei `dirxml_jremote_dev.tar.gz` an den gewünschten Speicherort auf dem Zielcomputer. Kopieren Sie die Datei beispielsweise in `C:\NetIQ\idm`.

8 Kopieren Sie eine der folgenden Dateien an den gewünschten Speicherort auf dem Zielcomputer:

- `dirxml_jremote.tar.gz`
- `dirxml_jremote_mvs.tar`

  Wenn Sie weitere Informationen zu mvs benötigen, entpacken Sie die Datei `dirxml_jremote_mvs.tar`, und öffnen Sie das Dokument `usage.html`.

9 Entpacken und extrahieren Sie die `.tar.gz`-Dateien auf dem Zielcomputer.

  Beispiel: Verwenden Sie 7-Zip oder eine unterstützte Software zum Entpacken der `TAR.GZ`-Dateien.

10 Legen Sie die CLASSPATH-Umgebungsvariable auf alle JAR-Dateien fest, die sich im `lib`-Ordner befinden. Wenn Ihnen abhängige JAR-Dateien vorliegen, die für einen bestimmten Treiber spezifisch sind, kopieren Sie diese JAR-Dateien in den `lib`-Ordner. Legen Sie anschließend die CLASSPATH-Umgebungsvariable ebenfalls auf diese JAR-Dateien fest.

  Legen Sie beispielsweise in der Eingabeaufforderung den CLASSPATH fest:

```
CLASSPATH=E:\RL\JAVARL\lib\activation.jar;E:\RL\JAVARL\lib\commondrive
rshim.jar;E:\RL\JAVARL\lib\delimitedtextshim.jar;E:\RL\JAVARL\lib\deli
mitedtextutil.jar;E:\RL\JAVARL\lib\dirxml.jar;E:\RL\JAVARL\lib\dirxml_
misc.jar;E:\RL\JAVARL\lib\dirxml_remote.jar;E:\RL\JAVARL\lib\jco3envir
onment.jar;E:\RL\JAVARL\lib\mail.jar;E:\RL\JAVARL\lib\mapdb<version>.j
ar;E:\RL\JAVARL\lib\nxsl.jar;E:\RL\JAVARL\lib\shimwrapper.jar;E:\RL\JA
VARL\lib\xds.jar;E:\RL\JAVARL\lib\xp.jar
```

11 Legen Sie die PATH-Umgebungsvariable auf den `bin`-Ordner von JDK oder JRE für `Java.exe` fest.

12 Sie müssen den Ort der jar-Dateien im Skript `dirxml_jremote` angeben, das sich im Bibliotheksunterverzeichnis des nicht getarten Verzeichnisses `dirxml_jremote.tar.gz` befindet. Beispiel: `\lib\*.jar`.

13 Konfigurieren Sie die Beispielkonfigurationsdatei `config8000.txt` zur Verwendung mit dem Anwendungsschnittstellenmodul.

Die JAR-Datei `dirxml_jremote.tar.gz` enthält diese Datei. Weitere Informationen finden Sie unter Konfigurieren des Remote Loader und der Treiber im *Verwaltungshandbuch zu OpenText™ Identity Manager CE 24.4 (v4.10)*.

14 Starten Sie den Remote Loader mit den folgenden Befehlen:

14a So geben Sie ein Passwort für den Remote Loader an:

```
java.exe -classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config <config
file name> -sp <Remote Loader Password> <Object Driver Password>
```

Beispiel:

```
java.exe -classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config
e:\RL\JAVARL\config8000.txt -sp novell novell
```

14b So starten Sie den Remote Loader:

```
java.exe -classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config <config
file name>
```

Beispiel:

```
java.exe -classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config
e:\RL\JAVARL\config8000.txt
```

14c So stoppen Sie den Remote Loader:

HINWEIS: Öffnen Sie eine neue Eingabeaufforderung, und führen Sie den folgenden Befehl aus, um die aktuelle Remote Loader-Instanz zu stoppen.

```
java.exe -classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config <config
file name> -unload
```

Beispiel:

```
java.exe -classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config
e:\RL\JAVARL\config8000.txt -unload
```

Installieren des .NET Remote Loader

So installieren Sie den .NET Remote Loader als verwaltungsbefugter Benutzer:

1. Melden Sie sich als Administrator an dem Computer an, auf dem der .NET Remote Loader installiert werden soll.
2. Greifen Sie mit einem der folgenden Schritte auf das Installationsprogramm zu:
   - **2a** (Bedingt) Wenn Ihnen die `.iso`-Image-Datei für das OpenText Identity Manager-Installationspaket vorliegt, navigieren Sie zu dem Verzeichnis, in dem sich die .NET Remote Loader-Installationsdateien befinden (standardmäßig unter `\products\idm\windows\setup\`).
   - **2b** (Bedingt) Wenn Sie die Installationsdateien für den .NET Remote Loader von der OpenText-Downloads-Website heruntergeladen haben, führen Sie die folgenden Schritte aus:
     - Navigieren Sie zur `.tgz`-Datei für das heruntergeladene Image.
     - Extrahieren Sie den Inhalt der Datei in einen Ordner auf dem lokalen Computer.
3. Führen Sie das Programm `idm_install.exe` im Installationsverzeichnis aus.
4. Akzeptieren Sie die Lizenzvereinbarung, und klicken Sie auf **Weiter**.
5. Wählen Sie im Fenster für die Komponentenauswahl den .NET Remote Loader aus.
6. (Optional) Wählen Sie mit den folgenden Schritten bestimmte Treiber für die einzelnen Komponenten aus:
   - **6a** Klicken Sie auf **Ausgewählte Komponenten anpassen** und dann auf **Weiter**.
   - **6b** Erweitern Sie den Eintrag **Treiber** unter der zu installierenden Komponente.
   - **6c** Wählen Sie die zu installierenden Treiber aus.
7. Klicken Sie auf **Weiter**.
8. Klicken Sie im Fenster mit dem Aktivierungshinweis auf **OK**.
9. Wählen Sie auf Ihrem Computer das .NET Remote Loader-Installationsverzeichnis aus.
10. Prüfen Sie die Zusammenfassung und klicken Sie auf **Installieren**, um die Installation abzuschließen.

Installieren von SSPR

Das Installationsprogramm enthält eine Option zur separaten Installation von SSPR. Mit dieser Option installieren Sie Identity Applications und SSPR auf separaten Computern. Dies ist die einzige Option zur Installation von SSPR in einer Standard Edition. SSPR wird in der Standard Edition nicht automatisch installiert.

SSPR kann interaktiv oder automatisch installiert werden.

Interaktive Installation

1. Laden Sie die Datei `Identity_Manager_4.10.0_Windows.iso` von der OpenText-Downloads-Website herunter.
2. Hängen Sie die heruntergeladene `.iso`-Datei ein.
3. Navigieren Sie zum Verzeichnis `<Speicherort der eingehängten ISO-Datei>\common\sspr`.
4. Führen Sie die Datei `install.exe` aus.
5. Wählen Sie die Sprache für die Installation aus und klicken Sie auf **OK**.
6. Klicken Sie auf **Weiter**.
7. Lesen Sie die Lizenzvereinbarung durch und bestätigen Sie Ihr Einverständnis.
8. Klicken Sie auf **Weiter**.
9. Geben Sie den Installationsordner an und klicken Sie auf **Weiter**.
10. Geben Sie die Konfigurationseinstellungen für SSPR an. Weitere Informationen finden Sie unter „Konfiguration des Arbeitsblatts für Self-Service Password Reset“, auf Seite 59.
11. Klicken Sie auf **Weiter**.
12. Klicken Sie auf **Installieren**.

Automatische Installation

1. Laden Sie die Datei `Identity_Manager_4.10.0_Windows.iso` von der OpenText-Downloads-Website herunter.
2. Hängen Sie die heruntergeladene `.iso`-Datei ein.
3. Navigieren Sie zum Verzeichnis `<Speicherort der eingehängten ISO-Datei>\common\sspr`.
4. Führen Sie zur Ausführung der automatischen Installation folgenden Befehl im Verzeichnis mit der Eigenschaftendatei aus:

   ```
   install.exe -i silent -f sspr_silentinstall.properties
   ```

Konfigurationseinstellungen in

Anhand der folgenden Arbeitsblätter können Sie die Informationen sammeln, die Sie zur Konfiguration der OpenText Identity Manager-Komponenten angeben müssen.

Arbeitsblatt für die Konfiguration der OpenText Identity Manager-Engine

Anhand des folgenden Arbeitsblatts können Sie die Informationen sammeln, die Sie zur Konfiguration der OpenText Identity Manager-Engine angeben müssen.

Tabelle 3-2 *Einstellungen der OpenText Identity Manager-Engine*

Parameter	Beschreibung
DIB-Speicherort des Identitätsdepots	Geben Sie den DIB-Speicherort des Identitätsdepots an.
Neuen Baum erstellen	Wählen Sie diese Option aus, wenn Sie einen neuen Identitätsdepotbaum erstellen möchten.
Baumname	*Gilt nur dann, wenn Sie die Option* **Neuen Baum erstellen** *ausgewählt haben.* Geben Sie den Baumnamen des Identitätsdepots an.
Zu einem vorhandenen Baum hinzufügen	Wählen Sie diese Option aus, wenn Sie eine Verbindung zu einem Identitätsdepotbaum auf einem Remote-Server herstellen möchten. Sie müssen nur eine IP-Adresse angeben. Der Hostname oder FQDN wird nicht unterstützt.
Host	*Gilt nur dann, wenn Sie die Option* **Zu einem vorhandenen Baum hinzufügen** *ausgewählt haben.* Geben Sie die IP-Adresse für das Identitätsdepot an.
Sicherer LDAP-Port	*Gilt nur dann, wenn Sie die Option* **Zu einem vorhandenen Baum hinzufügen** *ausgewählt haben.* Gibt den Port an, den das Identitätsdepot mit dem SSL-Protokoll (Secure Sockets Layer) auf LDAP-Anforderungen überwachen soll. Der Standardwert ist 636. Wenn ein Dienst, der bereits vor der Installation von OpenText eDirectory auf dem Server geladen war, den Port nutzt, müssen Sie einen anderen Port angeben.
Administrator-DN	Geben Sie den Administratornamen für die OpenText Identity Manager-Engine an. Der Standardwert lautet `cn=admin,ou=sa,o=system`.
Administratorpasswort	Geben Sie das Passwort für das Administratorobjekt an. Beispiel: `Passwort`.
Kontext des Identitätsdepot-Servers (im LDAP-Format)	Geben Sie den DN für den Server-Container an. Der Standardwert lautet `ou=servers, o=system`
Identitätsdepot-Treibersatz (im LDAP-Format)	Geben Sie den Kontext-DN für den Treibersatz an. Der Standardwert lautet `cn=DriverSet, o=system`.
Klartext-LDAP-Port	Geben Sie den Port an, den das Identitätsdepot auf LDAP-Anforderungen im Klartext überwachen soll. Der Standardwert ist 389.
Sicherer LDAP-Port	Geben Sie den Port an, den das Identitätsdepot mit dem SSL-Protokoll (Secure Sockets Layer) auf LDAP-Anforderungen überwachen soll. Der Standardwert ist 636. Wenn ein Dienst, der bereits vor der Installation von OpenText eDirectory auf dem Server geladen war, den Port nutzt, müssen Sie einen anderen Port angeben.

Parameter	Beschreibung
Klartext-HTTP-Port	Geben Sie den Port an, an dem der HTTP-Stapel in Klartext arbeitet. Der Standardwert ist 8028.
Sicherer HTTP-Port	Geben Sie den Port an, an dem der HTTP-Stack mit dem TLS/SSL-Protokoll arbeitet. Der Standardwert ist 8030.
RSA-Schlüsselgröße	*Gilt nur dann, wenn Sie die Option* **Neuen Baum erstellen** *ausgewählt haben.* Geben Sie die Schlüsselgröße für RSA-Zertifikate an. Zulässige Werte sind 2048, 4096 und 8192 Bit. Der Standardwert ist 4096.
EC-Kurve	*Gilt nur dann, wenn Sie die Option* **Neuen Baum erstellen** *ausgewählt haben.* Geben Sie den Grenzwert der elliptischen Kurve (EC) für EC-Zertifikate an. Zulässige Werte sind P256, P384 und P521. Der Standardwert ist P384.
Zertifikatslebensdauer	*Gilt nur dann, wenn Sie die Option* **Neuen Baum erstellen** *ausgewählt haben.* Geben Sie die Lebensdauer des Zertifikats in Jahren an.

Arbeitsblatt zur Konfiguration von Identity Applications

Anhand des folgenden Arbeitsblatts können Sie die Informationen sammeln, die Sie zur Konfiguration von Identity Applications angeben müssen.

Tabelle 3-3 *Einstellungen für Identity Applications*

Parameter	Beschreibung
Self-Service Password Reset installieren	Geben Sie an, ob die SSPR-Komponente installiert werden soll.
Host	Geben Sie die IP-Adresse des Servers an, auf dem das Identitätsdepot installiert ist.
Sicherer LDAP-Port	Geben Sie den Port an, den das Identitätsdepot mit dem SSL-Protokoll (Secure Sockets Layer) auf LDAP-Anforderungen überwachen soll. Der Standardwert ist 636. Wenn ein Dienst, der bereits vor der Installation von OpenText eDirectory auf dem Server geladen war, den Port nutzt, müssen Sie einen anderen Port angeben.
Administrator-DN	Geben Sie den Administratornamen für die OpenText Identity Manager-Engine an. Der Standardwert lautet cn=admin,ou=sa,o=system.

Parameter	Beschreibung
Administratorpasswort	Gilt nur dann, wenn Sie einen neuen Authentifizierungsserver installieren. Geben Sie das Passwort des Administratorkontos für den LDAP-Authentifizierungsserver an.
Master-Keystore-Passwort	Geben Sie das Master-Keystore-Passwort für die Identity Application an.
Stammcontainer-DN	Geben Sie den Root-Container an. Der Standardwert lautet `o=data`.
Benutzer-Container-DN	*Gilt nur dann, wenn Sie einen neuen Authentifizierungsserver installieren.* Geben Sie den Container auf dem LDAP-Authentifizierungsserver an, in dem die Benutzerkonten für die Anmeldung bei Access Review gespeichert sind. Beispiel: `o=data`.
Administrator-Container-DN	*Gilt nur dann, wenn Sie einen neuen Authentifizierungsserver installieren.* Geben Sie den Container auf dem LDAP-Authentifizierungsserver an, in dem die Administratorkonten gespeichert sind.
Treibersatz-DN	Geben Sie den DN für den Treibersatz an.
Identity Applications-Treiber	Wählen Sie diese Option aus, wenn Sie den Benutzeranwendungstreiber und den Rollen- und Ressourcenservice-Treiber bereitstellen möchten.
Datenbankplattform für Identity Applications auswählen	Wählen Sie die Datenbank aus, die Sie mit Identity Applications verwenden möchten. Die Optionen sind PostgreSQL, Oracle und Microsoft SQL Server.
Neuer PostgreSQL-Server	Wählen Sie diese Option aus, wenn Sie eine neue Instanz der PostgreSQL-Datenbank installieren möchten.
Vorhandener PostgreSQL-Server	Wählen Sie diese Option aus, wenn Sie eine Verbindung zu einem bestehenden PostgreSQL-Datenbankserver herstellen möchten.
Datenbank-Host	Geben Sie den Namen bzw. die IP-Adresse des Servers an.
Datenbankport	Geben Sie den Port an, über den der Server mit der Benutzeranwendung kommunizieren soll. Standardmäßig ist der Wert auf 5432 festgelegt.
Name der Identity Applications-Datenbank	Geben Sie den Namen der Datenbank für Identity Applications an.
Name der Workflow-Engine-Datenbank	Geben Sie den Namen der Datenbank für die Workflow-Engine an.
Datenbankbenutzer	Geben Sie den Namen eines Kontos an, über das die Benutzeranwendung auf die Daten in den Datenbanken zugreifen und diese Daten bearbeiten kann.

Parameter	Beschreibung
Datenbankbenutzer-Passwort	Geben Sie das Benutzerpasswort für die Datenbank an.
Datenbanktreiber-JAR	Geben Sie die JAR-Datei für die Datenbankplattform an. Der Hersteller der Datenbank stellt die Treiber-JAR-Datei bereit, die als Thin-Client-JAR-Datei für den Datenbankserver fungiert. Beispielsweise könnten Sie für PostgreSQL `postgresql-9.4-1212.jdbc42.jar` angeben, standardmäßig im Ordner `C:\NetIQ\idm\apps\Postgres`. Wir unterstützen keine JAR-Daten für Treiber von Drittanbietern.
Wann soll das Schema erstellt werden	Geben Sie den Zeitpunkt für die Erstellung des Datenbankschemas als Teilprozess an. Die verfügbaren Optionen sind **Jetzt**, **Beim Start der Anwendung** und **SQL in Datei schreiben**.
Host des Anwendungsservers	Geben Sie die IP-Adresse an, unter der Tomcat installiert ist.
Anwendungsserver-HTTPS-Port	Geben Sie den Port an, an dem Tomcat installiert ist. Standardmäßig ist der Wert auf 8543 festgelegt.
Name für den Anmeldebildschirm	Geben Sie den benutzerdefinierten Namen an, der auf dem Benutzeranmeldebildschirm angezeigt werden soll. Der Standardwert lautet `Identity Access`. Wenn Sie Identity Applications aktualisieren, ändert sich der Name des Anmeldebildschirms automatisch in `OpenText Access`.
Identity Applications-Administrator	Geben Sie den DN eines Administratorkontos für den LDAP-Authentifizierungsserver an. Beispiel: `cn=uaadmin,ou=sa,o=data`
Administratorpasswort	Geben Sie das Administratorpasswort für Identity Applications an.
Dieses Passwort als allgemeines Passwort für andere Einstellungen festlegen	Wählen Sie diese Option aus, wenn Sie ein allgemeines Passwort festlegen möchten. **HINWEIS:** Das Standardpasswort für den Tomcat-Keystore lautet `changeit`.
Passwort für OAuth-Keystore	*Gilt nur, wenn Sie das Kontrollkästchen* **Dieses Passwort als allgemeines Passwort für andere Einstellungen festlegen** *aktiviert haben.* Geben Sie das Passwort für den OAuth-Keystore an.
SSO-Client-Passwort	*Gilt nur, wenn Sie das Kontrollkästchen* **Dieses Passwort als allgemeines Passwort für andere Einstellungen festlegen** *aktiviert haben.* Geben Sie das SSO-Client-Passwort an.

Parameter	Beschreibung
SSPR-Konfigurationspasswort	*Gilt nur, wenn Sie das Kontrollkästchen* **Dieses Passwort als allgemeines Passwort für andere Einstellungen festlegen** *aktiviert haben.* Geben Sie das SSPR-Client-Passwort an.
HTTPS-Port für Formular-Renderer	Geben Sie den HTTPS-Port für den Formular-Renderer an. Standardmäßig ist der Wert auf `8600` festgelegt.
Workflow-Engine-ID	Geben Sie einen eindeutigen Wert für die Workflow-Engine-ID an.

Arbeitsblatt zur Konfiguration von Identity Reporting

Anhand des folgenden Arbeitsblatts können Sie die Informationen sammeln, die Sie zur Konfiguration von Identity Reporting angeben müssen.

HINWEIS: Konfigurieren Sie Identity Reporting vor der Installation für die Oracle- oder MS SQL-Datenbank. Weitere Informationen finden Sie unter Manuelles Generieren des Datenbankschemas.

Tabelle 3-4 *Einstellungen für Identity Reporting*

Parameter	Beschreibung
Host	Geben Sie die IP-Adresse des Servers an, auf dem das Identitätsdepot installiert ist.
Sicherer LDAP-Port	Geben Sie den Port an, den das Identitätsdepot mit dem SSL-Protokoll (Secure Sockets Layer) auf LDAP-Anforderungen überwachen soll. Der Standardwert ist 636. Wenn ein Dienst, der bereits vor der Installation von OpenText eDirectory auf dem Server geladen war, den Port nutzt, müssen Sie einen anderen Port angeben.
Administrator-DN	Geben Sie den Administratornamen für die OpenText Identity Manager-Engine an. Der Standardwert lautet `cn=admin,ou=sa,o=system`.
Administratorpasswort	Geben Sie das Passwort des Administratorkontos für den LDAP-Authentifizierungsserver an.
Master-Keystore-Passwort	Geben Sie das Master-Keystore-Passwort für das Identity Reporting an.
Benutzer-Container-DN	*Gilt nur dann, wenn Sie einen neuen Authentifizierungsserver installieren.* Geben Sie den Container auf dem LDAP-Authentifizierungsserver an, in dem die Benutzerkonten für die Anmeldung bei Access Review gespeichert sind. Beispiel: `o=data`.

Parameter	Beschreibung
Administrator-Container-DN	*Gilt nur dann, wenn Sie einen neuen Authentifizierungsserver installieren.* Geben Sie den Container auf dem LDAP-Authentifizierungsserver an, in dem die Administratorkonten gespeichert sind.
Treibersatz-DN	Geben Sie den DN für den Treibersatz an.
Identity Reporting-Treiber bereitstellen	Wählen Sie diese Option aus, wenn Sie den Treiber der Datenerfassungsdienste und den Treiber von „Verwaltetes System – Gateway“ bereitstellen möchten.
Datenbankplattform für Identity Reporting auswählen	Wählen Sie die Datenbank aus, die Sie mit Identity Reporting verwenden möchten. Die Optionen sind PostgreSQL, Oracle und Microsoft SQL Server.
Neuer PostgreSQL-Server	Wählen Sie diese Option aus, wenn Sie eine neue Instanz der PostgreSQL-Datenbank installieren möchten.
Vorhandener PostgreSQL-Server	Wählen Sie diese Option aus, wenn Sie eine Verbindung zu einem bestehenden PostgreSQL-Datenbankserver herstellen möchten.
Datenbank-Host	Geben Sie den Namen bzw. die IP-Adresse des Servers an.
Datenbankport	Geben Sie den Port an, über den der Server mit Identity Reporting kommunizieren soll. Standardmäßig ist der Wert auf 5432 festgelegt.
Datenbankname	Geben Sie den Namen der Datenbank für Identity Reporting an.
Datenbankbenutzer-Passwort	Geben Sie das Benutzerpasswort für die Datenbank an.
Passwort für Datenbankkonto	Geben Sie das Passwort für das Datenbankkonto für Identity Reporting an.
Host des Anwendungsservers	Geben Sie die IP-Adresse an, unter der Tomcat installiert ist.
Anwendungsserver-HTTPS-Port	Geben Sie den Port an, an dem Tomcat installiert ist. Standardmäßig ist der Wert auf 8543 festgelegt.
Externer OSP-Server	Wählen Sie diese Option aus, wenn Sie eine Verbindung zu einem externen OSP-Server herstellen möchten. Mit dieser Option können Sie beispielsweise eine Verbindung zu einem Remote-OSP herstellen, der von Identity Applications genutzt wird.
OSP-Server-Host	*Gilt nur dann, wenn Sie die Option* **Externer OSP-Server** *ausgewählt haben.* Geben Sie die IP-Adresse des Servers an, auf dem OSP installiert ist.

Parameter	Beschreibung
OSP-Server-Port	*Gilt nur dann, wenn Sie die Option* **Externer OSP-Server** *ausgewählt haben.* Geben Sie den OSP-Server-Port an.
OSP-Keystore	*Gilt nur dann, wenn Sie die Option* **Externer OSP-Server** *ausgewählt haben.* Geben Sie den Speicherort der OSP-Keystore-Datei an.
OSP-Keystore-Passwort	*Gilt nur dann, wenn Sie die Option* **Externer OSP-Server** *ausgewählt haben.* Geben Sie das OSP-Keystore-Passwort an.
OSP-Client-Passwort	*Gilt nur dann, wenn Sie die Option* **Externer OSP-Server** *ausgewählt haben.* Geben Sie das OSP-Client-Passwort an.
Identity Reporting-Administrator	Gibt den Namen des Administrators für Identity Reporting an. Der Standardwert lautet `cn=uaadmin,ou=sa,o=data`.
Identity Reporting-Administratorpasswort	Gibt das Administratorpasswort für Identity Reporting an.
Dieses Passwort als allgemeines Passwort für andere Einstellungen festlegen	Wählen Sie diese Option aus, wenn Sie ein allgemeines Passwort festlegen möchten.

Konfiguration des Arbeitsblatts für Self-Service Password Reset

Anhand des folgenden Arbeitsblatts können Sie die Informationen sammeln, die Sie zur Konfiguration von Self-Service Password Reset (SSPR) angeben müssen.

Dieser Abschnitt ist nur interessant, wenn Sie Identity Applications und SSPR auf separaten Computern installieren möchten.

Tabelle 3-5 *SSPR-Einstellungen*

Parameter	Beschreibung
Host	Geben Sie die IP-Adresse des Servers an, auf dem das Identitätsdepot installiert ist.
Sicherer LDAP-Port	Geben Sie den Port an, den das Identitätsdepot mit dem SSL-Protokoll (Secure Sockets Layer) auf LDAP-Anforderungen überwachen soll. Der Standardwert ist 636. Wenn ein Dienst, der bereits vor der Installation von OpenText eDirectory auf dem Server geladen war, den Port nutzt, müssen Sie einen anderen Port angeben.
Administrator-DN	Geben Sie den Administratornamen für die OpenText Identity Manager-Engine an. Der Standardwert lautet `cn=admin,ou=sa,o=system`.

Parameter	Beschreibung
Administratorpasswort	Geben Sie das Passwort des Administratorkontos für den LDAP-Authentifizierungsserver an.
Benutzer-Container-DN	*Gilt nur dann, wenn Sie einen neuen Authentifizierungsserver installieren.* Geben Sie den Container auf dem LDAP-Authentifizierungsserver an, in dem die Benutzerkonten für die Anmeldung bei Access Review gespeichert sind. Beispiel: `o=data`.
Administrator-Container-DN	*Gilt nur dann, wenn Sie einen neuen Authentifizierungsserver installieren.* Geben Sie den Container auf dem LDAP-Authentifizierungsserver an, in dem die Administratorkonten gespeichert sind.
Host des Anwendungsservers	Geben Sie die IP-Adresse an, unter der Tomcat installiert ist.
Anwendungsserver-HTTPS-Port	Geben Sie den Port an, an dem Tomcat installiert ist. Standardmäßig ist der Wert auf 8543 festgelegt.
Identity Applications-Administrator	Geben Sie den DN eines Administratorkontos für den LDAP-Authentifizierungsserver an. Beispiel: `cn=uaadmin,ou=sa,o=data`
Administratorpasswort	Geben Sie das Administratorpasswort für Identity Applications an.
Host des Authentifizierungsservers	Geben Sie die IP-Adresse des Servers an, auf dem OSP installiert ist.
HTTPS-Port des Authentifizierungsservers	Geben Sie den HTTPS-Port für den OSP-Server an.
Client-Passwort für den Authentifizierungsserver	Geben Sie das OSP-Client-Passwort an.

Schritte nach der Installation

In diesem Abschnitt erfahren Sie, wie Sie Ihre Tomcat-Umgebung im Anschluss an die Installation der Identity Applications aktualisieren.

- „Übergeben der preferIPv4Stack-Eigenschaft an die JVM“, auf Seite 61
- „Prüfen des Serverzustands“, auf Seite 61
- „Überwachen der Zustandsstatistiken“, auf Seite 61
- „Erstellen von Verbundindizes“, auf Seite 62
- „Konfigurieren der Identity-Anwendung für das Ablehnen einer vom Client initiierten erneuten SSL-Aushandlung“, auf Seite 63

Übergeben der preferIPv4Stack-Eigenschaft an die JVM

Die Caching-Implementierung erfolgt bei den Identity Applications mithilfe von JGroups. Bei einigen Konfigurationen muss dabei für JGroups die preferIPv4Stack-Eigenschaft auf „true“ gesetzt werden, damit die mcast_addr-Bindung erfolgreich hergestellt werden kann.

Ohne diese Option tritt möglicherweise der folgende Fehler auf:

```
[10/1/09 16:11:22:147 EDT] 0000000d UDP          W org.jgroups.util.Util
createMulticastSocket could not bind to /228.8.8.8 (IPv4 address); make
sure
your mcast_addr is of the same type as the IP stack (IPv4 or IPv6).
```

Unter Umständen wird der folgende Fehler angezeigt:

```
[3/21/12 10:04:32:470 EDT] 00000024 UDP      E org.jgroups.protocols.TP
down
failed sending message to null (131 bytes)
        java.lang.Exception: dest=/228.8.8.8:45654 (134 bytes)
    at org.jgroups.protocols.UDP._send(UDP.java:353)
```

Der Parameter `java.net.preferIPv4Stack=true` ist eine Systemeigenschaft, die auf dieselbe Weise festgelegt werden kann wie andere Systemeigenschaften, wie z. B. `extend.local.config.dir`.

Prüfen des Serverzustands

Die meisten Lastausgleichprogramme bieten eine Funktion zur Zustandsprüfung, um herauszufinden, ob ein HTTP-Server aktiv ist und die Überwachung durchführt. Die Benutzeranwendung enthält eine URL, die zum Konfigurieren des HTTP-Server-Zustands auf Ihrem Lastausgleichprogramm verwendet wird. Die URL lautet:

`http://<Knoten-IP>:port/IDMProv/jsps/healthcheck.jsp`

Überwachen der Zustandsstatistiken

Mit der REST-API werden Informationen über den Zustand der Benutzeranwendung abgerufen. Die API greift auf das System zu, um die aktuell ausgeführten Threads, den Arbeitsspeicherverbrauch, den Cache und die Clusterinformationen abzurufen; die Informationen werden mit der GET-Operation zurückgegeben.

- **Arbeitsspeicherinformationen (JVM und Systemarbeitsspeicher):** Liest die Arbeitsspeicherinformationen wie den von der JVM belegten Systemarbeitsspeicher und Arbeitsspeicher.

  Beispiel:

  `http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/memoryinfo`

- **Thread-Informationen:** Liest die Informationen über die CPU-intensiven Threads und gibt die Liste der Top-Threads zurück, die die CPU enorm auslasten.

  Beispiel:

  `http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/threadinfo`

Legen Sie den Stack-Parameter auf **true** fest, um auf den Stacktrace in der JVM zuzugreifen.

Beispiel:

```
http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/
threadinfo?stack=true
```

Geben Sie die Anzahl der Threads in der JVM mit dem Wert für den **thread-count**-Parameter an.

Beispiel:

```
http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/
threadinfo?thread-count=1
```

- **Cache-Informationen:** Liest die Cache-Informationen für die Benutzeranwendung.

  Beispiel:

  ```
  http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/cacheinfo
  ```

- **Clusterinformationen:** Liest die clusterbezogenen Informationen.

  Beispiel:

  ```
  http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/clusterinfo
  ```

HINWEIS: Sie müssen ein Sicherheitsadministrator sein, um die Zustandsstatistiken für die Benutzeranwendung anhand der REST API anzuzeigen.

Erstellen von Verbundindizes

Nach dem Installieren oder Aktualisieren der Identity Applications erstellen Sie manuell die Verbundindizes für die einzelnen Attribute, nach denen die Benutzer im OpenText Identity Manager-Dashboard sortiert werden sollen. Sie können die Verbundindizes mit dem Dienstprogramm `ndsindex`im OpenText eDirectory-Installationspfad erstellen. Sollen mehrere Attribute zur Verbundindizierung angegeben werden, trennen Sie die Attribute jeweils mit dem Zeichen $. Für die folgenden grundlegenden Attribute ist eine Verbundindizierung erforderlich:

- Nachname,Vorname
- Vorname,Nachnahme
- cn,Nachname
- Titel,Nachname
- Telefonnummer,Nachname
- Internet-Email-Adresse,Nachname
- L,Nachname
- OU,Nachname

Der folgende Befehl erleichtert die Erstellung von Verbundindizes mit dem Dienstprogramm `ndsindex`:

```
ndsindex add [-h <hostname>] [-p <port>] -D <admin DN> -W|[-w <password>] -
s <eDirectory Server DN> [<indexName1>, <indexName2>.....]
```

Mit dem folgenden Befehl sortieren Sie die Benutzer beispielsweise nach **Title**:

```
ndsindex add -h <hostname> -p <ldap port> -D <admin DN> -w <admin passwd> -
s <eDirectory Server DN> Title-SN;Title$Surname;value
```

Außerdem können Sie mit dem Dienstprogramm für Exportkonversionen auch Verbundindizes erstellen.

Für die Erstellung von Indizes benötigen Sie LDIF-Dateien. Nach dem Import der LDIF-Datei müssen Sie die Indizierungsaktivität einleiten, indem Sie Limber auslösen. Sonst findet eine Indizierung nur statt, wenn Limber automatisch ausgelöst wird.

Beispiel für eine LDIF-Datei für Verbundindizes für die Sortierung von Benutzern nach dem Attribut **Titel**:

```
dn: cn=osg-nw5-7, o=Novell

changetype: modify

add: indexDefinition

indexDefinition: 0$sntitleindex$0$0$0$1$Title$surname
```

Weitere Informationen zur Verwendung von LDIF-Dateien finden Sie in LDIF Files in *OpenText eDirectory Administration Guide (https://www.netiq.com/documentation/edirectory-93/edir_admin/data/bookinfo.html)* ("LDIF-Dateien" im "OpenText eDirectory-Administrationshandbuch").

Konfigurieren der Identity-Anwendung für das Ablehnen einer vom Client initiierten erneuten SSL-Aushandlung

Standardmäßig konfiguriert das Installationsprogramm der Identity Applications eine nicht sichere Verbindung (http). Unter bestimmten Umständen besteht die Gefahr eines DoS-Angriffs (Denial of Service) auf OpenText Identity Manager über eine nicht sichere Verbindung, der durch die vom Client initiierte erneute SSL-Aushandlung mit dem Identity Applications-Server ausgelöst wird. Damit dieses Problem nicht auftritt, ergänzen Sie den Eintrag `CATALINA_OPTS` in der Datei `<Tomcat-Installationsverzeichnis>\bin\setenv.bat` mit dem nachfolgenden Flag.

```
 "-Djdk.tls.rejectClientInitiatedRenegotiation=true"
```

4 Abschließende Konfigurationsschritte

Nach der Installation und Konfiguration der OpenText Identity Manager-Komponenten müssen Sie bestimmte Aufgaben ausführen, damit die Lösung in Ihrer Umgebung ordnungsgemäß funktioniert. Konfigurieren Sie beispielsweise die installierten Treiber, um die von Ihren Geschäftsprozessen definierten Richtlinien und Anforderungen zu erfüllen, und konfigurieren Sie Sentinel Log Management für IGA zum Sammeln von Auditereignissen.

Zu den Aufgaben nach der Installation gehören in der Regel die folgenden Elemente:

- „Das Konfigurieren des Identitätsdepots“, auf Seite 65
- „Konfigurieren des Remote Loader und der Treiber“, auf Seite 66
- „Konfigurieren der „Passwort vergessen“-Verwaltung“, auf Seite 66
- „Konfigurieren der Datenbank für Identity Applications“, auf Seite 71
- „Konfigurieren von Identity Applications“, auf Seite 74
- „Konfigurieren der Laufzeitumgebung für die Datenerfassung“, auf Seite 102
- „Konfigurieren von Identity Reporting“, auf Seite 112
- „OpenText Identity Manager aktivieren“, auf Seite 119

HINWEIS: Stellen Sie nach der Installation und Konfiguration von Identity Applications und Identity Reporting die während der Installation verwendeten JAR-Dateien – entweder `ojdbc8.jar` für Oracle oder `mssql-jdbc-9.2.1.jre8.jar` für MSSQL – basierend auf der verwendeten Datenbank im Verzeichnis `tomcat/lib` wieder her. Starten Sie dann die Tomcat-Dienste neu.

Das Konfigurieren des Identitätsdepots

- Manuelles Importieren der Identity Applications- und Identity Reporting-Zertifikate im Identitätsdepot

Manuelles Importieren der Identity Applications- und Identity Reporting-Zertifikate im Identitätsdepot

- Wenn Ihnen benutzerdefinierte Zertifikate für Identity Applications- und Identity Reporting-Komponenten vorliegen, importieren Sie diese Zertifikate im Identitätsdepot in cacerts (`C:\NetIQ\eDirectory\jre\lib\security\cacerts`).

  Sie können die Zertifikate beispielsweise mit dem folgenden Keytool-Befehl im Identitätsdepot importieren:

  ```
  keytool -import -trustcacerts -alias <User Application certificate
  alias name> -keystore <cacerts file> -file <User Application
  certificate file>
  ```

- Wenn Sie SSPR auf einem anderen Server als dem Anwendungsserver installieren, importieren Sie das SSPR-Anwendungszertifikat in der Benutzeranwendung in idm.jks (`C:\NetIQ\idm\apps\tomcat\conf\idm.jks`).

  Sie können die Zertifikate beispielsweise mit dem folgenden Keytool-Befehl in der Benutzeranwendung importieren:

  ```
  keytool -import -trustcacerts -alias <SSPR certificate alias name> -
  keystore <idm.jks> -file <SSPR certificate file>
  ```

Konfigurieren des Remote Loader und der Treiber

Remote Loader ermöglicht den OpenText Identity Manager-Treibern den Zugriff auf die verbundene Anwendung, ohne das Identitätsdepot und die OpenText Identity Manager-Engine auf dem selben Server als Anwendung installieren zu müssen. Für Remote Loader müssen Sie das Anwendungs-Shim konfigurieren, sodass es sich sicher mit der OpenText Identity Manager-Engine verbinden kann. Außerdem müssen sowohl der Remote Loader als auch die OpenText Identity Manager-Treiber konfiguriert werden. Detaillierte Informationen hierzu finden Sie unter Konfigurieren des Remote Loader und der Treiber im *Verwaltungshandbuch zu OpenText™ Identity Manager CE 24.4 (v4.10)-Treiber*.

Konfigurieren der „Passwort vergessen“-Verwaltung

Die OpenText Identity Manager-Installation umfasst eine Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung, sodass Sie ein vergessenes Passwort schnell und einfach zurücksetzen können. Alternativ können Sie ein externes Passwortverwaltungssystem nutzen.

- „Verwenden der Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung für die „Passwort vergessen“-Verwaltung“, auf Seite 66
- „Verwenden eines externen Systems für die „Passwort vergessen“-Verwaltung“, auf Seite 69
- „Aktualisieren der SSPR-Links im Dashboard für eine dezentrale Umgebung oder eine Cluster-Umgebung“, auf Seite 71

Verwenden der Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung für die „Passwort vergessen“-Verwaltung

In der Regel wird die „Passwort vergessen“-Verwaltungsfunktion beim Installieren von SSPR und der Identity Applications aktiviert. Ggf. haben Sie dabei nicht die URL der Portalseite für Identity Applications angegeben, an die SSPR die Benutzer nach einer Änderung des Passworts weiterleiten soll. Unter Umständen müssen Sie die „Passwort vergessen“-Verwaltung aktivieren. Dieser Abschnitt enthält die folgenden Informationen:

- „Konfigurieren von OpenText Identity Manager für die Verwendung der Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung“, auf Seite 67
- „Konfigurieren der Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung für OpenText Identity Manager“, auf Seite 67
- „Sperren der SSPR-Konfiguration“, auf Seite 68

Konfigurieren von OpenText Identity Manager für die Verwendung der Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung

In diesem Abschnitt wird beschrieben, wie Sie OpenText Identity Manager für die Verwendung von SSPR konfigurieren.

1. Melden Sie sich bei dem Server an, auf dem Sie Identity Applications installiert haben.
2. Starten Sie das Dienstprogramm zur Aktualisierung der Konfiguration. Weitere Informationen finden Sie unter Abschnitt 3, „Überblick über den Installations- und Konfigurationsvorgang“, auf Seite 43.
3. Navigieren Sie im Dienstprogramm zu **Authentifizierung** > **Passwortverwaltung**.
4. Geben Sie für **Passwortverwaltungsanbieter > Self Service Password Reset (SSPR)** an.
5. (Optional) Wenn Sie auf der Anmeldeseite von Identity Applications Links zum Zurücksetzen des Benutzernamens oder Passworts oder zur Aktivierung eines neuen Benutzerkontos bereitstellen möchten, wählen Sie in der Dropdown-Liste **Benutzeroberfläche** die Option **Andere Links** und aktivieren Sie anschließend das gewünschte Kontrollkästchen. Alternativ können Sie auch einen gemeinsamen Link angeben, indem Sie **"Können Sie sich nicht anmelden?"** in der Dropdown-Liste **Benutzeroberfläche** wählen. Der folgende Link wird auf der Anmeldeseite von Identity Applications angezeigt: **Klicken Sie hier, wenn Sie Ihren Benutzernamen oder Ihr Passwort vergessen haben oder wenn Sie sich registrieren müssen.**
6. Navigieren Sie zu **IDM SSO-Clients** > **Self Service Password Reset**.
7. Geben Sie unter **oAuth-Client-ID** den Namen an, mit dem sich der Single-Sign-On-Client für SSPR beim Authentifizierungsserver anmelden soll. Der Standardwert lautet `sspr`.
8. Geben Sie unter **oAuth-Client-Geheimnis** das Passwort des Single-Sign-On-Clients für SSPR an.
9. Geben Sie unter **URL für die oAuth-Umleitung** die absolute URL an, zur der der Authentifizierungsserver einen Browser-Client nach erfolgter Authentifizierung weiterleiten soll.

   Hierbei gilt das folgende Format: `Protokoll://Server:Port/Pfad`. Beispiel: `http://10.10.10.48:8180/sspr/public/oauth`.
10. Speichern Sie die Änderungen, und schließen Sie das Dienstprogramm.

Konfigurieren der Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung für OpenText Identity Manager

In diesem Abschnitt wird beschrieben, wie Sie SSPR für die Verwendung mit OpenText Identity Manager konfigurieren. Beispielsweise können Sie die Passwortrichtlinien und die Challenge-Response-Fragen bearbeiten.

Wenn Sie SSPR mit OpenText Identity Manager installiert haben, haben Sie ein Passwort angegeben, mit dem ein Administrator die Anwendung konfigurieren kann. Wir empfehlen, die SSPR-Einstellungen zu bearbeiten und dann ein Administratorkonto oder eine Gruppe festzulegen, die SSPR konfigurieren soll.

HINWEIS: Wenn Sie SSPR auf einem anderen Server installieren (also nicht auf dem Server der Benutzeranwendung), muss das SSPR-Anwendungszertifikat zu den `cacerts` der Benutzeranwendung hinzugefügt werden.

1. Melden Sie sich mit dem Konfigurationspasswort, das Sie während der Installation angegeben haben, bei SSPR an.
2. Bearbeiten Sie auf der Seite „Einstellungen“ die Einstellungen für die Passwortrichtlinie und die Challenge-Response-Fragen. Weitere Informationen zum Konfigurieren der Standardwerte für SSPR-Einstellungen finden Sie unter Configuring Self Service Password Reset (https://www.netiq.com/documentation/self-service-password-reset-41/adminguide/data/b14gnrxl.html) (Konfigurieren der Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung) im *Self Service Password Reset Administration Guide* (NetIQ-Administrationshandbuch für die Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung).
3. Sperren Sie die SSPR-Konfigurationsdatei (SSPR`Configuration.xml`). Weitere Informationen zum Sperren der Konfigurationsdatei finden Sie in „Sperren der SSPR-Konfiguration“, auf Seite 68.
4. (Optional) Sollen die SSPR-Einstellungen nach dem Sperren der Konfiguration bearbeitet werden, müssen Sie die Einstellung `configIsEditable` in der Datei SSPR`Configuration.xml` auf `true` setzen.
5. Melden Sie sich bei SSPR ab.
6. Starten Sie Tomcat neu, damit die Änderungen in Kraft treten.

Sperren der SSPR-Konfiguration

1. Gehen Sie zu der Adresse **http://<IP/DNS-Name>:<Port>/sspr**. Mit diesem Link gelangen Sie zum SSPR-Portal.
2. Melden Sie sich mit einem Administratorkonto oder mit Ihrer vorhandenen Anmeldeberechtigung bei OpenText Identity Manager an.
3. Klicken Sie oben auf der Seite auf **Konfigurationsmanager**, und geben Sie das Konfigurationspasswort an, das Sie während der Installation festgelegt haben.
4. Klicken Sie auf **Konfigurationseditor**, und navigieren Sie zu **Einstellungen > LDAP-Einstellungen**.
5. Sperren Sie die SSPR-Konfigurationsdatei (SSPR`Configuration.xml`).
   - **5a** Definieren Sie im Bereich der Administratorberechtigungen einen Filter im LDAP-Format für einen Benutzer oder eine Gruppe, die über Administratorrechte auf SSPR im Identitätsdepot verfügt. Standardmäßig ist der Filter auf `groupMembership=cn=Admins,ou=Groups,o=example` eingestellt.

     Für den Benutzeranwendungsadministrator geben Sie hier beispielsweise `uaadmin` (`cn=uaadmin`) an.

     Damit wird verhindert, dass die Benutzer die Konfiguration in SSPR verändern; dies kann nur der SSPR-Admin-Benutzer erledigen, der die uneingeschränkten Rechte zum Bearbeiten der Einstellungen besitzt.
   - **5b** Überprüfen Sie, ob die LDAP-Abfrage tatsächlich Ergebnisse zurückgibt. Klicken Sie hierzu auf **Übereinstimmungen anzeigen**.

Falls die Einstellung fehlerhaft ist, können Sie nicht mit der nächsten Konfigurationsoption fortfahren. Anhand der Fehlerdetails in SSPR können Sie die Fehlersuche vornehmen.

5c Klicken Sie auf **Speichern**.

5d Klicken Sie im Bestätigungsfenster auf **OK**.

Wenn SSPR gesperrt ist, stehen dem Admin-Benutzer zusätzliche Optionen in der Administrationsoberfläche zur Verfügung (z. B. Dashboard, Benutzeraktivität oder Datenanalyse), die vor dem Sperren von SSPR nicht verfügbar waren.

6 (Optional) Sollen die SSPR-Einstellungen nach dem Sperren der Konfiguration bearbeitet werden, müssen Sie die Einstellung `configIsEditable` in der Datei `SSPRConfiguration.xml` auf `true` setzen.

7 Melden Sie sich bei SSPR ab.

8 Melden Sie sich als der Admin-Benutzer, den Sie in Schritt 3 definiert haben, wieder bei SSPR an.

9 Klicken Sie auf **Konfiguration schließen**, und dann zum Bestätigen auf **OK**.

10 Starten Sie Tomcat neu, damit die Änderungen in Kraft treten.

Verwenden eines externen Systems für die „Passwort vergessen“-Verwaltung

Soll ein externes System verwendet werden, müssen Sie den Speicherort einer WAR-Datei mit der „Passwort vergessen“-Funktion angeben. Dieser Vorgang umfasst folgende Schritte:

- „Angeben einer externen WAR-Datei für die „Passwort vergessen“-Verwaltung“, auf Seite 69
- „Testen der externen „Passwort vergessen“-Konfiguration“, auf Seite 70
- „Konfigurieren der SSL-Kommunikation zwischen Anwendungsservern“, auf Seite 70

Angeben einer externen WAR-Datei für die „Passwort vergessen“-Verwaltung

Wenn Sie diese Werte nicht während der Installation angegeben haben und nun die Einstellungen bearbeiten möchten, verwenden Sie wahlweise das RBPM-Konfigurationsprogramm, oder nehmen Sie die Änderungen als Administrator in der Benutzeranwendung vor.

1 (Bedingt) Sollen die Einstellungen im RBPM-Konfigurationsprogramm bearbeitet werden, führen Sie die folgenden Schritte aus:

1a Melden Sie sich bei dem Server an, auf dem Sie Identity Applications installiert haben.

1b Führen Sie das RBPM-Konfigurationsprogramm aus. Weitere Informationen finden Sie unter Abschnitt 3, „Überblick über den Installations- und Konfigurationsvorgang“, auf Seite 43.

1c Navigieren Sie im Dienstprogramm zu **Authentifizierung > Passwortverwaltung**.

1d Wählen Sie unter **Passwortverwaltungsanbieter** die Option **Benutzeranwendung (alt)**.

2 (Bedingt) Sollen die Einstellungen in der Benutzeranwendung bearbeitet werden, führen Sie die folgenden Schritte aus:

   2a Melden Sie sich als Benutzeranwendungsadministrator an.

   2b Navigieren Sie zu **Administration > Anwendungskonfiguration > Setup des Passwortmoduls > Anmelden**.

3 Wählen Sie unter **Passwort vergessen** die Option **Extern**

4 Geben Sie unter **„Passwort vergessen“-Link** den Link an, der angezeigt werden soll, wenn der Benutzer auf der Anmeldeseite auf **Passwort vergessen** klickt. Sobald der Benutzer auf diesen Link klickt, leitet die Anwendung den Benutzer zum externen Passwortverwaltungssystem weiter. Beispiel:

   ```
   http://localhost:8180/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp
   ```

5 Geben Sie unter **Link zurück zu „Passwort vergessen“** den Link an, der angezeigt werden soll, wenn der Benutzer das „Passwort vergessen“-Verfahren abgeschlossen hat. Wenn der Benutzer auf diesen Link klickt, wird er auf den angegebenen Link umgeleitet. Beispiel:

   ```
   http://localhost/IDMProv
   ```

6 Geben Sie unter **Webservice-URL zu „Passwort vergessen“** die URL für den Webservice an, mit der die externe WAR-Datei für „Passwort vergessen“ Identity Applications aufruft. Verwenden Sie das folgende Format:

   ```
   https://idmhost:sslport/idm/pwdmgt/service
   ```

   Der Link zurück zu „Passwort vergessen“ muss SSL verwenden, sodass eine sichere Web-Service-Kommunikation mit den Identity Applications gewährleistet ist. Weitere Informationen finden Sie unter „Konfigurieren der SSL-Kommunikation zwischen Anwendungsservern“, auf Seite 70.

7 Kopieren Sie `ExternalPwd.war` manuell in den Bereitstellungsordner des Remote-JBoss-Servers, auf dem die Funktionalität der externen Passwort-WAR ausgeführt wird.

Testen der externen „Passwort vergessen“-Konfiguration

Wenn Sie eine externe Passwort-WAR-Datei verwenden und die „Passwort vergessen“-Funktion testen möchten, können Sie wie folgt auf sie zugreifen:

- Direkt, in einem Browser. Gehen Sie zu der Seite „Passwort vergessen“ in der externen Passwort-WAR-Datei. Beispiel: `http://localhost:8180/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp`.
- Klicken Sie auf der Anmeldeseite der Benutzeranwendung auf den Link **Passwort vergessen**.

Konfigurieren der SSL-Kommunikation zwischen Anwendungsservern

Wenn Sie mit einem externen Passwortverwaltungssystem arbeiten, müssen Sie die SSL-Kommunikation zwischen den Tomcat-Instanzen konfigurieren, auf denen Sie Identity Applications und die externe WAR-Datei für die „Passwort vergessen“-Verwaltung bereitstellen. Weitere Informationen finden Sie in der Tomcat-Dokumentation.

Aktualisieren der SSPR-Links im Dashboard für eine dezentrale Umgebung oder eine Cluster-Umgebung

Der Installationsvorgang setzt voraus, dass Sie SSPR auf demselben Anwendungsserver wie Identity Applications und Identity Reporting bereitstellen. Standardmäßig gilt für die integrierten Links auf der Seite **Anwendungen** im Dashboard ein relatives URL-Format, das auf SSPR auf dem lokalen System verweist. Beispiel: `\sspr\private\changepassword`. Wenn Sie die Anwendungen in einer dezentralen Umgebung oder einer Cluster-Umgebung installieren, müssen Sie die URLs für die SSPR-Links entsprechend aktualisieren.

Weitere Informationen finden Sie in der *Hilfe zu den Identity Applications*.

1. Melden Sie sich beim Dashboard als Administrator an. Melden Sie sich beispielsweise als `uaadmin` an.
2. Klicken Sie auf **Bearbeiten**.
3. Zeigen Sie auf der Seite „Startseitenelemente bearbeiten“ auf das zu aktualisierende Element, und klicken Sie auf das Bearbeitungssymbol. Wählen Sie beispielsweise **Passwort ändern**.
4. Geben Sie unter **Link** die absolute URL an. Beispiel: `http://10.10.10.48:8180/sspr/changepassword`.
5. Klicken Sie auf **Speichern**.
6. Wiederholen Sie diesen Vorgang für alle zu aktualisierenden SSPR-Links.
7. Klicken Sie abschließend auf **Fertig**.
8. Melden Sie sich ab, melden Sie sich dann als normaler Benutzer wieder an, und testen Sie die Änderungen.

Konfigurieren der Datenbank für Identity Applications

Die Datenbank für Identity Applications unterstützt beispielsweise das Speichern der Konfigurationsdaten oder der Daten für Workflow-Aufgaben. Vor dem Installieren der Anwendungen muss die Datenbank installiert und konfiguriert sein. Weitere Informationen zu unterstützten Datenbanken finden Sie auf der Seite der Identity Manager-Systemanforderungen (https://www.netiq.com/documentation/identity-manager-4.10/).

HINWEIS: Wenn Sie auf eine neue Version des RBPM und der Identity Applications migrieren, müssen Sie dieselbe Datenbank verwenden wie in der bisherigen Installation. (Dies ist die Installation, von der aus Sie die Migration vornehmen.)

- „Konfigurieren einer Oracle-Datenbank“, auf Seite 71
- „Konfigurieren einer SQL Server-Datenbank“, auf Seite 73

Konfigurieren einer Oracle-Datenbank

In diesem Abschnitt finden Sie die Konfigurationsoptionen zur Verwendung einer Oracle-Datenbank für die Benutzeranwendung. Informationen zu unterstützten Versionen unter Oracle finden Sie auf der Website der technischen Daten zu OpenText Identity Manager (https://www.netiq.com/Support/identity-manager/SP_IDM_Components.asp).

Prüfen der Kompatibilitätsstufe der Datenbanken

Datenbanken aus verschiedenen Oracle-Versionen sind kompatibel, wenn Sie dieselben Funktionen unterstützen und diese Funktionen auf dieselbe Weise ausgeführt werden. Wenn sie nicht kompatibel sind, funktionieren bestimmte Funktionen oder Vorgänge möglicherweise nicht erwartungsgemäß. Beispielsweise wird das Schema nicht erstellt und Identity Applications werden nicht bereitgestellt.

Führen Sie die folgenden Schritte aus, um die Kompatibilitätsstufe Ihrer Datenbank zu prüfen:

1. Aufbauen einer Verbindung zur Datenbank-Engine.
2. Nach dem Aufbau einer Verbindung zur entsprechenden Instanz der SQL-Serverdatenbank-Engine klicken Sie unter **Object Explorer** auf den Servernamen.
3. Erweitern Sie **Datenbanken** und wählen Sie abhängig von der Datenbank entweder eine Benutzerdatenbank oder erweitern Sie **Systemdatenbanken** und wählen Sie eine Systemdatenbank aus.
4. Klicken Sie mit der rechten Maustaste auf die Datenbank und klicken Sie dann auf **Eigenschaften**.

   Das Dialogfeld **Datenbankeigenschaften** wird geöffnet.
5. Klicken Sie im Bereich **Seite auswählen** auf **Optionen**.

   Die aktuelle Kompatibilitätsstufe wird im Listenfeld **Kompatibilitätsstufe** angezeigt.
6. Geben Sie zur Prüfung der **Kompatibilitätsstufe** Nachfolgendes im Abfragefenster ein und klicken Sie auf **Ausführen**.

   ```
   SQL> SELECT name, value FROM v$parameter
   WHERE name = 'compatible';
   ```

Die erwartete Ausgabe ist: 12.2.0.1

Konfigurieren des Zeichensatzes

Die Benutzeranwendungsdatenbank muss einen Zeichensatz mit Unicode-Kodierung nutzen. Legen Sie diesen Zeichensatz beim Erstellen der Datenbank mit der Option AL32UTF8 fest.

Überprüfen Sie mit dem folgenden Befehl, ob der UTF-8-Zeichensatz für eine Oracle 12c-Datenbank festgelegt ist:

```
select * from nls_database_parameters;
```

Wenn die Datenbank nicht für UTF-8 konfiguriert ist, gibt das System die folgenden Informationen zurück:

```
NLS_CHARACTERSET
WE8MSWIN1252
```

Ansonsten gibt das System die folgenden Informationen zurück, mit denen bestätigt wird, dass die Datenbank für UTF-8 konfiguriert ist:

```
NLS_CHARACTERSET
AL32UTF8
```

HINWEIS: Die JDBC-JAR-Version `ojdbc6.jar` wird empfohlen.

Weitere Informationen zum Konfigurieren eines Zeichensatzes finden Sie unter „Choosing an Oracle Database Character Set“ (Auswählen eines Zeichensatzes für eine Oracle-Datenbank).

Konfigurieren des Admin-Benutzerkontos

Die Benutzeranwendung setzt voraus, dass das Benutzerkonto für die Oracle-Datenbank bestimmte Rechte besitzt. Geben Sie die folgenden Befehle im SQL Plus-Dienstprogramm ein:

```
CREATE USER idmuser IDENTIFIED BY password
GRANT CONNECT, RESOURCE to idmuser
ALTER USER idmuser quota 100M on USERS;
```

Hierbei gilt: *`idmuser`* steht für das Benutzerkonto.

Konfigurieren einer SQL Server-Datenbank

In diesem Abschnitt finden Sie die Konfigurationsoptionen zur Verwendung einer SQL Server-Datenbank für die Benutzeranwendung. Informationen zu unterstützten Versionen des SQL-Servers finden Sie auf der Website der technischen Daten zu OpenText Identity Manager (https://www.netiq.com/Support/identity-manager/SP_IDM_Components.asp).

Konfigurieren des Zeichensatzes

Bei SQL Server ist es nicht möglich, den Zeichensatz für Datenbanken auszuwählen. Die Benutzeranwendung speichert SQL Server-Zeichendaten als NCHAR-Spaltentyp, der UTF-8 unterstützt.

HINWEIS: Die einzige unterstützte Sortierung für SQL ist SQL_Latin1_General_CP1_CI_AS.

Konfigurieren des Admin-Benutzerkontos

Erstellen Sie nach dem Installieren einer unterstützten Version von Microsoft SQL Server mit einer Anwendung wie SQL Server Management Studio eine Datenbank und einen Datenbankbenutzer. Das Datenbankbenutzerkonto muss die folgenden Rechte aufweisen:

- `CREATE TABLE`
- `DELETE`
- `INSERT`
- `SELECT`
- `UPDATE`

HINWEIS: Es wird empfohlen, die JDBC JAR-Version `sqljdbc4.jar` für Microsoft SQL Server 2014 und `mssql-jdbc-9.2.1.jre8.jar` für Microsoft SQL Server 2016 zu verwenden.

Konfigurieren von Identity Applications

- „Konfigurieren der Einstellungen für Identity Applications“, auf Seite 74
- „Bereitstellen von REST-APIs für Identity Applications“, auf Seite 98
- „Zugreifen auf die Oracle-Datenbank anhand des Oracle-Service-Namens“, auf Seite 99
- „Manuelles Erstellen der Datenbank“, auf Seite 99
- „Konfigurieren der Single Sign-on-Einstellungen für Identity Applications“, auf Seite 101
- „Starten der Identity Applications“, auf Seite 102
- „Überlegungen zur Konfiguration und Nutzung der Identity Applications“, auf Seite 102

Konfigurieren der Einstellungen für Identity Applications

Mit dem Konfigurationsprogramm für Identity Applications verwalten Sie die Einstellungen für die Benutzeranwendungstreiber und Identity Applications. Das Installationsprogramm für Identity Applications ruft eine Version dieses Dienstprogramms auf, sodass Sie die Anwendungen rascher konfigurieren können. Den Großteil dieser Einstellungen können Sie außerdem auch nach der Installation noch bearbeiten.

Die Datei, die für das Ausführen des Konfigurationsdienstprogramms benötigt wird (`configupdate.bat`), befindet sich standardmäßig in einem Installationsverzeichnis für Identity Applications (`C:\NetIQ\idm\apps\UserApplication`).

HINWEIS: In einem Cluster müssen die Konfigurationseinstellungen für alle Mitglieder des Clusters identisch sein. Kopieren Sie `ism-sensitive.properties`, `ism-configuration.properties` und `encrypt-keys.pkcs12` vom primären Knoten auf alle Knoten der Benutzeranwendungen.

In diesem Abschnitt werden die Einstellungen im Konfigurationsprogramm erläutert. Die Einstellungen sind in Registerkarten angeordnet. Wenn Sie Identity Reporting installieren, werden dabei Parameter für die Berichterstellung zu diesem Dienstprogramm hinzugefügt.

- „Ausführen des Konfigurationsprogramms der Identity Applications“, auf Seite 74
- „Speichern des Passworts für das Configupdate-Dienstprogramm (Optional)“, auf Seite 75
- „Parameter für Benutzeranwendung“, auf Seite 75
- „Parameter für die Berichterstellung“, auf Seite 87
- „Parameter für Authentifizierung“, auf Seite 89
- „Parameter für SSO-Clients“, auf Seite 93
- „CEF-Revisionsparameter“, auf Seite 98

Ausführen des Konfigurationsprogramms der Identity Applications

1 Öffnen Sie die Datei `configupdate.properties` in einem Texteditor und stellen Sie sicher, dass folgende Optionen konfiguriert sind:

```
edit_admin="true"

use_console="false"
```

2 Führen Sie mithilfe der Eingabeaufforderung das Konfigurationsdienstprogramm (`configupdate.bat`) aus.

HINWEIS: Unter Umständen dauert das Starten des Dienstprogramms mehrere Minuten.

HINWEIS: Da Identity Manager kein NAM OAuth unterstützt, verwenden Sie nicht die Option **OpenText Access Manager ist der OAuth-Anbieter** auf der Registerkarte "Authentifizierungsserver" des Konfigurationsprogramms.

Speichern des Passworts für das Configupdate-Dienstprogramm (Optional)

Beim Starten von „configupdate“ wird der Benutzer aufgefordert, das Master-Keystore-Passwort (encrypt-keys.pkcs12) unter `C:\NetIQ\IDM\apps\tomcat\conf` einzugeben. Der verschlüsselte Wert dieses Passworts wird in der Datei `ism-sensitive.properties gespeichert, die sich in C:\NetIQ\IDM\apps\tomcat\conf befindet`. Wenn Sie das Passwort für den Master-Keystore mit dem Keytool-Befehl ändern möchten, muss es verschlüsselt und in `ism-sensitive.properties` aktualisiert werden.

Führen Sie die folgenden Schritte aus, um das Passwort zu ändern und zu verschlüsseln:

1. Führen Sie in der Eingabeaufforderung den folgenden Befehl aus, um Ihr Passwort für das Configupdate-Dienstprogramm zu ändern:

   ```
   keytool -storepasswd -new <new master keystore password> -keystore
   C:\NetIQ\IDM\apps\tomcat\conf\encrypt-keys.pkcs12 -storepass -storetype
   PKCS12
   ```

2. Führen Sie zum Verschlüsseln des neuen Passworts den folgenden Befehl aus:

   ```
   C:\NetIQ\Common\JRE\bin\java -cp
   C:\NetIQ\IDM\apps\tomcat\lib\obscurity-<version>-uber.jar
   com.netiq.ism.obfuscate.server.util.PasswordObfuscator <new master
   keystore password>
   ```

3. Achten Sie darauf, das verschlüsselte Passwort zu speichern, indem Sie den Wert für `com.microfocus.ism.master-storepass` in der Datei `ism-sensitive.properties` am Speicherort `C:\NetIQ\IDM\apps\tomcat\conf` ändern.

Parameter für Benutzeranwendung

Beim Konfigurieren der Identity Applications definieren Sie auf dieser Registerkarte die Werte, mit denen die Anwendungen mit dem Identitätsdepot kommunizieren. Einige Einstellungen sind erforderlich, damit der Installationsvorgang abgeschlossen werden kann.

Standardmäßig werden auf dieser Registerkarte nur die grundlegenden Optionen angezeigt. Mit **Erweiterte Optionen anzeigen** lassen Sie alle Einstellungen einblenden. Diese Registerkarte umfasst die folgenden Gruppen von Einstellungen:

- „Identitätsdepoteinstellungen“, auf Seite 76
- „Identitätsdepot-DNs“, auf Seite 77
- „Identitätsdepot-Benutzeridentität“, auf Seite 80

- „Identitätsdepot-Benutzergruppen“, auf Seite 81
- „Identitätsdepot-Zertifikate“, auf Seite 82
- „Email-Serverkonfiguration“, auf Seite 82
- „Speicher für Herkunftsverbürgungsschlüssel“, auf Seite 84
- „Zertifikat und Schlüssel für NetIQ Sentinel-Digitalsignatur“, auf Seite 85
- „Sonstige“, auf Seite 85
- „Containerobjekt“, auf Seite 87

Identitätsdepoteinstellungen

In diesem Abschnitt werden die Einstellungen für den Zugriff der Identity Applications auf die Identitäten und Rollen der Benutzer im Identitätsdepot definiert. Einige Einstellungen sind erforderlich, damit der Installationsvorgang abgeschlossen werden kann.

Identitätsdepot-Server

Erforderlich

Gibt den Hostnamen oder die IP-Adresse des LDAP-Servers an. Beispiel: `meinLDAPHost`.

LDAP-Port

Gibt den Port an, den das Identitätsdepot auf LDAP-Anforderungen im Klartext überwachen soll. Der Standardwert ist 389.

Sicherer LDAP-Port

Gibt den Port an, den das Identitätsdepot mit dem SSL-Protokoll (Secure Sockets Layer) auf LDAP-Anforderungen überwachen soll. Der Standardwert ist 636.

Wenn ein Dienst, der bereits vor der Installation von OpenText eDirectory auf dem Server geladen war, den Port nutzt, müssen Sie einen anderen Port angeben.

Identitätsdepot-Administrator

Erforderlich

Gibt den Berechtigungsnachweis für den LDAP-Administrator an. Beispielsweise `cn=admin`. Dieser Benutzer muss bereits im Identitätsdepot vorhanden sein.

Über dieses Konto stellen Identity Applications eine administrative Verbindung zum Identitätsdepot her. Dieser Wert ist mit dem Master-Schlüssel verschlüsselt.

Identitätsdepot-Administratorpasswort

Erforderlich

Gibt das Passwort für den LDAP-Administrator an. Dieses Passwort ist mit dem Master-Schlüssel verschlüsselt.

Öffentliches anonymes Konto verwenden

Gibt an, ob nicht angemeldete Benutzer auf das öffentliche anonyme LDAP-Konto zugreifen dürfen.

Sichere Administratorverbindung

Gibt an, ob RBPM die gesamte Kommunikation über das Admin-Konto mit dem SSL-Protokoll vornehmen soll. Mit dieser Einstellung wird es möglich, andere Vorgänge, für die kein SSL erforderlich ist, tatsächlich ohne SSL durchzuführen.

HINWEIS: Diese Option kann die Leistung unter Umständen beeinträchtigen.

Sichere Benutzerverbindung

Gibt an, ob RBPM die gesamte Kommunikation über das Konto des angemeldeten Benutzers mit dem TLS/SSL-Protokoll vornehmen soll. Mit dieser Einstellung wird es möglich, andere Vorgänge, für die kein TLS/SSL erforderlich ist, tatsächlich ohne TLS/SSL durchzuführen.

HINWEIS: Diese Option kann die Leistung unter Umständen beeinträchtigen.

Identitätsdepot-DNs

In diesem Abschnitt werden die eindeutigen Namen der Container und Benutzerkonten definiert, die die Kommunikation zwischen den Identity Applications und anderen OpenText Identity Manager-Komponenten ermöglichen. Einige Einstellungen sind erforderlich, damit der Installationsvorgang abgeschlossen werden kann.

Stammcontainer-DN

Erforderlich

Gibt den eindeutigen LDAP-Namen des Stammcontainers an. Diese Angabe wird als Standard-Suchstamm der Entitätsdefinition verwendet, sofern in der Verzeichnisabstraktionsschicht kein Suchstamm angegeben wurde. Beispiel:·o=meinefirma.

Benutzer-Container-DN

Erforderlich

Wenn die erweiterten Optionen eingeblendet sind, wird dieser Parameter unter „Identitätsdepot-Benutzeridentität“ aufgeführt.

Gibt den eindeutigen LDAP-Namen (DN) oder den vollständig qualifizierten LDAP-Namen des Benutzer-Containers an. Bei dieser Einstellung sind die folgenden Überlegungen zu beachten:

- Benutzer in diesem Container (und unterhalb) dürfen sich bei den Identity Applications anmelden.
- Wenn Sie Tomcat, auf dem Identity Applications gehostet werden, bereits gestartet haben, können Sie diese Einstellung nicht mithilfe der Datei `configupdate.bat` ändern.
- Der Benutzeranwendungsadministrator, den Sie beim Einrichten des Benutzeranwendungstreibers angegeben haben, muss sich in diesem Container befinden. Ansonsten kann das angegebene Konto keine Workflows ausführen.

Gruppencontainer-DN

Erforderlich

Wenn die erweiterten Optionen eingeblendet sind, wird dieser Parameter unter „Identitätsdepot-Benutzergruppen“ aufgeführt.

Gibt den eindeutigen LDAP-Namen (DN) oder den vollständig qualifizierten LDAP-Namen des Gruppencontainers an. Bei dieser Einstellung sind die folgenden Überlegungen zu beachten:

- Dieser DN wird von Entitätsdefinitionen in der Verzeichnisabstraktionsschicht genutzt.
- Wenn Sie Tomcat, auf dem Identity Applications gehostet werden, bereits gestartet haben, können Sie diese Einstellung nicht mithilfe der Datei `configupdate.bat` ändern.

Benutzeranwendungstreiber

Erforderlich

Gibt den eindeutigen Namen für den Benutzeranwendungstreiber an.

Wenn Sie beispielsweise den Treiber „UserApplicationDriver“ und den Treibersatz „meinTreibersatz“ verwenden, der sich im Kontext „o=meineFirma“, befindet, geben Sie entsprechend `cn=UserApplicationDriver,cn=meinTreibersatz,o=meineFirma` an.

Benutzeranwendungsadministrator

Erforderlich

Gibt an, dass ein vorhandenes Benutzerkonto im Identitätsdepot berechtigt ist, administrative Tätigkeiten für den in der Benutzeranwendung angegebenen Benutzer-Container auszuführen. Bei dieser Einstellung sind die folgenden Überlegungen zu beachten:

- Wenn Sie Tomcat, auf dem die Benutzeranwendung gehostet wird, bereits gestartet haben, können Sie diese Einstellung nicht mithilfe der Datei `configupdate.bat` ändern.
- Diese Zuweisung kann nach dem Bereitstellen der Benutzeranwendung über die Seiten **Administration > Sicherheit** in der Benutzeranwendung geändert werden.
- Dieses Benutzerkonto ist berechtigt, das Portal über die Registerkarte **Administration** in der Benutzeranwendung zu verwalten.
- Wenn der Benutzeranwendungsadministrator Aufgaben zur Workflow-Administration bearbeitet, die in Designer oder der Benutzeranwendung (Registerkarte **Anforderungen und Genehmigungen**) aufgeführt sind, müssen Sie dem entsprechenden Administrator ausreichende Trustee-Rechte auf die Objektinstanzen im Benutzeranwendungstreiber gewähren. Weitere Informationen finden Sie im *User Application Administration Guide* (Benutzeranwendung: Administrationshandbuch).

Bereitstellungsadministrator

Gibt ein vorhandenes Benutzerkonto im Identitätsdepot an, das die in der gesamten Benutzeranwendung verfügbaren Bereitstellungs-Workflow-Funktionen verwalten soll.

Sie können diese Zuweisung nach dem Bereitstellen der Benutzeranwendung über die Seite **Verwaltung > Administratorzuweisung** in der Benutzeranwendung ändern.

Konformitätsadministrator

Gibt ein vorhandenes Konto im Identitätsdepot an, das eine Systemrolle übernimmt und so den Mitgliedern das Ausführen aller Funktionen auf der Registerkarte **Konformität** ermöglicht. Bei dieser Einstellung sind die folgenden Überlegungen zu beachten:

- Sie können diese Zuweisung nach dem Bereitstellen der Identity Applications über die Seite **Verwaltung > Administratorzuweisung** in der Benutzeranwendung ändern.
- Bei einer Aktualisierung der Konfiguration treten Änderungen an diesem Wert nur dann in Kraft, wenn kein gültiger Konformitätsadministrator zugewiesen wurde. Wenn ein gültiger Konformitätsadministrator existiert, werden Ihre Änderungen nicht gespeichert.

Rollenadministrator

Gibt die Rolle an, mit der die Mitglieder alle Rollen erstellen, entfernen oder bearbeiten sowie Rollenzuweisungen zu Benutzern, Gruppen oder Containern gewähren oder zurückziehen können. Außerdem können die Rollenmitglieder damit einen Bericht für einen beliebigen Benutzer ausführen. Bei dieser Einstellung sind die folgenden Überlegungen zu beachten:

- Standardmäßig wird diese Rolle dem Benutzeranwendungsadministrator zugewiesen.
- Sie können diese Zuweisung nach dem Bereitstellen der Identity Applications über die Seite **Verwaltung > Administratorzuweisung** in der Benutzeranwendung ändern.
- Bei einer Aktualisierung der Konfiguration treten Änderungen an diesem Wert nur dann in Kraft, wenn kein gültiger Rollenadministrator zugewiesen wurde. Wenn ein gültiger Rollenadministrator existiert, werden Ihre Änderungen nicht gespeichert.

Sicherheitsadministrator

Gibt die Rolle an, mit der die Mitglieder sämtliche Funktionen innerhalb der Sicherheitsdomäne nutzen können. Bei dieser Einstellung sind die folgenden Überlegungen zu beachten:

- Der Sicherheitsadministrator kann für alle Objekte alle möglichen Aktionen innerhalb der Sicherheitsdomäne durchführen. Mit der Sicherheitsdomäne ist der Sicherheitsadministrator in der Lage, Zugriffsberechtigungen für alle Objekte in allen Domänen innerhalb des RBPM zu konfigurieren. Der Sicherheitsadministrator kann Teams konfigurieren sowie Domänenadministratoren, beauftragte Administratoren und andere Sicherheitsadministratoren zuweisen.
- Sie können diese Zuweisung nach dem Bereitstellen der Identity Applications über die Seite **Verwaltung > Administratorzuweisung** in der Benutzeranwendung ändern.

Ressourcenadministrator

Gibt die Rolle an, mit der die Mitglieder sämtliche Funktionen innerhalb der Ressourcendomäne nutzen können. Bei dieser Einstellung sind die folgenden Überlegungen zu beachten:

- Der Ressourcenadministrator kann für alle Objekte alle möglichen Aktionen innerhalb der Ressourcendomäne durchführen.
- Sie können diese Zuweisung nach dem Bereitstellen der Identity Applications über die Seite **Verwaltung > Administratorzuweisung** in der Benutzeranwendung ändern.

RBPM-Konfigurationsadministrator

Gibt die Rolle an, mit der die Mitglieder sämtliche Funktionen innerhalb der Konfigurationsdomäne nutzen können. Bei dieser Einstellung sind die folgenden Überlegungen zu beachten:

- Der RBPM-Konfigurationsadministrator kann für alle Objekte alle möglichen Aktionen innerhalb der Konfigurationsdomäne durchführen. Der RBPM-Konfigurationsadministrator steuert den Zugriff auf Navigationselemente innerhalb des RBPM. Außerdem konfiguriert der RBPM-Konfigurationsadministrator den Delegierungs- und Vertretungsservice, die Bereitstellungsbenutzeroberfläche und die Workflow-Engine.
- Sie können diese Zuweisung nach dem Bereitstellen der Identity Applications über die Seite **Verwaltung > Administratorzuweisung** in der Benutzeranwendung ändern.

RBPM-Berichtsadministrator

Gibt den Berichtsadministrator an. Das Installationsprogramm setzt diesen Wert standardmäßig auf denselben Benutzer wie die anderen Sicherheitsfelder.

Identitätsdepot-Benutzeridentität

In diesem Abschnitt werden die Einstellungen für die Kommunikation der Identity Applications mit einem Benutzer-Container im Identitätsdepot definiert. Einige Einstellungen sind erforderlich, damit der Installationsvorgang abgeschlossen werden kann.

Diese Einstellungen werden nur dann im Dienstprogramm angezeigt, wenn die Option **Erweiterte Optionen anzeigen** aktiviert ist.

Benutzer-Container-DN

Erforderlich

Wenn die erweiterten Optionen ausgeblendet sind, wird dieser Parameter unter „Identitätsdepot-DNs“ aufgeführt.

Gibt den eindeutigen LDAP-Namen (DN) oder den vollständig qualifizierten LDAP-Namen des Benutzer-Containers an. Bei dieser Einstellung sind die folgenden Überlegungen zu beachten:

- Benutzer in diesem Container (und unterhalb) dürfen sich bei den Identity Applications anmelden.
- Wenn Sie Tomcat, auf dem Identity Applications gehostet werden, bereits gestartet haben, können Sie diese Einstellung nicht mithilfe der Datei `configupdate.bat` ändern.
- Der Benutzeranwendungsadministrator, den Sie beim Einrichten des Benutzeranwendungstreibers angegeben haben, muss sich in diesem Container befinden. Ansonsten kann das angegebene Konto keine Workflows ausführen.

Benutzersuchbereich

Gibt die Tiefe des Bereichs an, den die Identitätsdepotbenutzer nach dem Container durchsuchen können.

Benutzerobjektklasse

Gibt die Objektklasse des LDAP-Benutzers an. In der Regel lautet die Klasse `inetOrgPerson`.

Anmeldeattribut

Gibt das LDAP-Attribut für den Anmeldenamen des Benutzers an. Beispiel: `CN`.

Benennungsattribut

Gibt das LDAP-Attribut an, das beim Nachschlagen von Benutzern oder Gruppen als ID fungiert. Dieses Attribut ist nicht identisch mit dem Anmeldeattribut, das nur für die Anmeldung verwendet wird. Beispiel: CN.

Benutzermitgliedschaftsattribut

(Optional) Gibt das LDAP-Attribut für die Gruppenmitgliedschaft des Benutzers an. Der Name darf keine Leerzeichen enthalten.

Identitätsdepot-Benutzergruppen

In diesem Abschnitt werden die Einstellungen für die Kommunikation der Identity Applications mit einem Gruppencontainer im Identitätsdepot definiert. Einige Einstellungen sind erforderlich, damit der Installationsvorgang abgeschlossen werden kann.

Diese Einstellungen werden nur dann im Dienstprogramm angezeigt, wenn die Option **Erweiterte Optionen anzeigen** aktiviert ist.

Gruppencontainer-DN

Erforderlich

Wenn die erweiterten Optionen ausgeblendet sind, wird dieser Parameter unter „Identitätsdepot-DNs“ aufgeführt.

Gibt den eindeutigen LDAP-Namen (DN) oder den vollständig qualifizierten LDAP-Namen des Gruppencontainers an. Bei dieser Einstellung sind die folgenden Überlegungen zu beachten:

- Dieser DN wird von Entitätsdefinitionen in der Verzeichnisabstraktionsschicht genutzt.
- Wenn Sie Tomcat, auf dem Identity Applications gehostet werden, bereits gestartet haben, können Sie diese Einstellung nicht mithilfe der Datei `configupdate.bat` ändern.

Gruppencontainerbereich

Gibt die Tiefe des Bereichs an, den die Identitätsdepotbenutzer nach dem Gruppencontainer durchsuchen können.

Gruppenobjektklasse

Gibt die Objektklasse der LDAP-Gruppe an. In der Regel lautet die Klasse `groupofNames`.

Gruppenmitgliedschaftsattribut

(Optional) Gibt die Gruppenmitgliedschaft des Benutzers an. Der Name darf keine Leerzeichen enthalten.

Dynamische Gruppen verwenden

Gibt an, ob dynamische Gruppen verwendet werden sollen.

Sie müssen außerdem einen Wert für **Klasse für dynamisches Gruppenobjekt** angeben.

Klasse für dynamisches Gruppenobjekt

Gilt nur dann, wenn Sie die Option **Dynamische Gruppen verwenden** *wählen.*

Gibt die Objektklasse der dynamischen LDAP-Gruppe an. In der Regel lautet die Klasse `dynamicGroup`.

Identitätsdepot-Zertifikate

In diesem Abschnitt werden der Pfad und das Passwort für den JRE-Keystore definiert. Einige Einstellungen sind erforderlich, damit der Installationsvorgang abgeschlossen werden kann.

Keystore-Pfad

Erforderlich

Gibt den vollständigen Pfad zur Keystore-Datei (`cacerts`) der JRE an, mit der Tomcat ausgeführt wird. Sie können den Pfad manuell eingeben oder zur Datei `cacerts` navigieren. Bei dieser Einstellung sind die folgenden Überlegungen zu beachten:

- In Umgebungen müssen Sie das RBPM-Installationsverzeichnis angeben. Der Standardwert ist auf den richtigen Speicherort gesetzt.
- Die Keystore-Datei wird vom Installationsprogramm für Identity Applications bearbeitet.

Keystore-Passwort

Erforderlich

Gibt das Passwort für die Keystore-Datei an. Die Vorgabe ist `changeit`.

Email-Serverkonfiguration

In diesem Abschnitt werden die Werte definiert, die Email-Benachrichtigungen aktivieren; sie stehen für Email-basierten Genehmigungen zur Verfügung. Weitere Informationen finden Sie im *OpenText™ Identity Manager CE 24.4 (v4.10) – Administratorhandbuch zu Identity Applications*.

Benachrichtigungsschablonen-Host

Gibt den Namen oder die IP-Adresse von Tomcat an, auf dem Identity Applications gehostet werden. Beispiel: `meinAnwendungsserverServer`.

Dieser Wert ersetzt das $HOST$-Token in Email-Schablonen. Das Installationsprogramm erstellt aus diesen Angaben eine URL zu den Bereitstellungsanforderungsaufgaben und den Benachrichtigungen über Bereitstellungsgenehmigungen.

Benachrichtigungsschablonen-Port

Gibt die Port-Nummer von Tomcat an, auf dem Identity Applications gehostet werden.

Dieser Wert ersetzt das $PORT$-Token in Email-Schablonen, die für Bereitstellungsanforderungsaufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden.

Sicherer Benachrichtigungsschablonen-Port

Gibt die Nummer des sicheren Ports von Tomcat an, auf dem Identity Applications gehostet werden.

Dieser Wert ersetzt das $SECURE_PORT$-Token in Email-Schablonen, die für Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden.

Benachrichtigungsschablonenprotokoll

Gibt ein nicht sicheres Protokoll in der URL beim Versenden von Benutzer-Emails an. Beispiel: `http`.

Dieser Wert ersetzt das $PROTOCOL$-Token in Email-Schablonen, die für Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden.

Sicheres Benachrichtigungsschablonenprotokoll

Gibt das nicht sichere Protokoll in der URL beim Versenden von Benutzer-Emails an. Beispiel: `https`.

Dieser Wert ersetzt das $SECURE_PROTOCOL$-Token in Email-Schablonen, die für Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden.

Benachrichtigungs-SMTP-Email von

Gibt das Email-Konto an, von dem aus Identity Applications die Email-Benachrichtigungen senden.

SMTP-Servername

Gibt die IP-Adresse oder den DNS-Namen des SMTP-Email-Hosts an, den Identity Applications für Bereitstellungs-Emails verwenden. Verwenden Sie nicht `localhost`.

Für den Server ist eine Authentifizierung erforderlich

Gibt an, ob für den Server eine Authentifizierung erforderlich sein soll.

Sie müssen außerdem den Berechtigungsnachweis für den Email-Server angeben.

Benutzername

Gilt nur dann, wenn Sie die Option **Für den Server ist eine Authentifizierung erforderlich** *aktivieren.*

Gibt den Namen eines Anmeldekontos für den Email-Server an.

Passwort

Gilt nur dann, wenn Sie die Option **Für den Server ist eine Authentifizierung erforderlich** *aktivieren.*

Gibt das Passwort des Anmeldekontos für den Email-Server an.

SMTP-TLS verwenden

Gibt an, ob der Inhalt von Email-Nachrichten bei der Übertragung zwischen Mailservern gesichert werden soll.

Speicherort des Email-Benachrichtigungsbilds

Gibt den Pfad zum Image an, das in Email-Benachrichtigungen gesendet werden soll.

Wenn sowohl der Identity Applications-Server als auch der E-Mail-Server auf die Verwendung einer sicheren Verbindung festgelegt sind, müssen folgende Bedingungen erfüllt sein:

- Das Zertifikat, das zum Aufbau einer sicheren Verbindung zwischen dem Identity Applications-Server und dem E-Mail-Server verwendet wird, ist ein vertrauenswürdiges Zertifikat einer Zertifizierungsstelle.
- Verwenden Sie `https` im Image-Pfad. Beispiel: `https://localhost:8543/IDMProv/images`

Wenn Identity Applications auf einem Server betrieben wird, der HTTP für die Klartextkommunikation verwendet, ersetzen Sie im Image-Pfad `https` durch `http`. Beispiel für den Image-Pfad: `http://localhost:8080/IDMProv/images`

Email signieren

Gibt an, ob ausgehenden Nachrichten eine digitale Signatur hinzugefügt werden soll.

Wenn Sie diese Option aktivieren, müssen Sie auch Einstellungen für den Keystore und den Signaturschlüssel angeben.

Keystore-Pfad

Gilt nur, wenn Sie die Option **E-Mail signieren** *aktivieren.*

Gibt den vollständigen Pfad zur Keystore-Datei (`cacerts`) an, die für digitale Signaturen für E-Mails verwendet werden sollen. Sie können den Pfad manuell eingeben oder zur Datei `cacerts` navigieren.

Beispiel: `C:\NetIQ\idm\apps\jre\lib\security\cacerts`.

Keystore-Passwort

Gilt nur, wenn Sie die Option **E-Mail signieren** *aktivieren.*

Gibt das Passwort für die Keystore-Datei an. Beispiel: `changeit`.

Alias des Signaturschlüssels

Gilt nur, wenn Sie die Option **E-Mail signieren** *aktivieren.*

Gibt das Alias für den Signaturschlüssel im Keystore an. Beispiel: `idmapptest`.

Signaturschlüsselpasswort

Gilt nur, wenn Sie die Option **E-Mail signieren** *aktivieren.*

Gibt das Passwort an, das die Datei mit dem Signaturschlüssel schützt. Beispiel: `changeit`.

Speicher für Herkunftsverbürgungsschlüssel

In diesem Abschnitt werden die Werte für den Speicher für Herkunftsverbürgungsschlüssel für Identity Applications definiert. Diese Einstellungen werden nur dann im Dienstprogramm angezeigt, wenn die Option **Erweiterte Optionen anzeigen** aktiviert ist.

Pfad für Herkunftsverbürgungsspeicher

Gibt den Speicher für Herkunftsverbürgungsschlüssel an, der alle verbürgten Zertifikate der Signierer enthält. Wurde kein Pfad angegeben, rufen Identity Applications den Pfad von der Systemeigenschaft `javax.net.ssl.trustStore` ab. Wenn die Systemeigenschaft keinen Pfad enthält, verwendet das Installationsprogramm standardmäßig den Wert `jre\lib\security\cacerts`.

Passwort für Herkunftsverbürgungsspeicher

Gibt das Passwort für den Speicher für Herkunftsverbürgungsschlüssel an. Wurde kein Passwort angegeben, rufen Identity Applications das Passwort von der Systemeigenschaft `javax.net.ssl.trustStorePassword` ab. Wenn die Systemeigenschaft keinen Pfad enthält, verwendet das Installationsprogramm standardmäßig den Wert `changeit`.

Dieses Passwort ist mit dem Master-Schlüssel verschlüsselt.

Typ des Herkunftsverbürgungsspeichers

Gibt an, ob der Pfad des Herkunftsverbürgungsspeichers mit einem Java-Keystore (JKS) oder mit PKCS12 digital signiert wird.

Zertifikat und Schlüssel für NetIQ Sentinel-Digitalsignatur

In diesem Abschnitt werden die Werte für die Kommunikation von OpenText Identity Manager für Revisionsereignisse mit Sentinel definiert. Diese Einstellungen werden nur dann im Dienstprogramm angezeigt, wenn die Option **Erweiterte Optionen anzeigen** aktiviert ist.

Zertifikat für Sentinel-Digitalsignatur

Gibt das benutzerdefinierte Zertifikat mit öffentlichem Schlüssel an, mit dem der OAuth-Server die an Sentinel gesendeten Revisionsmeldungen authentifizieren soll.

Privater Schlüssel für Sentinel-Digitalsignatur

Gibt den Pfad zur benutzerdefinierten Datei mit dem privaten Schlüssel an, mit dem der OAuth-Server die an Sentinel gesendeten Revisionsmeldungen authentifizieren soll.

Sonstige

Diese Einstellungen werden nur dann im Dienstprogramm angezeigt, wenn die Option **Erweiterte Optionen anzeigen** aktiviert ist.

OCSP-URI

Gibt den URI (Uniform Resource Identifier) an, der zum Einsatz kommen soll, wenn die Client-Installation das OCSP (On-Line Certificate Status Protocol) verwendet. Beispiel: `http://host:port/ocspLocal`.

Die OCSP-URI aktualisiert den Status der verbürgten Zertifikate online.

Konfigurationspfad für Autorisierung

Gibt den vollständig qualifizierten Name der Konfigurationsdatei für die Autorisierung an.

Identitätsdepotindizes

Gibt an, ob das Installationsprogramm während der Installation Indizes für die Attribute "manager" und "srvprvUUID" erstellen soll. Nach der Installation können Sie die Einstellungen bearbeiten, sodass sie auf einen neuen Speicherort der Indizes verweisen. Bei dieser Einstellung sind die folgenden Überlegungen zu beachten:

- Sind für diese Attribute keine Indizes vorhanden, kann dies eine eingeschränkte Leistung der Identity Applications zur Folge haben.
- Sie können diese Indizes manuell mit der OpenText Identity Console erstellen, nachdem Sie Identity Applications installiert haben.

- Zur Erzielung einer optimalen Leistung sollten Sie den Index während der Installation erstellen.
- Die Indizes müssen sich im Online-Modus befinden, bevor Sie Identity Applications den Benutzern zur Verfügung stellen.
- Zum Erstellen oder Löschen eines Index müssen Sie außerdem einen Wert für **Server-DN** angeben.

Server-DN

Gilt nur dann, wenn Sie einen Identitätsdepot-Index erstellen oder löschen möchten.

Gibt den OpenText eDirectory-Server an, auf dem die Indizes erstellt oder entfernt werden sollen.

Sie können jeweils nur einen Server angeben, nicht mehrere Server gleichzeitig. Sollen Indizes auf mehreren OpenText eDirectory-Servern konfiguriert werden, müssen Sie das RBPM-Konfigurationsprogramm mehrmals ausführen.

RBPM-Sicherheit neu initiieren

Gibt an, ob die RBPM-Sicherheit nach Abschluss des Installationsvorgangs zurückgesetzt werden soll. Sie müssen außerdem Identity Applications erneut bereitstellen.

IDMReport-URL

Gibt die URL des OpenText Identity Manager-Berichterstellungsmoduls an. Beispiel: `http://hostname:port/IDMRPT`.

Kontextname für benutzerdefinierte Themen

Gibt den Namen des benutzerdefinierten Themas an, mit dem Identity Applications im Browser dargestellt werden sollen.

Bezeichnerpräfix für Protokollierungsmeldung

Gibt den Wert an, der im Layoutmuster für die CONSOLE- und FILE-Appender in der Datei `idmuserapp_logging.xml` verwendet werden soll. Der Standardwert lautet RBPM.

Name des RBPM-Kontexts ändern

Gibt an, ob der Kontextname für RBPM geändert werden soll.

Sie müssen außerdem den neuen Namen und den DN des Rollen- und Ressourcenservice-Treibers angeben.

Name des RBPM-Kontexts

Gilt nur dann, wenn Sie die Option **Name des RBPM-Kontexts ändern** *wählen.*

Gibt den neuen Kontextnamen für RBPM an.

Rollentreiber-DN

Gilt nur dann, wenn Sie die Option **Name des RBPM-Kontexts ändern** *wählen.*

Gibt den DN des Rollen- und Ressourenservice-Treibers an.

Containerobjekt

Diese Parameter gelten nur während der Installation.

In diesem Abschnitt wird beschrieben, wie Sie die Werte für Containerobjekte definieren oder neue Containerobjekte erstellen.

Ausgewählt

Gibt die zu verwendenden Containerobjekttypen an.

Containerobjekttyp

Gibt den Typ für den Container an: Standort, Land, Organisationseinheit, Organisation oder Domäne.

Sie können in der OpenText Identity Console auch eigene Container definieren und sie unter **Neues Containerobjekt hinzufügen** hinzufügen.

Containerattributname

Gibt den Namen des Attributtyps an, der dem angegebenen Containerobjekttyp zugewiesen ist.

Neues Containerobjekt hinzufügen: Containerobjekttyp

Gibt den LDAP-Namen einer Objektklasse aus dem Identitätsdepot an, die als neuer Container fungieren kann.

Neues Containerobjekt hinzufügen: Containerattributname

Gibt den Namen des Attributtyps an, der dem neuen Containerobjekttyp zugewiesen ist.

Parameter für die Berichterstellung

Beim Konfigurieren der Identity Applications definieren Sie auf dieser Registerkarte die Werte für die Verwaltung von Identity Reporting. Diese Registerkarte wird zum Dienstprogramm hinzugefügt, sobald Sie Identity Reporting installieren.

Standardmäßig werden auf dieser Registerkarte nur die grundlegenden Optionen angezeigt. Mit **Erweiterte Optionen anzeigen** lassen Sie alle Einstellungen einblenden. Diese Registerkarte umfasst die folgenden Gruppen von Einstellungen:

- „Email-Lieferkonfiguration“, auf Seite 87
- „Berichtbeibehaltungswerte“, auf Seite 88
- „Gebietsschema bearbeiten“, auf Seite 89
- „Rollenkonfiguration“, auf Seite 89
- „Ausgangs-Proxy“, auf Seite 89

Email-Lieferkonfiguration

In diesem Abschnitt werden die Werte zum Senden von Benachrichtigungen definiert.

Hostname des SMTP-Servers

Gibt den DNS-Namen oder die IP-Adresse des Email-Servers an, über den Identity Reporting die Benachrichtigungen senden soll. Verwenden Sie nicht `localhost`.

Port des SMTP-Servers

Gibt die Port-Nummer für den SMTP-Server an.

SMTP mit SSL

Gibt an, ob die Kommunikation mit dem Email-Server über das TLS/SSL-Protokoll erfolgen soll.

Authentifizierung für Server erforderlich

Gibt an, ob für die Kommunikation mit dem Email-Server eine Authentifizierung erforderlich sein soll.

SMTP-Benutzername

Gibt die Email-Adresse für die Authentifizierung an.

Sie müssen einen Wert angeben. Wenn für den Server keine Authentifizierung erforderlich ist, können Sie eine ungültige Adresse angeben.

SMTP-Benutzerpasswort

Gilt nur dann, wenn Sie angeben, dass für den Server eine Authentifizierung erforderlich ist.

Geben Sie das Passwort für das SMTP-Benutzerkonto an.

Standardmäßige Email-Adresse

Gibt die Email-Adresse an, die Identity Reporting als Absender für Email-Benachrichtigungen verwenden soll.

Berichtbeibehaltungswerte

In diesem Abschnitt werden die Werte zum Speichern abgeschlossener Berichte definiert.

Berichtseinheit, Berichtslebensdauer

Gibt den Zeitraum an, über den die abgeschlossenen Berichte in Identity Reporting beibehalten werden sollen, bevor sie gelöscht werden. Sollen beispielsweise sechs Monate angegeben werden, geben Sie die Zahl 6 in das Feld **Berichtslebensdauer** ein und wählen Sie dann die Option **Monat** im Feld **Berichtseinheit**.

Speicherort der Berichte

Gibt einen Pfad an, in dem die Berichtsdefinitionen gespeichert werden sollen. Beispiel: `C:\NetIQ\idm\apps\IdentityReporting`.

Gebietsschema bearbeiten

In diesem Abschnitt werden die Werte für die Sprache von Identity Reporting definiert. Identity Reporting nutzt die angegebenen Gebietsschemas in den Suchvorgängen. Weitere Informationen finden Sie im OpenText™ Identity Manager CE 24.4 (v4.10) – Administratorhandbuch zu Identity Applications.

Rollenkonfiguration

In diesem Abschnitt werden die Werte für die Authentifizierungsquellen von Identity Reporting definiert.

Authentifizierungsquelle hinzufügen

Gibt den Typ der Authentifizierungsquelle an, die für die Berichterstellung hinzugefügt werden soll. Mögliche Authentifizierungsquellen:

- **Standard**
- **LDAP-Verzeichnis**
- **Datei**

Ausgangs-Proxy

In diesem Abschnitt werden die Werte für den Reverse-Proxy-Server definiert, den Identity Reporting zum Herunterladen von Berichten verwendet.

Proxy verwenden

Gibt an, dass ein Reverse-Proxy-Server für die Berichterstellung verwendet wird.

- **Hostname oder IP-Adresse**
- **Port**
- **TLS verwenden**

  Gilt nur, wenn als Netzwerkprotokoll TCP verwendet werden soll.

Parameter für Authentifizierung

Beim Konfigurieren der Identity Applications werden auf dieser Registerkarte die Parameter definiert, mit denen Tomcat die Benutzer zu den Seiten der Identity Applications und der Passwortverwaltung weiterleitet.

Standardmäßig werden auf dieser Registerkarte nur die grundlegenden Optionen angezeigt. Mit **Erweiterte Optionen anzeigen** lassen Sie alle Einstellungen einblenden. Diese Registerkarte umfasst die folgenden Gruppen von Einstellungen:

- „Beglaubigungsserver“, auf Seite 90
- „Authentifizierungskonfiguration“, auf Seite 90
- „Authentifizierungsmethode“, auf Seite 91
- „Passwortverwaltung“, auf Seite 92
- „Zertifikat und Schlüssel für Sentinel-Digitalsignatur“, auf Seite 93

Beglaubigungsserver

In diesem Abschnitt werden die Einstellungen zum Herstellen einer Verbindung der Identity Applications zum Authentifizierungsserver definiert.

Hostkennung für OAuth-Server

Erforderlich

Gibt die relative URL des Authentifizierungsservers an, der Token an den OSP ausgibt. Zum Beispiel 192.168.0.1.

TCP-Port für OAuth-Server

Gibt den Port für den Authentifizierungsserver an.

Access Manager ist OAuth-Anbieter

Die Konvertierung von OSP zu NAM für OAuth wird auf der Registerkarte „Authentifizierung“ des Konfigurationsaktualisierungsprogramms nicht unterstützt. Um diese Option auszublenden, legen Sie in der Datei `configupdate.sh.properties` den Wert *no_nam_oauth* auf `"true"` fest.

OAuth-Server verwendet TLS/SSL

Gibt an, ob der Authentifizierungsserver das TLS/SSL-Protokoll für die Kommunikation nutzt.

Datei für optionalen TLS/SSL-Truststore

Gilt nur dann, wenn Sie die Option **OAuth-Server verwendet TLS/SSL** *wählen und die erweiterten Optionen im Dienstprogramm eingeblendet sind.*

Passwort für optionalen TLS/SSL-Truststore

Gilt nur dann, wenn Sie die Option **OAuth-Server verwendet TLS/SSL** *wählen und die erweiterten Optionen im Dienstprogramm eingeblendet sind.*

Gibt das Passwort zum Laden der Keystore-Datei für den TLS/SSL-Authentifizierungsserver an.

HINWEIS: Sollten Sie keinen Keystore-Pfad und kein Passwort angeben und befindet sich das vertrauenswürdige Zertifikat nicht im JRE-Truststore (cacerts), können sich Identity Applications nicht mit dem Authentifizierungsdienst verbinden, der das TLS/SSL-Protokoll nutzt.

Authentifizierungskonfiguration

In diesem Abschnitt werden die Einstellungen für den Authentifizierungsserver definiert.

LDAP-DN für Admin-Container

Erforderlich

Gibt den eindeutigen Namen des Containers im Identitätsdepot an, in dem sich Administratorbenutzerobjekte befinden, die durch den OSP authentifiziert werden müssen. Beispiel: `ou=sa,o=data`.

Doppeltes Auflösungsbenennungsobjekt

Gibt den Namen des LDAP-Attributs an, mit dem mehrere OpenText eDirectory-Benutzerobjekte mit demselben `cn`-Wert voneinander unterschieden werden können. Der Standardwert lautet `mail`.

Authentifizierungsquellen auf Kontexte beschränken

Gibt an, ob Suchvorgänge in den Benutzer- und Administratorcontainern im Identitätsdepot ausschließlich auf die Benutzerobjekte in diesen Containern beschränkt sind oder ob auch Untercontainer durchsucht werden sollen.

Sitzungszeitüberschreitung (Minuten)

Gibt den Zeitraum (in Minuten) an, über den eine Sitzung inaktiv sein darf, bevor der Server diese Benutzersitzung wegen Zeitüberschreitung beendet. Der Standardwert ist 20 Minuten.

Lebensdauer des Zugriffstokens (Sekunden)

Gibt den Zeitraum (in Sekunden) an, über den ein OSP-Zugriffstoken gültig ist. Der Standardwert ist 60 Sekunden.

Lebensdauer des Aktualisierungstokens (Stunden)

Gibt den Zeitraum (in Sekunden) an, über den ein OSP-Aktualisierungstoken gültig ist. Das Aktualisierungstoken wird intern durch den OSP verwendet. Der Standardwert beträgt 48 Stunden.

Authentifizierungsmethode

In diesem Abschnitt werden die Werte für die Authentifizierung der Benutzer, die sich bei den browsergestützten Komponenten von OpenText Identity Manager anmelden, in OSP definiert.

Methode

Gibt den Typ der Authentifizierung an, die in OpenText Identity Manager verwendet werden soll, wenn ein Benutzer sich anmeldet.

- **Name und Passwort:** Der OSP überprüft die Authentifizierung beim Identitätsdepot.
- **Kerberos:** Der OSP akzeptiert die Authentifizierung sowohl durch einen Kerberos-Ticketserver als auch durch das Identitätsdepot. Sie müssen außerdem einen Wert für **Zuordnungsattributname** angeben.
- **SAML 2.0:** Der OSP akzeptiert die Authentifizierung sowohl durch einen SAML-Identitätsanbieter als auch durch das Identitätsdepot. Sie müssen außerdem einen Wert für **Zuordnungsattributname** und **Metadaten-URL** angeben.

Zuordnungsattributname

Gilt nur dann, wenn Sie die Option **Kerberos** *oder* **SAML** *wählen.*

Gibt den Namen des Attributs an, das dem Kerberos-Ticketserver oder den SAML-Darstellungen beim Identitätsanbieter zugeordnet ist.

Metadaten-URL

Gilt nur dann, wenn Sie die Option **SAML** *wählen.*

Gibt die URL an, über die der OSP die Authentifizierungsanforderung an SAML weiterleitet.

Passwortverwaltung

In diesem Abschnitt werden die Werte definiert, mit denen die Benutzer in die Lage versetzt werden, ihr Passwort per Selbstbedienung zu ändern.

Passwortverwaltungsanbieter

Gibt den Typ des zu verwendenden Passwortverwaltungsanbieters an.

Benutzeranwendung (alt): Verwendet das bislang genutzte Passwortverwaltungsprogramm in OpenText Identity Manager. Mit dieser Option können Sie außerdem ein externes Passwortverwaltungsprogramm angeben.

Self Service Password Reset (SSPR): Nutzen Sie den Self Service Password Reset-Dienst, der in Identity Applications enthalten ist und der es Benutzern ermöglicht, ihr Passwort ohne administrativen Eingriff zurückzusetzen. Sie können die Links wählen, die auf der Anmeldeseite des Identity Applications-Dashboards angezeigt werden, sodass Benutzer je nach Bedarf die entsprechende Aktion zum Zurücksetzen des Anmeldezugangs wählen können. Weitere Informationen finden Sie unter „User Interface“, auf Seite 93.

SSPR ist die Standardauswahl für das Feld **Passwortverwaltungsanbieter**.

Vergessenes Passwort

Diese Menüliste gilt nur dann, wenn Sie **Benutzeranwendung (alt)** *wählen.*

Gibt an, ob das integrierte Passwortverwaltungssystem in der Benutzeranwendung oder ein externes System verwendet werden soll.

- **Intern:** Verwendet die interne Standardfunktion für die Passwortverwaltung: `./jsps/pwdmgt/ForgotPassword.jsp` (ohne http[s] am Anfang). Hierdurch wird der Benutzer nicht zu einer externen WAR-Datei, sondern zur in der Benutzeranwendung integrierten Funktionalität „Passwort vergessen“ umgeleitet.
- **Extern**: Ruft die Benutzeranwendung mithilfe einer externen WAR-Datei für „Passwort vergessen“ über einen Webservice auf. Sie müssen außerdem die Einstellungen für das externe System festlegen.

„Passwort vergessen“-Link

Gilt nur dann, wenn ein externes Passwortverwaltungssystem verwendet werden soll.

Gibt die URL an, die auf die „Passwort vergessen“-Funktionsseite verweist. Geben Sie eine `ForgotPassword.jsp`-Datei an, die sich in einer externen oder in einer internen WAR-Datei für die Passwortverwaltung befindet.

Link zurück zu „Passwort vergessen“

Gilt nur dann, wenn ein externes Passwortverwaltungssystem verwendet werden soll.

Gibt die URL für den **Link zurück zu „Passwort vergessen“** an, den der Benutzer nach Durchführung eines „Passwort vergessen“-Vorgangs anklicken kann.

Webservice-URL zu „Passwort vergessen“

Gilt nur dann, wenn ein externes Passwortverwaltungssystem verwendet werden soll.

Gibt die URL an, über die die externe WAR-Datei für „Passwort vergessen“ die Benutzeranwendung zum Durchführen der „Passwort vergessen“-Kernfunktionen aufruft. Verwenden Sie das folgende Format:

`https://<idmhost>:<sslport>/<idm>/pwdmgt/service`

User Interface

Diese Menüliste ist nur relevant, wenn Sie **Self Service Password Reset (SSPR)** *wählen.*

Gibt die Links an, die Sie auf der Anmeldeseite des Identity Applications-Dashboards anzeigen möchten. Die Standardauswahl, **"Können Sie sich nicht anmelden?"** zeigt einen gemeinsamen Link zum Zurücksetzen des Benutzernamens oder Passworts oder zur Registrierung für die Zugriffsberechtigung auf der Anmeldeseite an. Wenn Sie **Keine** wählen, hat der Benutzer keine Möglichkeit, das Passwort selbst zurückzusetzen.

Wenn Sie „**Andere Links**“ wählen, stehen Ihnen die folgenden Optionen zur Auswahl:

- **Passwort vergessen**: Stellt einen Link zur Verfügung, auf den ein bestehender Benutzer klicken kann, um sein Passwort zurückzusetzen, falls er es vergessen hat.
- **Benutzername vergessen**: Stellt einen Link zur Verfügung, auf den ein bestehender Benutzer klicken kann, um Benutzernamen und Passwort zurückzusetzen, falls er es vergessen hat.
- **Konto aktivieren**: Stellt einen Link zur Verfügung, auf den der Benutzer klicken kann, um ein neues Benutzerkonto für den Zugriff auf Identity Applications zu erstellen.

Zertifikat und Schlüssel für Sentinel-Digitalsignatur

In diesem Abschnitt werden die Werte für die Kommunikation von OpenText Identity Manager für Revisionsereignisse mit Sentinel definiert.

Zertifikat für Sentinel-Digitalsignatur

Gibt ein benutzerdefiniertes Zertifikat mit öffentlichem Schlüssel an, mit dem der OSP-Server die an das Revisionssystem gesendeten Revisionsmeldungen authentifizieren soll.

Weitere Informationen zum Konfigurieren von Zertifikaten für Novell Audit finden Sie unter „Managing Certificates“ (Verwalten von Zertifikaten) im *Novell Audit Administration Guide* (Novell Audit-Administrationshandbuch).

Privater Schlüssel für Sentinel-Digitalsignatur

Gibt den Pfad zur benutzerdefinierten Datei mit dem privaten Schlüssel an, mit dem der OSP-Server die an das Revisionssystem gesendeten Revisionsmeldungen authentifizieren soll.

Parameter für SSO-Clients

Beim Konfigurieren der Identity Applications definieren Sie auf dieser Registerkarte die Werte für die Verwaltung des Single-Sign-On-Zugriffs auf die Anwendungen.

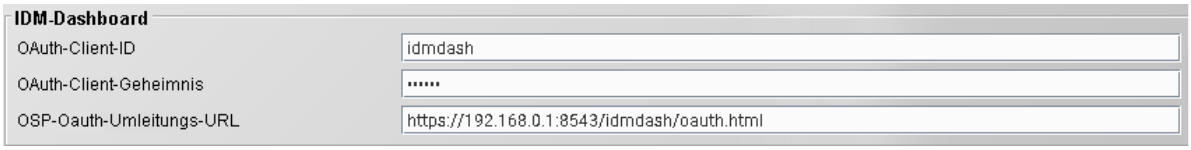
Standardmäßig werden auf dieser Registerkarte nur die grundlegenden Optionen angezeigt. Mit **Erweiterte Optionen anzeigen** lassen Sie alle Einstellungen einblenden. Diese Registerkarte umfasst die folgenden Gruppen von Einstellungen:

- „IDM-Dashboard“, auf Seite 94
- „IDM-Administrator“, auf Seite 94
- „RBPM“, auf Seite 95
- „Berichte“, auf Seite 96
- „IDM-Datenerfassungsdienst“, auf Seite 96

- „DCS-Treiber“, auf Seite 97
- „Zurücksetzen von Passwörtern per Selbstbedienung“, auf Seite 97

IDM-Dashboard

In diesem Abschnitt werden die Werte für die URL definiert, die Benutzer für den Zugriff auf das Identity Manager-Dashboard benötigen, den primären Anmeldungsspeicherort für Identity Applications.



OAuth-Client-ID

Erforderlich

Gibt den Namen an, mit dem sich der Single-Sign-on-Client für das Dashboard beim Authentifizierungsserver anmelden soll. Der Standardwert lautet `idmdash`.

OAuth-Client-Geheimnis

Erforderlich

Gibt das Passwort für den Single-Sign-on-Client für das Dashboard an.

OSP-OAuth-Umleitungs-URL

Erforderlich

Gibt die absolute URL an, zur der der Authentifizierungsserver einen Browser-Client nach erfolgter Authentifizierung weiterleiten soll.

Hierbei gilt das folgende Format: `Protokoll://Server:Port/Pfad`. Beispiel: `https://192.168.0.1:8543/idmdash/oauth.html`.

IDM-Administrator

In diesem Abschnitt werden die Werte für die URL definiert, über die die Benutzer auf die Seite des OpenText Identity Manager-Administrators zugreifen.

OAuth-Client-ID

Erforderlich

Gibt den Namen an, mit dem sich der Single-Sign-On-Client für den OpenText Identity Manager-Administrator beim Authentifizierungsserver anmelden soll. Der Standardwert lautet `idmadmin`.

OAuth-Client-Geheimnis

Erforderlich

Gibt das Passwort für den Single-Sign-On-Client für den OpenText Identity Manager-Administrator an.

OSP-OAuth-Umleitungs-URL

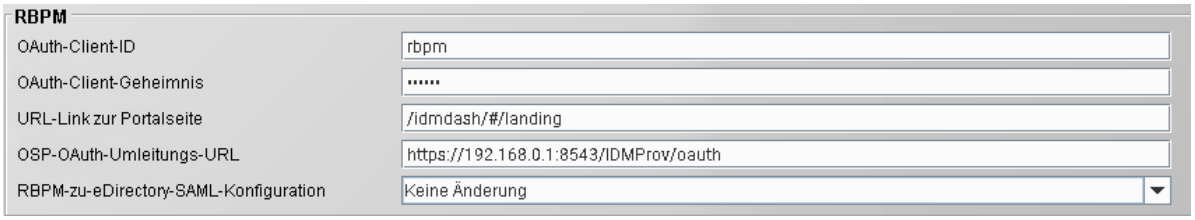
Erforderlich

Gibt die absolute URL an, zur der der Authentifizierungsserver einen Browser-Client nach erfolgter Authentifizierung weiterleiten soll.

Hierbei gilt das folgende Format: `Protokoll://Server:Port/Pfad`. Beispiel: `https://192.168.0.1:8543/idmadmin/oauth.html`.

RBPM

In diesem Abschnitt werden die Werte für die URL definiert, über die die Benutzer auf die Benutzeranwendung zugreifen.



OAuth-Client-ID

Erforderlich

Gibt den Namen an, mit dem sich der Single-Sign-On-Client für die Benutzeranwendung beim Authentifizierungsserver anmelden soll. Der Standardwert lautet `rbpm`.

OAuth-Client-Geheimnis

Erforderlich

Gibt das Passwort für den Single-Sign-On-Client für die Benutzeranwendung an.

URL-Link zur Portalseite

Erforderlich

Gibt die relative URL an, mit der Sie von der Benutzeranwendung aus auf das Dashboard zugreifen. Der Standardwert lautet `/landing`.

OSP-OAuth-Umleitungs-URL

Erforderlich

Gibt die absolute URL an, zur der der Authentifizierungsserver einen Browser-Client nach erfolgter Authentifizierung weiterleiten soll.

Hierbei gilt das folgende Format: `Protokoll://Server:Port/Pfad`. Beispiel: `https://192.168.0.1:8543/IDMProv/oauth`.

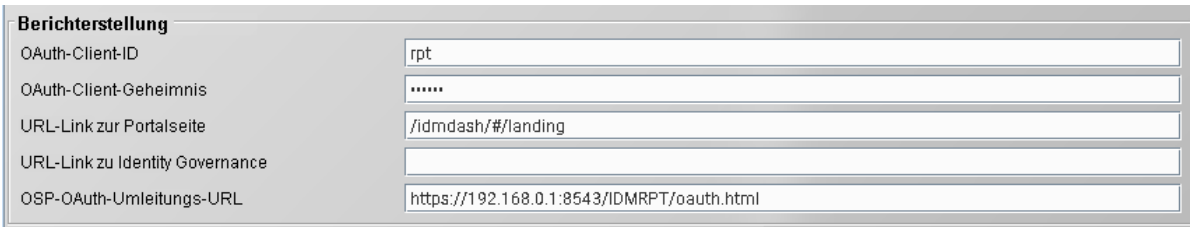
RBPM-zu-OpenText eDirectory-SAML-Konfiguration

Erforderlich

Gibt die erforderlichen RBPM-zu-OpenText eDirectory-SAML-Einstellungen für die SSO-Authentifizierung an.

Berichte

In diesem Abschnitt werden die Werte für die URL definiert, über die die Benutzer auf Identity Reporting zugreifen. Diese Werte werden im Dienstprogramm nur dann deaktiviert, wenn Sie Identity Reporting zur OpenText Identity Manager-Lösung hinzufügen.



OAuth-Client-ID

Erforderlich

Gibt den Namen an, mit dem sich der Single-Sign-On-Client für Identity Reporting beim Authentifizierungsserver anmelden soll. Der Standardwert lautet `rpt`.

OAuth-Client-Geheimnis

Erforderlich

Gibt das Passwort für den Single-Sign-On-Client für Identity Reporting an.

URL-Link zur Portalseite

Erforderlich

Gibt die relative URL an, mit der Sie von Identity Reporting aus auf das Dashboard zugreifen. Der Standardwert lautet `/idmdash/#/landing`.

Wenn Sie Identity Reporting und Identity Applications auf separaten Servern installiert haben, geben Sie eine absolute URL an. Hierbei gilt das folgende Format: `Protokoll://Server:Port/Pfad`. Beispiel: `https://192.168.0.1:8543/IDMRPT/oauth`.

OSP-OAuth-Umleitungs-URL

Erforderlich

Gibt die absolute URL an, zur der der Authentifizierungsserver einen Browser-Client nach erfolgter Authentifizierung weiterleiten soll.

Hierbei gilt das folgende Format: `Protokoll://Server:Port/Pfad`. Beispiel: `https://192.168.0.1:8543/IDMRPT/oauth`.

IDM-Datenerfassungsdienst

In diesem Abschnitt werden die Werte für die URL definiert, über die die Benutzer auf die Seite des OpenText Identity Manager-Datenerfassungsdiensts zugreifen.

OAuth-Client-ID

Erforderlich

Gibt den Namen an, mit dem sich der Single-Sign-On-Client für den OpenText Identity Manager-Datenerfassungsdienst beim Authentifizierungsserver anmelden soll. Der Standardwert lautet `idmdcs`.

OAuth-Client-Geheimnis

Erforderlich

Gibt das Passwort für den Single-Sign-On-Client für den OpenText Identity Manager-Datenerfassungsdienst an.

OSP-OAuth-Umleitungs-URL

Erforderlich

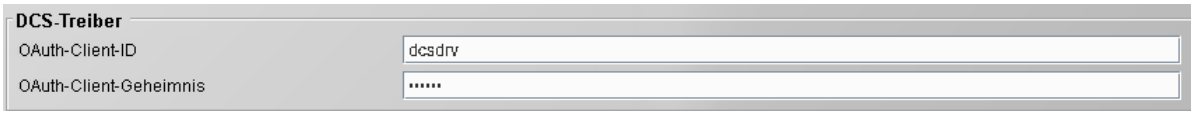
Gibt die absolute URL an, zur der der Authentifizierungsserver einen Browser-Client nach erfolgter Authentifizierung weiterleiten soll.

Hierbei gilt das folgende Format: `Protokoll://Server:Port/Pfad`. Beispiel: `https://192.168.0.1:8543/idmdcs/oauth.html`.

DCS-Treiber

In diesem Abschnitt werden die Werte für die Verwaltung des Treibers für den Datenerfassungsdienst (DCS-Treiber) definiert.

Abbildung 4-1



OAuth-Client-ID

Gibt den Namen an, mit dem sich der Single-Sign-On-Client für den DCS-Treiber beim Authentifizierungsserver anmelden soll. Der Standardwert für diesen Parameter lautet `dcsdrv`.

OAuth-Client-Geheimnis

Gibt das Passwort für den Single-Sign-On-Client für den DCS-Treiber an.

Zurücksetzen von Passwörtern per Selbstbedienung

In diesem Abschnitt werden die Werte für die URL definiert, über die die Benutzer auf SSPR zugreifen.

OAuth-Client-ID

Erforderlich

Gibt den Namen an, mit dem sich der Single-Sign-On-Client für SSPR beim Authentifizierungsserver anmelden soll. Der Standardwert lautet `sspr`.

OAuth-Client-Geheimnis

Erforderlich

Gibt das Passwort für den Single-Sign-On-Client für SSPR an.

OAuth-Umleitungs-URL

Erforderlich

Gibt die absolute URL an, zur der der Authentifizierungsserver einen Browser-Client nach erfolgter Authentifizierung weiterleiten soll.

Hierbei gilt das folgende Format: `Protokoll://Server:Port/Pfad`. Beispiel: `https://192.168.0.1:8543/sspr/public/oauth.html`.

CEF-Revisionsparameter

In diesem Abschnitt werden die Werte für die Verwaltung der CEF-Revisionsparameter definiert.

Auditereignisse senden

Gibt an, ob Auditereignisse in den Identity Applications über CEF gesendet werden sollen.

Ziel-Host

Gibt den DNS-Namen bzw. die IP-Adresse des Audit-Servers an.

Zielanschluß

Gibt die Portnummer des Audit-Servers an.

Netzwerkprotokoll

Gibt das Netzwerkprotokoll an, über das der Audit-Server die CEF-Ereignisse erhalten soll.

TLS verwenden

Gilt nur, wenn als Netzwerkprotokoll TCP verwendet werden soll.

Gibt an, ob der Audit-Server für TLS mit TCP konfiguriert ist.

Ereignis-Zwischenspeicherverzeichnis

Gibt den Speicherort des Cache-Verzeichnisses an, bevor die CEF-Ereignisse an den Audit-Server gesendet werden.

HINWEIS: Stellen Sie sicher, dass die `novlua`-Berechtigungen für das Ereignis-Zwischenspeicherverzeichnis festgelegt sind. Ansonsten können Sie nicht auf die IDMDash- und IDMProv-Anwendungen zugreifen. Außerdem werden keine OSP-Ereignisse im Ereignis-Zwischenspeicherverzeichnis gespeichert. Ändern Sie die Berechtigungen und das Eigentum für das Verzeichnis beispielsweise mit dem Befehl `chown novlua:novlua <Verzeichnispfad>`, wobei `<Verzeichnispfad>` den Pfad zum Ereignis-Zwischenspeicherverzeichnis angibt.

Bereitstellen von REST-APIs für Identity Applications

Die Komponenten der Identity Applications umfassen verschiedene REST-APIs, die verschiedene Funktionen innerhalb von Identity Applications aktivieren. Die REST-Services verwenden das OAUTH2-Protokoll für die Authentifizierung. Diese APIs können mit einem Browser oder curl-Befehl in Skripts aufgerufen werden, um die Verwaltungsaufgaben zu automatisieren. Die REST-APIs und die

entsprechende Dokumentation sind in Datei `idmappsdoc.war` verfügbar. Die WAR-Datei wird automatisch bei der Installation von Identity Applications bereitgestellt. Weitere Informationen finden Sie in der REST-API-Dokumentation.

Geben Sie in der Adressleiste Ihres Browsers `https://<Identity Applications-Servername>:<Port>/idmappsdoc` an, um auf dem Server, auf dem Identity Applications installiert sind, auf die REST-API-Dokumentation zuzugreifen. Beispiel: `https://192.168.0.1:8543/idmappsdoc`.

Zugreifen auf die Oracle-Datenbank anhand des Oracle-Service-Namens

Eine Verbindung zur Oracle-Datenbank wird mit der Oracle System-ID (SID) oder dem Oracle-Servicenamen hergestellt. Das Installationsprogramm für Identity Applications akzeptiert nur SID. Wenn Sie mit einem Servicenamen auf die Datenbank zugreifen möchten, führen Sie die Installation der Identity Applications in einer Datenbankinstanz aus, indem Sie eine Verbindung über SID herstellen. Führen Sie nach der Installation die folgenden Aktionen aus:

1. Erstellen Sie einen Servicenamen in der Oracle-Datenbank, indem Sie folgenden Befehl ausführen:

   ```
   alter system set service_names='SERVICE1' scope=both sid='*';
   ```

   wobei `SERVICE 1` der Name des Oracle-Service ist.

   HINWEIS: Der Servicename kann in Groß- oder Kleinbuchstaben angegeben werden. Die Groß-/Kleinschreibung wird dabei nicht berücksichtigt.

   ---

2. Definieren Sie den Servicenamen in der Tomcat-Datei `server.xml`, indem Sie die Oracle-Datenquellendetails in der Datei bearbeiten:

   ```
   url="jdbc:oracle:thin:@IP:PORT/service1"
   ```

3. Starten Sie Tomcat neu.
4. Vergewissern Sie sich, dass der Servicename in der Protokolldatei `catalina.out` enthalten ist.
5. Vergewissern Sie sich, dass Identity Applications ordnungsgemäß mit der Datenbank verbunden sind.

Manuelles Erstellen der Datenbank

Beim Erstellen der Identity Applications können Sie das Herstellen einer Verbindung zur Datenbank oder das Erstellen von Tabellen in der Datenbank auf einen späteren Zeitpunkt verschieben. Falls Sie keine Berechtigungen für die Datenbank besitzen, müssen Sie diese Option unter Umständen auswählen. Das Installationsprogramm erstellt eine SQL-Datei, mit der Sie das Datenbankschema erstellen können. Sie können die Datenbanktabellen außerdem nach der Installation neu erstellen, ohne die Installation wiederholen zu müssen. Löschen Sie hierzu die Datenbank für Identity Applications, und erstellen Sie eine neue Datenbank mit demselben Namen.

Generieren des Datenbankschemas mit der SQL-Datei

In diesem Abschnitt wird vorausgesetzt, dass das Installationsprogramm eine SQL-Datei erstellt hat, mit der Sie das Datenbankschema erstellen können. Falls Ihnen keine SQL-Datei vorliegt, beachten Sie die Anweisungen in „Manuelles Erstellen der SQL-Datei zum Generieren des Datenbankschemas“, auf Seite 100.

HINWEIS: Führen Sie die SQL-Datei nicht mit SQL*Plus aus. Die Zeilen in der Datei sind länger als 4000 Zeichen.

---

1. Halten Sie den Anwendungsserver an.
2. Melden Sie sich beim Datenbankserver an.
3. Löschen Sie die Datenbank, die von den Identity Applications genutzt wird.
4. Erstellen Sie eine neue Datenbank mit demselben Namen wie die Datenbank, die Sie in Schritt 3 gelöscht haben.
5. Navigieren Sie zum SQL-Skript, das im Rahmen des Installationsvorgangs erstellt wurde (standardmäßig im Verzeichnis `/Installationspfad/userapp/sql`).
6. (Bedingt) Bei einer Oracle-Datenbank fügen Sie einen umgekehrten Schrägstrich (/) nach der Definition der Funktion CONCAT_BLOB ein. Beispiel:

```
  -- Changeset icfg-data-load.xml::700::IDMRBPM
CREATE OR REPLACE FUNCTION CONCAT_BLOB(A IN BLOB, B IN BLOB) RETURN BLOB
AS
                C BLOB;
            BEGIN
                DBMS_LOB.CREATETEMPORARY(C, TRUE);
                DBMS_LOB.APPEND(C, A);
                DBMS_LOB.APPEND(C, B);
                RETURN c;
            END;
/
```

7. Bitten Sie den Datenbankadministrator, das SQL-Skript auszuführen, sodass die Datenbank für die Benutzeranwendung erstellt und konfiguriert werden kann.
8. Starten Sie Tomcat neu.

Manuelles Erstellen der SQL-Datei zum Generieren des Datenbankschemas

Sie können die Datenbanktabellen nach der Installation neu erstellen, ohne die Installation wiederholen zu müssen und ohne dass die SQL-Datei erforderlich ist. In diesem Abschnitt wird beschrieben, wie Sie das Datenbankschema ändern können, falls Ihnen die entsprechende SQL-Datei nicht vorliegt.

1. Halten Sie Tomcat an.
2. Melden Sie sich bei dem Server an, auf dem die Datenbank der Identity Applications gehostet wird.
3. Löschen Sie die vorhandene Datenbank.

4 Erstellen Sie eine neue Datenbank mit demselben Namen wie die Datenbank, die Sie in Schritt 3 gelöscht haben.

5 Öffnen Sie die Datei `NetIQ-Custom-Install.log` (standardmäßig im Stammverzeichnis des Installationsverzeichnisses für Identity Applications) in einem Texteditor. Beispiel:

```
C:\NetIQ\idm\apps\UserApplication
```

6 Suchen Sie in der Datei `NetIQ-Custom-Install.log` nach dem folgenden Befehl, und kopieren Sie ihn:

```
C:\NetIQ\idm\jre\bin\java -Xms256m -Xmx256m -Dwar.context.name=IDMProv
-Ddriver.dn="cn=User Application Driver,cn=driverset1,o=system" -
Duser.container="o=data" -jar C:\NetIQ\idm\jre\liquibase.jar --
databaseClass=liquibase.database.core.PostgresDatabase --
driver=org.postgresql.Driver --
classpath=C:\NetIQ\idm\apps\postgresql\postgresql-9.4.1212jdbc42.jar
C:\NetIQ\idm\apps\UserApplication\IDMProv.war --
changeLogFile=DatabaseChangeLog.xml --url="jdbc:postgresql://
localhost:5432/ idmuserappdb" --contexts="prov,newdb" --logLevel=info -
- logFile=C:\NetIQ\idm\apps\UserApplication\db.out --username********
-- password******** update
```

7 Melden Sie sich bei dem Server an, auf dem Sie die Datenbank für Identity Applications installiert haben.

8 Fügen Sie die kopierte Befehlszeichenkette in ein Terminal ein.

HINWEIS: Der Befehl sollte wie folgt lauten: `updateSQL`. Wenn stattdessen der Befehl `update` vorliegt, ersetzen Sie ihn durch `updateSQL`.

---

9 Ersetzen Sie die Sternchen (*) im Befehl, die für den Benutzernamen und das Passwort stehen, durch die tatsächlichen Angaben für die Authentifizierung. Achten Sie außerdem darauf, dass der Name der SQL-Datei eindeutig ist.

10 Führen Sie folgenden Befehl aus.

11 (Bedingt) Wenn keine Daten in die Datenbank geschrieben werden, sondern stattdessen eine SQL-Datei erzeugt wird, übermitteln Sie die Datei an Ihren Datenbankadministrator, und bitten Sie ihn, die Datei in den Datenbankserver zu importieren. Weitere Informationen finden Sie unter „Generieren des Datenbankschemas mit der SQL-Datei“, auf Seite 100.

12 Sobald der Datenbankadministrator die SQL-Datei importiert hat, starten Sie Tomcat.

Konfigurieren der Single Sign-on-Einstellungen für Identity Applications

Im Installationsvorgang wird ein Authentifizierungsservice (OSP) für den Single Sign-on-Zugriff in OpenText Identity Manager installiert. Sie können den OSP-Authentifizierungsserver jedoch auch für die Authentifizierung per Kerberos-Ticketserver oder SAML konfigurieren. Informationen zum Konfigurieren der Single Sign-on-Einstellungen für Identity Applications nach der Installation finden Sie unter Konfigurieren des Single Sign-on-Zugriffs in Identity Manager im *OpenText™ Identity Manager CE 24.4 (v4.10) – Administratorhandbuch zu Identity Applications*.

Starten der Identity Applications

Nach dem Konfigurieren der Identity Applications müssen der Tomcat- und der ActiveMQ-Service in jedem Fall neu gestartet werden.

Navigieren Sie zu `Services > IDM Application Tomcat Service` (Dienste > Tomcat-Dienst IDM-Anwendung) und klicken Sie auf **Restart** (Neu starten) oder **Stop**, um die Tomcat-Dienste anzuhalten.

Überlegungen zur Konfiguration und Nutzung der Identity Applications

Für die Konfiguration und die erste Verwendung der Identity Applications gelten die nachfolgenden Überlegungen.

- Während des Installationsvorgangs legt das Installationsprogramm Protokolldateien im Installationsverzeichnis ab. Diese Dateien enthalten Informationen über Ihre Konfiguration. Nach erfolgter Konfiguration der Identity Applications sollten Sie diese Dateien löschen oder an einem sicheren Speicherort aufbewahren. Während des Installationsvorgangs können Sie angeben, dass das Datenbankschema in eine Datei geschrieben werden soll. Da diese Datei beschreibende Informationen über Ihre Datenbank enthält, sollten Sie sie nach Abschluss der Installation an einem sicheren Speicherort aufbewahren.
- (Bedingt) Soll eine Revision der Identity Applications erfolgen, müssen Identity Reporting und ein Revisionsservice in der Umgebung installiert und für die Erfassung von Ereignissen konfiguriert sein. Sie müssen außerdem Identity Applications für die Revision konfigurieren.
- Bevor die Benutzer auf Identity Applications zugreifen können, müssen Sie die folgenden Schritte ausführen:
  - Stellen Sie sicher, dass alle erforderlichen OpenText Identity Manager-Treiber installiert sind.
  - Aktivieren Sie Cookies in allen Browsern. Die Anwendungen sind nicht funktionsfähig, wenn Cookies deaktiviert sind.
- Wenn Sie Identity Applications und SSPR auf verschiedenen Servern installiert haben, müssen Sie das vertrauenswürdige SSPR-Zertifikat mit dem CN „Identity Applications“ in die Datei `cacerts` des Identity Applications-Servers importieren.

Konfigurieren der Laufzeitumgebung für die Datenerfassung

Dieser Abschnitt enthält Informationen zu zusätzlichen Konfigurationsschritten, die für die ordnungsgemäße Funktionsfähigkeit der Laufzeitumgebung sorgen. Hier finden Sie außerdem Verfahren zur Fehlersuche sowie Informationen zu wichtigen Datenbanktabellen.

Dieser Vorgang umfasst folgende Schritte:

- „Konfigurieren des DCS-Treibers für das Erfassen von Daten aus den Identity Applications“, auf Seite 103
- „Migrieren des DCS-Treibers“, auf Seite 104

- „Zusätzliche Unterstützung für benutzerdefinierte Attribute und Objekte“, auf Seite 106
- „Zusätzliche Unterstützung für mehrere Treibersätze“, auf Seite 109
- „Konfigurieren der Treiber für die Ausführung im Remote-Modus mit SSL“, auf Seite 110

Weitere Informationen zu Problemen mit einem oder mehreren Treibern auftreten, die Sie nicht ohne weiteres selbst beheben können, finden Sie unter „Troubleshooting the Drivers“ (Fehlersuche für die Treiber) im *Identity Reporting Module Guide* (Handbuch zum Berichterstellungsmodul in OpenText Identity Manager).

Konfigurieren des DCS-Treibers für das Erfassen von Daten aus den Identity Applications

Damit Identity Applications ordnungsgemäß mit Identity Reporting zusammenarbeiten, müssen Sie den DCS-Treiber für die Unterstützung des OAuth-Protokolls konfigurieren.

HINWEIS

- Der DCS-Treiber muss nur dann installiert und konfiguriert werden, wenn Sie Identity Reporting in Ihrer Umgebung nutzen.
- Wenn mehrere DCS-Treiber in Ihrer Umgebung konfiguriert sind, müssen Sie die nachfolgenden Schritte jeweils für alle Treiber ausführen.

---

1. Melden Sie sich bei Designer an.
2. Öffnen Sie Ihr Projekt in Designer.
3. (Bedingt) Falls Sie den DCS-Treiber noch nicht auf die unterstützte Patch-Version aufgerüstet haben, führen Sie die folgenden Schritte aus:
   - **3a** Laden Sie die aktuelle Patch-Datei für den DCS-Treiber herunter.
   - **3b** Extrahieren Sie die Patch-Datei in ein Verzeichnis auf Ihrem Server.
   - **3c** Navigieren Sie in einem Terminal zum Speicherort der extrahierten Patch-RPM-Datei für Ihre Umgebung, und führen Sie den folgenden Befehl aus:

     ```
     rpm -Uvh novell-DXMLdcs.rpm
     ```

   - **3d** Starten Sie das Identitätsdepot neu.
   - **3e** Überprüfen Sie in Designer, ob eine unterstützte Version des Datenerfassungsdienst-Basispakets installiert ist. Falls nötig, installieren Sie die aktuelle Version, bevor Sie den Vorgang fortsetzen.
   - **3f** Stellen Sie den DCS-Treiber in Designer erneut bereit, und starten Sie ihn neu.
4. Klicken Sie in der Ansicht **Gliederung** mit der rechten Maustaste auf den DCS-Treiber, und wählen Sie **Eigenschaften**.
5. Klicken Sie auf **Treiberkonfiguration**.
6. Klicken Sie auf die Registerkarte **Treiberparameter**.
7. Klicken Sie auf **Verbindungsparameter anzeigen**, und wählen Sie **Anzeigen**.
8. Klicken Sie auf **Unterstützung für SSO-Dienst**, und wählen Sie **Ja**.
9. Geben Sie die IP-Adresse und den Port für Identity Reporting ein.

10 Geben Sie das Passwort für den SSO-Dienst-Client ein. Das Standardpasswort lautet `driver`.

11 Klicken Sie auf **Anwenden** und dann auf **OK**.

12 Klicken Sie in der Ansicht **Modellierer** mit der rechten Maustaste auf den DCS-Treiber, und wählen Sie **Treiber > Bereitstellen**.

13 Klicken Sie auf **Bereitstellen**.

14 Wenn Sie aufgefordert werden, den DCS-Treiber neu zu starten, klicken Sie auf **Ja**.

15 Klicken Sie auf **OK**.

Migrieren des DCS-Treibers

Damit die Objekte mit dem Identity Information Warehouse synchronisiert werden können, müssen Sie den DCS-Treiber migrieren.

1 Melden Sie sich bei der OpenText Identity Console an.

2 Wählen Sie in der Kachel **IDM-Verwaltung** den Datenerfassungsdiensttreiber und gehen Sie zu **Datenumwandlung und Synchronisierung**.

3 Wählen Sie in der Ansicht "Datensynchronisierung" die Option **Aus Identitätsdepot migrieren**.

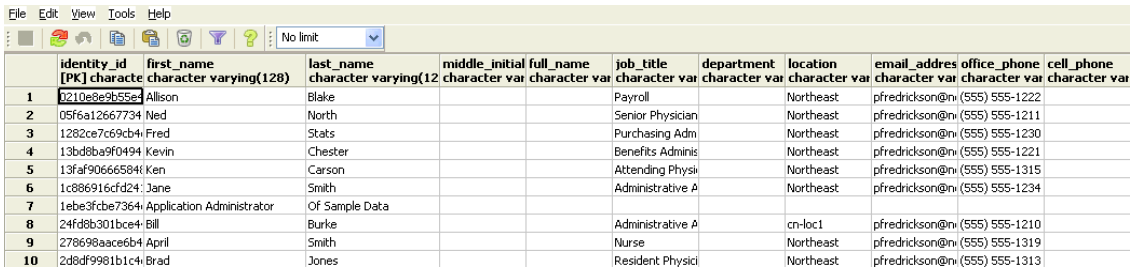
4 Wählen Sie die Organisationen aus, die relevante Daten enthalten, und klicken Sie auf **Starten**.

HINWEIS: Der Migrationsvorgang kann mehrere Minuten dauern, abhängig von der vorliegenden Datenmenge. Warten Sie in jedem Fall ab, bis der Migrationsvorgang abgeschlossen ist, und fahren Sie dann erst mit den nächsten Schritten fort.

---

5 Warten Sie ab, bis der Migrationsvorgang abgeschlossen ist.

6 Die Tabellen **idmrpt_identity** und **idmrpt_acct** enthalten Informationen zu den Identitäten und Konten im Identitätsdepot. Überprüfen Sie, ob die folgenden Arten von Informationen in diesen Tabellen vorliegen:

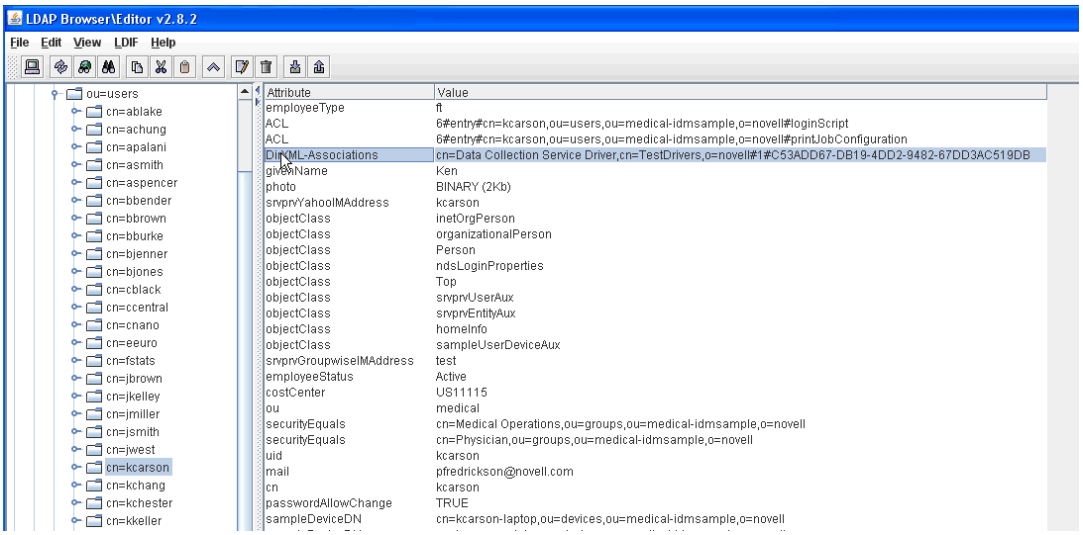

File Edit View Tools Help

No limit

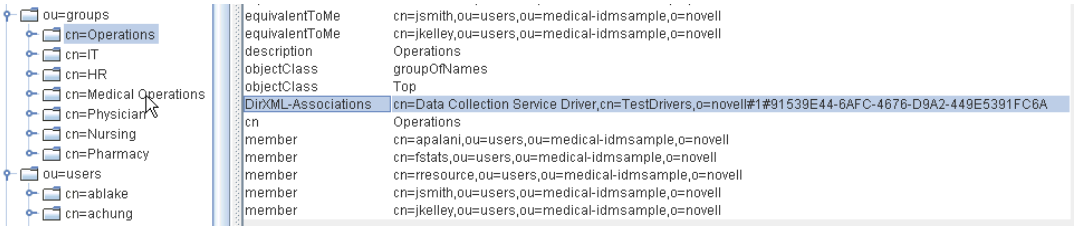
	identity_id [PK] characte	first_name character varying(128)	last_name character varying(12	middle_initial character var	full_name character var	job_title character var	department character var	location character var	email_addres character var	office_phone character var	cell_phone character var
1	0210e8e9b55e4	Allison	Blake			Payroll		Northeast	pfredrickson@n	(555) 555-1222	
2	05f6a12667734	Ned	North			Senior Physician		Northeast	pfredrickson@n	(555) 555-1211	
3	1282ce7c69cb4	Fred	Stats			Purchasing Adm		Northeast	pfredrickson@n	(555) 555-1230	
4	13bd8ba9f0494	Kevin	Chester			Benefits Adminis		Northeast	pfredrickson@n	(555) 555-1221	
5	13faf90666584	Ken	Carson			Attending Physi		Northeast	pfredrickson@n	(555) 555-1315	
6	1c886916cfd24	Jane	Smith			Administrative A		Northeast	pfredrickson@n	(555) 555-1234	
7	1ebe3fcbe7364	Application Administrator	Of Sample Data								
8	24fd8b301bce4	Bill	Burke			Administrative A		cn-loc1	pfredrickson@n	(555) 555-1210	
9	278698aace6b4	April	Smith			Nurse		Northeast	pfredrickson@n	(555) 555-1319	
10	2d8df9981b1c4	Brad	Jones			Resident Physici		Northeast	pfredrickson@n	(555) 555-1313	

7 Überprüfen Sie im LDAP-Browser, ob bei der Migration die folgenden Verweise auf DirXML-Verknüpfungen hinzugefügt wurden:

- Überprüfen Sie für alle Benutzer jeweils die folgenden Arten von Informationen:



- Überprüfen Sie für alle Gruppen jeweils die folgenden Arten von Informationen:



8 Die Daten in der Tabelle **idmrpt_group** müssen wie folgt aufgebaut sein (Beispiel):

group_name character var	group_desc character var	dynamic_gro boolean	dynamic_rule character var	nested_group boolean	idmrpt_valid_from timestamp without tin	idmrpt_deleted boolean	idmrpt_syn_state smallint
Pharmacy	Pharmacy	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
IT	Information Tec	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
HR	Human Resourc	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Physician	Physician	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Operations	Operations	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Medical Operatic	Medical Operatic	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Nursing	Nursing	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1

Diese Tabelle zeigt den Namen der einzelnen Gruppen und dazu die Flags, aus denen hervorgeht, ob eine Gruppe dynamisch oder verschachtelt ist. Außerdem ist hier ersichtlich, ob die Gruppe migriert wurde. Wenn ein Objekt in der Benutzeranwendung geändert, jedoch noch nicht migriert wurde, ist der Synchronisierungsstatus (idmrpt_syn_state) unter Umständen auf 0 gesetzt. Wenn Sie beispielsweise einen Benutzer zu einer Gruppe hinzugefügt haben, ohne den Treiber zu migrieren, ist dieser Wert ggf. gleich 0.

9 (Optional) Überprüfen Sie die Daten in den folgenden Tabellen:

- idmrpt_approver
- idmrpt_association
- idmrpt_category
- idmrpt_container
- idmrpt_idv_drivers
- idmrpt_idv_prd

- idmrpt_role
- idmrpt_resource
- idmrpt_sod

10 (Optional) Die Tabelle **idmrpt_ms_collect_state** enthält Informationen zum Datenerfassungsstatus des MSGW-Treibers. Überprüfen Sie, ob in dieser Tabelle nunmehr Zeilen vorliegen.

Aus dieser Tabelle geht hervor, welche REST-Endpunkte der verwalteten Systeme ausgeführt wurden. Derzeit weist die Tabelle noch keine Zeilen auf, da Sie die Erfassung mit diesem Treiber noch nicht gestartet haben.

Zusätzliche Unterstützung für benutzerdefinierte Attribute und Objekte

Sie können den DCS-Treiber so konfigurieren, dass Daten auch für benutzerdefinierte Attribute und Objekte gespeichert werden, die nicht zum standardmäßigen Datenerfassungsschema gehören. Hierzu bearbeiten Sie den Filter des DCS-Treibers. Das Bearbeiten des Filters löst nicht sofort die Objektsynchronisierung aus. Die neu hinzugefügten Attribute und Objekte werden stattdessen an die Datenerfassungsdienste gesendet, sobald Hinzufügungs-, Bearbeitungs- oder Löschvorgänge im Identitätsdepot erfolgen.

Wenn Sie die Unterstützung für benutzerdefinierte Attribute und Objekte hinzufügen, müssen Sie die Berichte so ändern, dass die erweiterten Attribut- und Objektdaten berücksichtigt werden. Die folgenden Ansichten zeigen aktuelle Daten und Verlaufsdaten für die erweiterten Objekte und Attribute:

- idm_rpt_cfg.idmrpt_ext_idv_item_v
- idm_rpt_cfg.idmrpt_ext_item_attr_v

Dieser Vorgang umfasst folgende Schritte:

- „Konfigurieren des Treibers für die Verwendung erweiterter Objekte“, auf Seite 106
- „Angeben eines Namens und einer Beschreibung in der Datenbank“, auf Seite 107
- „Hinzufügen von erweiterten Attributen zu bekannten Objekttypen“, auf Seite 108

Konfigurieren des Treibers für die Verwendung erweiterter Objekte

Sie können beliebige Objekte und Attribute in die Filterrichtlinie für den DCS-Treiber aufnehmen. Wenn Sie ein neues Objekt oder Attribut hinzufügen, müssen Sie jeweils die GUID (mit „subscriber sync“) und die Objektklasse (mit „subscriber notify“) wie im folgenden Beispiel zuordnen:

```
<filter-class class-name="Device" publisher="ignore" publisher-create-
homedir="true" publisher-track-template-member="false" subscriber="sync">
<filter-attr attr-name="CN" merge-authority="default" publisher="ignore"
publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="Description" merge-authority="default"
publisher="ignore" publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="GUID" merge-authority="default" publisher="ignore"
publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="Object Class" merge-authority="default"
publisher="ignore" publisher-optimize-modify="true" subscriber="notify"/>
<filter-attr attr-name="Owner" merge-authority="default"
publisher="ignore" publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="Serial Number" merge-authority="default"
publisher="ignore" publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="sampleDeviceModel" from-all-classes="true" merge-
authority="default" publisher="ignore" publisher-optimize-modify="true"
subscriber="sync"/>
<filter-attr attr-name="sampleDeviceType" from-all-classes="true" merge-
authority="default" publisher="ignore" publisher-optimize-modify="true"
subscriber="sync"/>
</filter-class>
```

Angeben eines Namens und einer Beschreibung in der Datenbank

Wenn das Objekt in der Datenbank mit einem Namen und einer Beschreibung versehen werden soll, fügen Sie eine Schemazuordnungsrichtlinie für „_dcsName“ und „_dcsDescription“ hinzu. Mit der Schemazuordnungsrichtlinie werden die Attributwerte in der Objektinstanz den Spalten „idmrpt_ext_idv_item.item_name“ bzw. „idmrpt_ext_idv_item.item_desc“ zugeordnet. Falls Sie keine Schemazuordnungsrichtlinie hinzufügen, werden die Attribute in die Untertabelle „idmrpt_ext_item_attr“ eingetragen.

Beispiel:

```
<attr-name class-name="Device">
<nds-name>CN</nds-name>
<app-name>_dcsName</app-name>
</attr-name>
<attr-name class-name="Device">
<nds-name>Description</nds-name>
<app-name>_dcsDescription</app-name>
</attr-name>
```

Im folgenden SQL-Beispiel werden die Objekt- und Attributwerte in der Datenbank aufgeführt:

```
SELECT
    item.item_dn,
    item.item_name,
    item.item_desc,
    attr.attribute_name,
    itemAttr.attribute_value,
    item.idmrpt_deleted as item_deleted,
    itemAttr.idmrpt_deleted as attr_deleted,
    item.item_desc,
    obj.object_class
FROM
    idm_rpt_data.idmrpt_ext_idv_item as item,
idm_rpt_data.idmrpt_ext_item_attr itemAttr, idm_rpt_data.idmrpt_ext_attr
as attr, idm_rpt_data.idmrpt_ext_obj as obj
WHERE
    item.object_id = obj.object_id and itemAttr.attribute_id =
attr.attribute_id and itemAttr.cat_item_id = item.item_id
ORDER BY
    item.item_dn, item.item_name
```

Hinzufügen von erweiterten Attributen zu bekannten Objekttypen

Wenn Sie ein Attribut in die Filterrichtlinie des DCS-Treibers aufnehmen und nicht explizit der Berichterstellungsdatenbank in der XML-Verweisdatei (`IdmrptIdentity.xml`) zuordnen, wird der Wert in die Tabelle „idmrpt_ext_item_attr table“ und der Attributverweis in die Tabelle „idmrpt_ext_attr“ eingetragen und dort verwaltet.

Das folgende SQL-Beispiel zeigt diese erweiterten Attribute:

```
SELECT
    acct.idv_acct_dn,
    attrDef.attribute_name,
    attribute_value,
    attrVal.idmrpt_valid_from,
    cat_item_attr_id,
    attrVal.idmrpt_deleted,
    attrVal.idmrpt_syn_state
FROM
    idm_rpt_data.idmrpt_ext_item_attr as attrVal,
idm_rpt_data.idmrpt_ext_attr as attrDef, idm_rpt_data.idmrpt_identity as
idd, idm_rpt_data.idmrpt_idv_acct as acct
WHERE attrVal.attribute_id = attrDef.attribute_id and idd.identity_id =
acct.identity_id and attrVal.cat_item_id = acct.identity_id and
cat_item_type_id = 'IDENTITY'
```

Neben dem Benutzerobjekt können Sie erweiterte Attribute zu den folgenden Objekten in die Filterrichtlinie aufnehmen und in die Datenbank eintragen:

- nrfRole
- nrfResource
- Container

HINWEIS: Das installierte Produkt unterstützt Organisationseinheiten, Organisationen und Domänen. Die Containertypen werden in der Tabelle „idmrpt_container_types table“ verwaltet.

- Gruppe
- nrfSod

Die Verknüpfung der erweiterten Attribute zur übergeordneten Tabelle oder zum übergeordneten Objekt ist in der Spalte „idmrpt_cat_item_types.idmrpt_table_name“ ersichtlich. Diese Spalte beschreibt, wie die Spalte „idm_rpt_data.idmrpt_ext_item_attr.cat_item_id“ mit dem primären Schlüssel der übergeordneten Tabelle verbunden werden soll.

Zusätzliche Unterstützung für mehrere Treibersätze

Das neue Paket für die DCS-Bereichsdefinition (NOVLDCSSCPNG) bietet statische und dynamische Bereichsdefinitionsfunktionen für Enterprise-Umgebungen mit mehreren Treibersätzen und mehreren DCS-/MSGW-Treiberpaaren.

Während oder nach der Installation müssen Sie die Rolle des DCS-Treibers festlegen, auf dem das Paket installiert wird. Wählen Sie eine der folgenden Rollen aus:

- **Primär** Der Treiber synchronisiert alle Elemente (ausgenommen Teilbäume anderer Treibersätze). Ein primärer DCS-Treiber kann durchaus ein ganzes Identitätsdepot pflegen oder auch mit einem oder mehreren sekundären Treibern zusammenarbeiten.
- **Sekundär** Der Treiber synchronisiert ausschließlich den jeweils eigenen Treibersatz (und keine weiteren Elemente). Für einen sekundären DCS-Treiber muss in der Regel ein primärer Treiber in einem anderen Treibersatz ausgeführt werden, da ansonsten keine Daten, die sich außerhalb des lokalen Treibersatzes befinden, an den Datenerfassungsdienst gesendet werden.
- **Benutzerdefiniert** Hiermit ist der Administrator in der Lage, benutzerdefinierte Scoping-Regeln zu definieren. Der lokale Treibersatz bildet den einzigen impliziten Bereich. Alle anderen Elemente werden als außerhalb des Bereichs betrachtet, sofern sie nicht explizit zur Liste der benutzerdefinierten Bereiche hinzugefügt werden. Ein benutzerdefinierter Bereich ist der eindeutige Name (mit Schrägstrichen) eines Containers im Identitätsdepot, dessen untergeordnete Einheiten oder dessen Teilbaum synchronisiert werden sollen.

Das Scoping-Paket ist nur in bestimmten Konfigurationsszenarien erforderlich:

- **Einzelner Server und Identitätsdepot mit einzelnem Treibersatz:** In diesem Szenario ist kein Scoping erforderlich, und Sie müssen das Scoping-Paket nicht installieren.
- **Mehrere Server und Identitätsdepot mit einzelnem Treibersatz:** In diesem Szenario ist Folgendes zu beachten:
  - Auf dem OpenText Identity Manager-Server müssen sich Reproduktionen aller Partitionen befinden, von denen Daten erfasst werden sollen.
  - In diesem Szenario ist kein Scoping erforderlich. Installieren Sie daher nicht das Scoping-Paket.
- **Mehrere Server und Identitätsdepot mit mehreren Treibersätzen:** In diesem Szenario gelten zwei grundlegende Konfigurationen:
  - Auf allen Servern befinden sich Reproduktionen aller Partitionen, von denen Daten erfasst werden sollen.

Bei dieser Konfiguration ist Folgendes zu beachten:

- Das Scoping ist erforderlich, damit eine Änderung nicht von mehreren DCS-Treibern verarbeitet wird.
- Sie müssen das Scoping-Paket auf allen DCS-Treibern installieren.
- Ein DCS-Treiber muss als primärer Treiber festgelegt werden.
- Alle anderen DCS-Treiber müssen als sekundäre Treiber konfiguriert werden.

- Nicht auf *allen* Servern befinden sich Reproduktionen aller Partitionen, von denen Daten erfasst werden sollen.

  Bei dieser Konfiguration sind zwei Situationen möglich:

  - Alle Partitionen, von denen Daten erfasst werden sollen, befinden sich *auf einem einzigen* OpenText Identity Manager-Server.

    In diesem Fall ist Folgendes zu beachten:

    - Das Scoping ist erforderlich, damit eine Änderung nicht von mehreren DCS-Treibern verarbeitet wird.
    - Sie müssen das Scoping-Paket auf allen DCS-Treibern installieren.
    - Alle DCS-Treiber müssen als primäre Treiber konfiguriert werden.

  - Die Partitionen, von denen Daten erfasst werden sollen, befinden sich *nicht allesamt* auf einem einzigen OpenText Identity Manager-Server. (Einige Partitionen gehören zu mehreren OpenText Identity Manager-Servern.)

    In diesem Fall ist Folgendes zu beachten:

    - Das Scoping ist erforderlich, damit eine Änderung nicht von mehreren DCS-Treibern verarbeitet wird.
    - Sie müssen das Scoping-Paket auf allen DCS-Treibern installieren.
    - Alle DCS-Treiber müssen als benutzerdefinierte Treiber konfiguriert werden.

      Für jeden Treiber müssen benutzerdefinierte Scoping-Regeln definiert werden, wobei sich die Bereiche nicht überschneiden dürfen.

Konfigurieren der Treiber für die Ausführung im Remote-Modus mit SSL

Beim Ausführen im Remote-Modus können Sie den DCS- und den MSGW-Treiber für die Verwendung von SSL konfigurieren. In diesem Abschnitt finden Sie die Schritte zum Konfigurieren der Treiber für die Ausführung im Remote-Modus mit SSL.

So konfigurieren Sie SSL mit einem Keystore für den MSGW-Treiber:

1. Erstellen Sie in der OpenText Identity Console ein Serverzertifikat.
   - **1a** Klicken Sie unter **OpenText eDirectory** auf **Zertifikatsverwaltung > Server-Zertifikatsverwaltung**.
   - **1b** Navigieren Sie zum Serverobjekt, in dem der MSGW-Treiber installiert ist, und wählen Sie das Objekt aus.
   - **1c** Geben Sie einen Kurznamen für das Zertifikat an.

1d Wählen Sie für die Erstellungsmethode die Option **Standard**, und klicken Sie auf **Weiter**.

1e Klicken Sie auf **Fertig stellen** und dann auf **Schließen**.

2 Exportieren Sie das Serverzertifikat mit der OpenText Identity Console.

2a Klicken Sie unter **OpenText eDirectory** auf **Zertifikatsverwaltung > Server-Zertifikatsverwaltung**.

2b Wählen Sie das Zertifikat aus, das Sie in Schritt 1 auf Seite 110 erstellt haben, und klicken Sie auf **Exportieren**.

2c Wählen Sie im Menü **Zertifikate** den Namen Ihres Zertifikats.

2d Die Option **Privaten Schlüssel exportieren** muss aktiviert sein.

2e Geben Sie ein Passwort ein, und klicken Sie auf **Weiter**.

2f Klicken Sie auf **Exportiertes Zertifikat speichern**, und speichern Sie das exportierte pfx-Zertifikat.

3 Importieren Sie das pfx-Zertifikat, das Sie in Schritt 2 auf Seite 111 erstellt haben, in den Java-Keystore.

3a Verwenden Sie das Keytool in Java. Sie müssen JDK 6 oder höher verwenden.

3b Geben Sie an einer Eingabeaufforderung den folgenden Befehl ein:

```
keytool -importkeystore -srckeystore pfx certificate -srcstoretype
PKCS12 -destkeystore Keystore Name
```

Beispiel:

```
keytool -importkeystore -srckeystore cert.pfx -srcstoretype PKCS12
-destkeystore msgw.jks
```

3c Geben Sie das Passwort ein, wenn Sie dazu aufgefordert werden.

4 Ändern Sie die Konfiguration des Managed System Gateway Driver, um den Schlüsselspeicher über die OpenText Identity Console zu verwenden.

4a Klicken Sie in **IDM-Verwaltung** auf das Treiberset, das den Managed System Gateway Driver enthält.

4b Klicken Sie auf das Symbol **Managed System Gateway Driver** und gehen Sie zu **Konfiguration**.

4c Klicken Sie auf das Dropdown-Menü **Treiberparameter**.

4d Legen Sie auf der Registerkarte **Treibereinstellungen** die **Verbindungsparameter** auf "Anzeigen" fest und setzen Sie den **Konfigurationsmodus des Treibers** auf "Remote".

4e Geben Sie den vollständigen Pfad zur Keystore-Datei sowie das Passwort ein.

4f Speichern Sie den Treiber, und starten Sie ihn neu.

5 Ändern Sie die Konfiguration des Datenerfassungsdiensttreibers, um den Schlüsselspeicher über die OpenText Identity Console zu verwenden.

5a Klicken Sie in **IDM-Verwaltung** auf das Treiberset, das den Datenerfassungsdiensttreiber enthält.

5b Klicken Sie auf das Symbol **Datenerfassungsdiensttreiber** und gehen Sie zu **Treiberkonfiguration**.

5c Klicken Sie auf die Dropdown-Liste **Treiberparameter** und legen Sie die **Registrierungsparameter** auf "Anzeigen" fest.

5d Wählen Sie unter **Registrierung des Managed System Gateway** für **Konfigurationsmodus des MSGW-Treibers** die Option „Remote“.

5e Geben Sie den vollständigen Pfad zur Keystore-Datei, das Passwort und das Alias aus Schritt 1c auf Seite 110 ein.

5f Speichern Sie den Treiber, und starten Sie ihn neu.

Konfigurieren von Identity Reporting

Auch nach der Installation von Identity Reporting können Sie noch zahlreiche Installationseigenschaften bearbeiten. Sollen Änderungen vorgenommen werden, führen Sie das Konfigurationsaktualisierungsprogramm (`configupdate.sh`) aus.

Wenn Sie eine Einstellung für Identity Reporting mit dem Konfigurationsprogramm ändern, müssen Sie Tomcat neu starten, damit die Änderungen in Kraft treten. Wenn Sie die Änderungen dagegen in der Webbenutzeroberfläche für Identity Reporting vornehmen, entfällt der Neustart des Servers.

- „Manuelles Hinzufügen der Datenquelle auf der Seite der Identity-Datenerfassungsdienste“, auf Seite 112
- „Ausführen von Berichten über eine Oracle-Datenbank“, auf Seite 113
- „Manuelles Erstellen des Datenbankschemas“, auf Seite 113
- „Bereitstellen von REST-APIs für Identity Reporting“, auf Seite 117
- „Verbinden mit einer entfernten PostgreSQL-Datenbank“, auf Seite 117
- „Schritte nach der Installation für Identity Reporting“, auf Seite 118

Manuelles Hinzufügen der Datenquelle auf der Seite der Identity-Datenerfassungsdienste

1. Melden Sie sich bei der Identity Reporting-Anwendung an.
2. Klicken Sie auf **Datenquellen**.
3. Klicken Sie auf **Hinzufügen**.
4. Klicken Sie im Dialogfeld **Datenquelle hinzufügen** auf die Optionsschaltfläche **Wählen Sie aus der vordefinierten Liste**.
5. Wählen Sie **IDMDCSDataSource**.
6. Klicken Sie auf **Speichern**.

Ausführen von Berichten über eine Oracle-Datenbank

Mit Identity Reporting können Berichte über Remote-Oracle-Datenbanken ausgeführt werden. Die Datei „ojbc8.jar“ muss sich dabei auf dem Server befinden, auf dem die Oracle-Datenbank ausgeführt wird.

Manuelles Erstellen des Datenbankschemas

Soll das Datenbankschema nach der Installation manuell erstellt werden, führen Sie eines der folgenden Verfahren aus:

- „Konfigurieren des Schemas „Create_rpt_roles_and_schemas.sql“ gegen eine PostgreSQL-Datenbank“, auf Seite 113
- „Konfigurieren des Schemas „Create_rpt_roles_and_schemas.sql“ gegen eine Oracle-Datenbank“, auf Seite 114
- „Konfigurieren des Schemas „Create_rpt_roles_and_schemas.sql“ in einer Oracle-Datenbank“, auf Seite 116
- „Löschen der Datenbank-Prüfsummen“, auf Seite 116

Konfigurieren des Schemas „Create_rpt_roles_and_schemas.sql“ gegen eine PostgreSQL-Datenbank

1. Fügen Sie der Datenbank die erforderlichen Rollen mit den SQL-Dateien `create_dcs_roles_and_schemas.sql` und `create_rpt_roles_and_schemas.sql` hinzu, die sich unter `C:\NetIQ\idm\apps\IdentityReporting\sql` befinden.
2. Melden Sie sich als Postgres-Benutzer bei PGAdmin an.
3. Führen Sie das Abfragewerkzeug aus.
4. Zum Erstellen der Verfahren `Create_rpt_roles_and_schemas` und `Create_dcs_roles_and_schemas` kopieren Sie den Inhalt dieser SQLs in das Abfragewerkzeug und starten Sie dann die Ausführung gegen die verbundene Datenbank.
5. Führen Sie zum Erstellen der Rollen `IDM_RPT_DATA`, `IDM_RPT_CFG` und `IDMRPTUSER` die folgenden Befehle in der angegebenen Reihenfolge aus:

   ```
   Select CREATE_DCS_ROLES_AND_SCHEMAS('<Set pwd for IDM_RPT_DATA>', '<Set pwd for IDMRPTUSER>');

   Select CREATE_RPT_ROLES_AND_SCHEMAS('<Set pwd for IDM_RPT_CFG>');
   ```

   Wenn das Passwort für `IDM_RPT_DATA`, `IDMRPTUSER` und `IDM_RPT_CFG` jeweils *password*, *password1* und *password2* lautet, müssen Sie folgende Befehle ausführen:

   ```
   Select CREATE_DCS_ROLES_AND_SCHEMAS('password', 'password1');

   Select CREATE_RPT_ROLES_AND_SCHEMAS('password2');
   ```

6. Kopieren Sie den Inhalt von `get_formatted_user_dn.sql` von `C:\NetIQ\idm\apps\IdentityReporting\sql` zum Abfragewerkzeug und führen Sie ihn in der verbundenen Datenbank aus.

HINWEIS: Die Funktion `get_formatted_user_dn.sql` muss manuell hinzugefügt werden, wenn Sie die Option zur Erstellung des Datenbankschemas als **Datei** auswählen. Wenn Sie die Option zur Erstellung des Datenbankschemas als **Jetzt** oder **Start** auswählen, fügt das Installationsprogramm diese Funktion zur Datenbank hinzu.

Konfigurieren des Schemas „Create_rpt_roles_and_schemas.sql“ gegen eine Oracle-Datenbank

1. Melden Sie sich bei SQL Developer als Datenbankadministrator an.
2. Erstellen Sie `Create_rpt_roles_and_schemas`, indem Sie den Inhalt des folgenden SQL in SQL Developer kopieren und ihn gegen die verbundene Datenbank ausführen:

```
alter session set "_ORACLE_SCRIPT"=true;

CREATE OR REPLACE PROCEDURE create_rpt_roles_and_schemas(
   idm_rpt_cfg_password character varying)
AUTHID CURRENT_USER
AS
   cnt number;
BEGIN
   /* Create user IDM_RPT_CFG if it does not exist */
   select count(*) into cnt from ALL_USERS WHERE USERNAME =
'IDM_RPT_CFG';
   IF cnt = 0 THEN
       execute immediate 'CREATE USER idm_rpt_cfg IDENTIFIED BY ' ||
idm_rpt_cfg_password;
       DBMS_OUTPUT.put_line('Created user idm_rpt_cfg');
   END IF;

   /* Grant rights to the idm_rpt_cfg user */
   execute immediate 'GRANT CREATE SESSION, CREATE TABLE, CREATE VIEW,
CREATE PROCEDURE, CREATE SEQUENCE, CREATE TRIGGER, UNLIMITED TABLESPACE
to idm_rpt_cfg';
   DBMS_OUTPUT.put_line('Granted rights to user idm_rpt_cfg');
   execute immediate 'alter session set "_ORACLE_SCRIPT"=true';
   execute immediate 'alter session set "_ORACLE_SCRIPT"=false';
END;
/
exec CREATE_RPT_ROLES_AND_SCHEMAS('Novell123');
/
alter session set "_ORACLE_SCRIPT"=false;
/
```

3. Melden Sie sich als Systembenutzer an und erstellen Sie `Create_dcs_roles_and_schemas`, indem Sie den Inhalt des folgenden SQL in SQL Developer kopieren und ihn gegen die verbundene Datenbank ausführen:

```
alter session set "_ORACLE_SCRIPT"=true;

CREATE OR REPLACE PROCEDURE create_dcs_roles_and_schemas(
   idm_rpt_data_password character varying,
   idmrptuser_password character varying)
AUTHID CURRENT_USER
AS
   cnt number;
BEGIN
/* Create user IDM_RPT_DATA if it does not exist already */
   select count(*) into cnt from ALL_USERS WHERE USERNAME =
'IDM_RPT_DATA';
   IF cnt = 0 THEN
       execute immediate 'CREATE USER idm_rpt_data IDENTIFIED BY ' ||
idm_rpt_data_password;
       DBMS_OUTPUT.put_line('Created user idm_rpt_data');
   END IF;

   /* Grant rights to the idm_rpt_data user */
   execute immediate 'GRANT CREATE SESSION, CREATE TABLE, CREATE VIEW,
CREATE PROCEDURE, CREATE SEQUENCE, CREATE TRIGGER, UNLIMITED TABLESPACE
to idm_rpt_data';
   execute immediate 'GRANT CREATE PUBLIC SYNONYM to IDM_RPT_DATA';
   execute immediate 'GRANT SELECT ON DBA_SEGMENTS TO IDM_RPT_DATA';
   DBMS_OUTPUT.put_line('Granted rights to user idm_rpt_data');
   /* Create user IDMRPTUSER if it does not exist */
   select count(*) into cnt from ALL_USERS WHERE USERNAME =
'IDMRPTUSER';
   IF cnt = 0 THEN
       execute immediate 'CREATE USER idmrptuser IDENTIFIED BY ' ||
idmrptuser_password;
       DBMS_OUTPUT.put_line('Created user idmrptuser');
   END IF;

   /* Grant rights to the idmrptuser user */
   execute immediate 'GRANT CREATE SESSION to idmrptuser';
   execute immediate 'GRANT SELECT ON sys.all_tables TO idmrptuser';
   DBMS_OUTPUT.put_line('Granted rights to user idmrptuser');
END;
/
```

4 Führen Sie zum Erstellen der Rolle IDM_RPT_CFG den folgenden Befehl aus:

```
begin
CREATE_RPT_ROLES_AND_SCHEMAS('<Set pwd for IDM_RPT_CFG>');
end;
```

Wenn das Passwort für IDM_RPT_CFG zum Beispiel *password* lautet, müssen Sie folgenden Befehl ausführen:

```
begin
CREATE_RPT_ROLES_AND_SCHEMAS('password');
end;
```

5 Kopieren Sie den Inhalt von `get_formatted_user_dn-oracle.sql` zu SQL Developer aus `C:\NetIQ\idm\apps\IdentityReporting\sql` und führen Sie ihn in der verbundenen Datenbank aus.

HINWEIS: Die Funktion `get_formatted_user_dn.sql` muss der Datenbank manuell hinzugefügt werden, wenn Sie die Option zur Erstellung des Datenbankschemas als **Datei** auswählen. Wenn Sie die Option zur Erstellung des Datenbankschemas als **Jetzt** oder **Start** auswählen, fügt das Installationsprogramm diese Funktion zur Datenbank hinzu.

Konfigurieren des Schemas „Create_rpt_roles_and_schemas.sql“ in einer Oracle-Datenbank

1 Führen Sie `delete_create_dcs_roles_and_schemas-mssql.sql` und `delete_get_formatted_user_dn-mssql.sql` aus.

2 Fügen Sie der Datenbank die erforderlichen Rollen mit `create_dcs_roles_and_schemas.mssql` und `create_rpt_roles_and_schemas.mssql` aus `C:\NetIQ\idm\apps\IdentityReporting\sql` hinzu.

3 Melden Sie sich bei SQL Developer als Datenbankadministrator an.

4 Kopieren Sie zum Erstellen der Verfahren `Create_rpt_roles_and_schemas` und `Create_dcs_roles_and_schemas` den Inhalt von `create_dcs_roles_and_schemas.mssql` und `create_rpt_roles_and_schemas.mssql` zu SQL Developer und führen Sie ihn in der verbundenen Datenbank aus.

5 Führen Sie zum Erstellen der Rollen`IDM_RPT_DATA, IDM_RPT_CFG` und `IDMRPTUSER` die folgenden Befehle in der angegebenen Reihenfolge aus:

```
execute CREATE_DCS_ROLES_AND_SCHEMAS '<Passwort für IDM_RPT_DATA festlegen>', '<Passwort für IDMRPTUSER festlegen>'
```

```
execute CREATE_DCS_ROLES_AND_SCHEMAS '<Passwort für IDM_RPT_DATA festlegen>', '<Passwort für IDMRPTUSER festlegen>'
```

6 Kopieren Sie den Inhalt von `get_formatted_user_dn.sql` zu SQL Developer aus `C:\NetIQ\idm\apps\IdentityReporting\sql` und führen Sie ihn in der verbundenen Datenbank aus.

Löschen der Datenbank-Prüfsummen

1 Navigieren Sie zu den folgenden `.sql`-Dateien in `C:\NetIQ\idm\apps\IdentityReporting\sql`.

- `DbUpdate-01-run-as-idm_rpt_cfg.sql`
- `DbUpdate-02-run-as-idm_rpt_cfg.sql`
- `DbUpdate-03-run-as-idm_rpt_data.sql`
- `DbUpdate-04-run-as-idm_rpt_data.sql`
- `DbUpdate-05-run-as-idm_rpt_data.sql`
- `DbUpdate-06-run-as-idm_rpt_cfg.sql`

2 Löschen der Datenbank-Prüfsummen

2a Soll der Befehl „clearchsum“ mit jeder `.sql`-Datei ausgeführt werden, tragen Sie die folgende Zeile am Anfang der einzelnen Dateien ein:

```
update DATABASECHANGELOG set MD5SUM = NULL;
```

Der bearbeitete Inhalt sieht in etwa wie folgt aus:

```
--
**********************************************************************
**
-- Update Database Script
--
**********************************************************************
**
-- Change Log: IdmDcsDataDropViews.xml
-- Ran at: 2/23/18 5:17 PM
-- Against: IDM_RPT_CFG@jdbc:oracle:thin:@192.99.170.20:1521/orcl
-- Liquibase version: 3.5.1
--
**********************************************************************
**
update databasechangelog set md5sum = null;
```

2b Führen Sie die einzelnen `.sql`-Dateien jeweils mit dem zugehörigen Benutzer aus.

3 Übernehmen Sie die Änderungen in die Datenbank.

Bereitstellen von REST-APIs für Identity Reporting

Identity Reporting umfasst mehrere REST-APIs, die verschiedene Funktionen für die Berichterstellung bereitstellen. Die Authentifizierung dieser REST-APIs erfolgt über das OAuth2-Protokoll.

Auf Tomcat werden `rptdoc war` und `dcsdoc war` automatisch bei der Installation von Identity Reporting bereitgestellt.

Verbinden mit einer entfernten PostgreSQL-Datenbank

Wenn die PostgreSQL-Datenbank auf einem separaten Server installiert ist, müssen Sie die Standardeinstellungen in den Dateien `postgresql.conf` und `pg_hba.conf` in der entfernten Datenbank ändern.

1 Ändern Sie die Überwachungsadresse in der Datei `postgresql.conf`.

Standardmäßig kann mit PostgreSQL die localhost-Verbindung überwacht werden. Eine entfernte TCP/IP-Verbindung ist nicht zulässig. Soll eine entfernte TCP/IP-Verbindung überwacht werden, fügen Sie den folgenden Eintrag in die Datei `C:\NetIQ\idm\apps\postgres\data\postgresql.conf` ein:

```
listen_addresses = '*'
```

Wenn der Server mehrere Schnittstellen umfasst, können Sie eine bestimmte zu überwachende Schnittstelle festlegen.

2 Fügen Sie einen Eintrag für die Client-Authentifizierung in die Datei `pg_hba.conf` ein.

Standardmäßig akzeptiert PostgreSQL ausschließlich Verbindungen von `localhost`. Entfernte Verbindungen werden verweigert. Dies wird mithilfe einer Zugriffssteuerungsregel überwacht, mit dem sich ein Benutzer über eine IP-Adresse anmelden kann, sobald ein gültiges Passwort (das md5-Schlüsselwort) angegeben wurde. Soll eine entfernte Verbindung akzeptiert werden, fügen Sie den folgenden Eintrag in die Datei `C:\NetIQ\idm\apps\postgres\data\pg_hba.conf` ein:

```
host all all 0.0.0.0/0 md5
```

Beispiel: 192.168.104.24/26 trust

Dies funktioniert nur bei IPv4-Adressen. Bei IPv6-Adressen fügen Sie den folgenden Eintrag ein:

```
host all all ::0/0 md5
```

Soll eine Verbindung von mehreren Client-Computern in einem bestimmten Netzwerk zugelassen werden, geben Sie die Netzwerkadresse im CIDR-Adressformat in diesem Eintrag an.

Die Datei „pg_hba.conf“ unterstützt die nachfolgenden Formate für die Client-Authentifizierung.

- Lokale Datenbank Benutzer Authentifizierungsmethode [Authentifizierungsoption]
- Host-Datenbank Benutzer CIDR-Adresse Authentifizierungsmethode [Authentifizierungsoption]
- hostssl-Datenbank Benutzer CIDR-Adresse Authentifizierungsmethode [Authentifizierungsoption]
- hostnossl-Datenbank Benutzer CIDR-Adresse Authentifizierungsmethode [Authentifizierungsoption]

Anstelle des CIDR-Adressformats können Sie die IP-Adresse und die Netzwerkmaske in separate Felder im folgenden Format eingeben:

- Host-Datenbank Benutzer IP-Adresse IP-Maske Authentifizierungsmethode [Authentifizierungsoption]
- hostssl-Datenbank Benutzer IP-Adresse IP-Maske Authentifizierungsmethode [Authentifizierungsoption]
- hostnossl-Datenbank Benutzer IP-Adresse IP-Maske Authentifizierungsmethode [Authentifizierungsoption]

3 Testen Sie die entfernte Verbindung.

3a Starten Sie den entfernten PostgreSQL-Server neu.

3b Melden Sie sich mit dem Benutzernamen und dem Passwort entfernt beim Server an.

Schritte nach der Installation für Identity Reporting

Wenn Sie während der Installation bei der Aufforderung, `ein Schema für Identity Reporting zu erstellen`, die Option "Start" oder "Datei" wählen, müssen Sie die Datenquelle manuell über die Benutzeroberfläche von Identity Reporting hinzufügen. Navigieren Sie zum Hinzufügen zu der Option **Datenquellen**, klicken Sie auf **Hinzufügen** und wählen Sie dann `IDMDCSDataSource` aus der Liste aus.

Starten Sie außerdem Tomcat neu, nachdem Sie ihn einmal gestartet haben, um sicherzustellen, dass die verfügbare Datenbank ordnungsgemäß läuft.

OpenText Identity Manager aktivieren

Zum Installieren und Ausführen von OpenText Identity Manager benötigen Sie keinen Aktivierungscode. Wenn Sie keinen Aktivierungscode angeben, ist OpenText Identity Manager nach Ablauf von 90 Tagen ab der Installation jedoch nicht mehr nutzbar. Sie können OpenText Identity Manager jederzeit während oder auch nach dieser 90-Tage-Frist aktivieren. Weitere Informationen finden Sie unter Aktivieren von OpenText Identity Manager im *Überblick und Planungshandbuch zu OpenText™ Identity Manager CE 24.4 (v4.10)*.

IV Konfigurieren von OpenText Identity Manager im FIPS-Modus

OpenText Identity Manager nutzt die FIPS-konformen (Federal Information Processing Standards) Funktionen, um die Sicherheitsanforderungen von US-Bundesbehörden und Kunden mit hochsicheren Umgebungen zu erfüllen. Die FIPS 140-2 Standards regeln die Implementierung und Kommunikation von kryptographischer Software. Bouncy Castle verwendet einen Open Source JCA-Anbieter, der nach FIPS 140-2 Level 1 zertifiziert ist. Der Anbieter basiert auf dem etablierten und bekannten Open-Source-Kryptographie-Anbieter Bouncy Castle. Dieses Kapitel enthält Informationen zur Konfiguration und zum Betrieb von OpenText Identity Manager im FIPS-Modus.

HINWEIS:

- SSPR unterstützt den FIPS-Modus nicht. Sie müssen die Nicht-FIPS-SSPR-Einrichtung auf einen anderen Server migrieren. Weitere Informationen finden Sie unter Sichern von Konfigurationsinformationen und Importieren von Konfigurationsinformationen im *Self Service Password Reset 4.7 Administration Guide* (NetIQ-Administrationshandbuch für die Funktion zum Zurücksetzen von Passwörtern per Selbstbedienung).
- Vergewissern Sie sich, dass das Passwort des Master-Schlüsselspeichers mit dem Passwort des Tomcat-Schlüsselspeichers identisch ist. Weitere Informationen zum Ändern des Passworts finden Sie unter „Speichern des Passworts für das Configupdate-Dienstprogramm (Optional)“, auf Seite 75.
- Um OpenText eDirectory im FIPS-Modus zu konfigurieren, navigieren Sie zum Verzeichnis `HKLM\SOFTWARE\Novell\nici_x64` und ändern Sie „Restriction Level“ (Beschränkungsniveau) von 0 zu 1. Weitere Informationen finden Sie unter Bedienen von OpenText eDirectory im FIPS-Modus (https://www.netiq.com/documentation/edirectory-93/edir_install/data/b1gnsxb4.html).
- Um FIPS für Fanout-Agents zu aktivieren, generieren Sie eine Keystore-Datei im `config`-Ordner, bevor Sie die Sicherheitsverbesserung aktivieren.

Die folgenden Abschnitte enthalten Informationen zur Konfiguration und zum Betrieb von OpenText Identity Manager im FIPS-Modus.

- Kapitel 5, „Konfigurieren von JRE für FIPS“, auf Seite 123
- Kapitel 6, „Konfigurieren von OpenText Identity Manager Engine im FIPS-Modus“, auf Seite 125
- Kapitel 7, „Konfigurieren von Remote Loader im FIPS-Modus“, auf Seite 127
- Kapitel 8, „Konfigurieren des Fan-out-Agenten im FIPS-Modus“, auf Seite 129
- Kapitel 9, „Konfigurieren von Identity Applications und Identity Reporting im FIPS-Modus“, auf Seite 131

5 Konfigurieren von JRE für FIPS

So konfigurieren Sie JRE für den `nur-genehmigt`-Modus von BCFIPS:

1 Fügen Sie die BCFIPS `.jar`-Dateien zum Java-Klassenpfad hinzu.

Die folgenden BCFIPS-Dateien sind erforderlich:

- `bc-fips-1.0.2.5.jar`
- `bcpkix-fips-1.0.7.jar`
- `bctls-fips-1.0.19.jar`

HINWEIS: Die oben genannten JAR-Dateien können Sie über die folgenden Maven-Repositorys herunterladen:

- bc-fips (https://mvnrepository.com/artifact/org.bouncycastle/bc-fips)
- bcpkix-fips (https://mvnrepository.com/artifact/org.bouncycastle/bcpkix-fips)
- bctls-fips (https://mvnrepository.com/artifact/org.bouncycastle/bctls-fips)

---

2 Bearbeiten Sie die Datei `java.security` im Verzeichnis `<jre-root>/conf/security` und legen Sie eine BCFIPS-definierte Java-Systemeigenschaft fest.

Öffnen Sie die obige Datei für die JRE, die den Web-Container unter `<jre-root>/conf/security/java.security` hostet, in einem Texteditor. Suchen Sie die Liste der Sicherheitsanbieter, kommentieren Sie alle vorhandenen Anbieter aus und ersetzen Sie die Einträge wie folgt:

- `security.provider.1=BCFIPS`
- `security.provider.2=BCJSSE`
- `security.provider.3=SunJSSE`
- `security.provider.4=SUN`
- `security.provider.5=SunJCE`

Der SunJSSE-Anbieter (Java 11) ist erforderlich, da OSP bei der Initialisierung seiner Truststores bestimmte `TrustManager`-Implementierungen benötigt. Neben den Änderungen an den Sicherheitsanbietern muss auch die BCFIPS-JSSE-`KeyManager`-Implementierung verwendet werden. Dies ist hauptsächlich deshalb notwendig, weil bestimmte für FIPS erforderliche Festlegungen zu Schlüsseln aufgrund von Mängeln in der Sun-Implementierung nicht vorgenommen werden können. Dies geschieht durch Ersetzen der folgenden Zeile in `java.security`:

`ssl.KeyManagerFactory.algorithm=SunX509`

durch

`ssl.KeyManagerFactory.algorithm=PKIX`

Es ist auch besser, ältere SSL- und TLS-Algorithmen zu deaktivieren. Dies liegt daran, dass die für SSL-/TLS-Versionen vor TLS v2.0 erforderlichen Algorithmen nicht im `genehmigt`-Modus von BCFIPS verfügbar sind. Suchen Sie zum Deaktivieren der älteren Algorithmen den Eintrag `jdk.tls.disabledAlgorithms`.

Beispiel:

```
jdk.tls.disabledAlgorithms=SSLv3, RC4, MD5withRSA, DH keySize < 1024, \
EC keySize < 224, DES40_CBC, RC4_40, 3DES_EDE_CBC
```

Fügen Sie TLSv1, TLSv1.1 und TLSv1.2 zur Liste hinzu:

```
jdk.tls.disabledAlgorithms=SSLv3, TLSv1, TLSv1.1, TLSv1.2, RC4,
MD5withRSA, DH keySize < 1024, \ EC keySize < 224, DES40_CBC, RC4_40,
3DES_EDE_CBC
```

Die Deaktivierung von TLSv1 und TLSv1.1 ist optional, verhindert allerdings kryptische Fehlermeldungen, wenn OSP versucht, sich sicher mit Diensten (z. B. LDAP) zu verbinden, die nur TLS 1.1 oder früher unterstützen. Die Fehlermeldungen, die angezeigt werden, wenn die früheren TLS-Versionen deaktiviert sind, sind verständlicher und weisen direkt auf das Problem hin.

3 Fügen Sie der Umgebungsvariablen die folgenden Werte hinzu:

```
IS_FIPS_ENABLED=true

BC_FIPS_VERSION=1.0.2.5

JAVA_OPTS =" -Dorg.bouncycastle.fips.approved_only=true  -
Dorg.bouncycastle.rsa.allow_multi_use=true"

CLASSPATH=C:\NetIQ\Common\JRE\lib\bc-fips-1.0.2.5.jar
```

HINWEIS: Für den Zugriff auf `dxcmd` über Port 636 aktivieren Sie in den LDAP-Einstellungen das SSL EC-Zertifikat.

---

4 Navigieren Sie zum Ordner `C:\NetIQ\Common\JRE\lib\security`.

5 Erstellen Sie eine Sicherungskopie der Datei `cacerts`.

6 Konvertieren Sie zum Unterstützen der Sicherheitserweiterung die Datei `cacerts` mit dem folgenden Kommando in `bcfks`:

```
keytool -importkeystore -srckeystore cacerts -srcstorepass changeit -
srcstoretype JKS -destkeystore cacerts -deststorepass changeit -
deststoretype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
$CLASSPATH
```

HINWEIS: OpenText eDirectory 8.8 (oder früher) kann nicht mit sicherem LDAP verwendet werden, da es nur TLS 1.0 unterstützt. Wenn Sie sicheres LDAP nutzen möchten, müssen Sie OpenText eDirectory 9 oder höher verwenden. Alternativ können Sie den Keystore-Standardtyp ändern. Suchen Sie den Eintrag `keystore.type=jks` oder `keystore.type=pkcs12` und ändern Sie ihn zu `keystore.type=bcfks`.

---

6 Konfigurieren von OpenText Identity Manager Engine im FIPS-Modus

Führen Sie die folgenden Schritte aus, um den FIPS-Modus auf der OpenText Identity Manager-Engine zu konfigurieren:

1. Melden Sie sich bei der OpenText Identity Console an.
2. Gehen Sie zu **IDM-Administrator** und klicken Sie auf das Aktionsmenü des Treibersatzes.
3. Navigieren Sie zu **Eigenschaften des Treibersatzes > Konfiguration des Treibersatzes > Java-Umgebungsparameter**.
4. Geben Sie in den **JVM-Optionen** Folgendes ein:

   ```
   -Djavax.net.ssl.trustStore=C:\NetIQ\Common\JRE\lib\security\cacerts -
   Djavax.net.ssl.trustStorePassword=changeit -
   Djavax.net.ssl.trustStoreType=BCFKS
   ```

5. Klicken Sie auf **Speichern**.
6. Starten Sie OpenText eDirectory neu.

7 Konfigurieren von Remote Loader im FIPS-Modus

So konfigurieren Sie den FIPS-Modus auf dem Remote Loader:

1. Legen Sie die folgenden JAR-Dateien im Ordner `C:\NetIQ\IDM\RemoteLoader\lib` ab:
   - `bc-fips-1.0.2.5.jar`
   - `bcpkix-fips-1.0.7.jar`
   - `bctls-fips-1.0.19.jar`
2. Navigieren Sie zum Ordner „Remote Loader“ und starten Sie rlconsole.
3. Erstellen und starten Sie einen Treiber. Dabei wird eine `config`-Datei in dem Ordner erstellt.
4. Fügen Sie folgende Zeile in der `config`-Datei hinzu:

   ```
   is_fips_enabled=true
   ```

5. Speichern Sie die Datei und starten Sie die RL-Instanz neu.

8 Konfigurieren des Fan-out-Agenten im FIPS-Modus

Bevor Sie den FIPS-Modus über den Fan-out-Agenten von Identity Manager konfigurieren, sollten Sie folgende Voraussetzungen beachten:

- Starten Sie den Fan-out-Agenten, ohne die Sicherheitserweiterung zu aktivieren. Damit wird eine Keystore-Datei im Ordner `config` generiert.
- Legen Sie die folgenden JAR-Dateien im Ordner `C:\NetIQ\IDM\FanoutAgent\lib` ab:
  - `bc-fips-1.0.2.5.jar`
  - `bcpkix-fips-1.0.7.jar`
  - `bctls-fips-1.0.19.jar`
- Fügen Sie der Umgebungsvariablen die folgenden Werte hinzu:

  ```
  IS_FIPS_ENABLED=true

  BC_FIPS_VERSION=1.0.2.5

  JAVA_OPTS =" -Dorg.bouncycastle.fips.approved_only=true  -
  Dorg.bouncycastle.rsa.allow_multi_use=true"

  CLASSPATH=C:\NetIQ\IDM\FanoutAgent\lib\bc-fips-1.0.2.5.jar
  ```

Prozedur

1. Navigieren Sie zum Verzeichnis `C:\NetIQ\Common\JRE\conf\security`.
2. Erstellen Sie eine Sicherungskopie der Datei `java.security`.
3. Bearbeiten Sie die Datei `java.security` mit den folgenden Schritten:
   - **3a** Suchen Sie nach der Zeichenkette `Liste der Anbieter und ihrer Präferenzordnung`, kommentieren Sie alle vorhandenen Anbieter aus und fügen Sie die folgenden Einträge hinzu:

     ```
     security.provider.1=BCFIPS
     security.provider.2=BCJSSE
     security.provider.3=SunJSSE
     security.provider.4=SUN
     security.provider.5=SunJCE
     ```

   - **3b** Suchen Sie nach der Zeichenkette `ssl.KeyManagerFactory.algorithm=SunX509`, kommentieren Sie sie aus und fügen Sie Folgendes hinzu:

     ```
     ssl.KeyManagerFactory.algorithm=PKIX
     ```

   - **3c** Suchen Sie nach der Zeichenkette `jdk.tls.disabledAlgorithms` und fügen Sie TLSv1, TLSv1.1 und TLSv1.2 zur Liste hinzu.

Beispiel: `jdk.tls.disabledAlgorithms=SSLv3, TLSv1, TLSv1.1, and TLSv1.2 RC4, DES, MD5withRSA, DH keySize < 1024, \EC keySize < 224, 3DES_EDE_CBC, anon, NULL`

3d Suchen Sie nach der Zeichenkette `keystore.type`, kommentieren Sie sie aus und fügen Sie dann Folgendes hinzu:

```
keystore.type=bcfks
```

4 Navigieren Sie zum Ordner `C:\NetIQ\Common\JRE\lib\security`.

5 Erstellen Sie eine Sicherungskopie der Datei `cacerts`.

6 Um die Keystore-Datei von `jks` in `bcfks` zu konvertieren, führen Sie folgenden Befehl aus:

```
keytool -importkeystore -srckeystore
C:\NetIQ\IDM\FanoutAgent\config\keystore.jks -srcstorepass netiq123 -
srcstoretype PKCS12 -destkeystore
C:\NetIQ\IDM\FanoutAgent\config\keystore.jks -deststorepass netiq123 -
deststoretype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
$CLASSPATH
```

7 Navigieren Sie zum Ordner `C:\NetIQ\IDM\FanoutAgent\bin\` und aktualisieren Sie die folgenden Änderungen in der Datei `startAgent.bat`:

```
"%JAVA%" --add-opens=java.base/sun.security.internal.spec=ALL-UNNAMED -
Djavax.net.ssl.trustStore=C:\NetIQ\Common\JRE\lib\security\cacerts -
Djavax.net.ssl.trustStorePassword=changeit -Dkeystore.type=BCFKS -
Dorg.bouncycastle.fips.approved_only=true -
Dorg.bouncycastle.rsa.allow_multi_use=true -cp %CLASSPATH%
com.netiq.idm.fanoutagent.FanoutAgent !FILENAME! !SERVERONLY!.
```

8 Starten Sie den Fan-out-Agenten und prüfen Sie die Protokolle.

9 Konfigurieren von Identity Applications und Identity Reporting im FIPS-Modus

Bevor Sie den FIPS-Modus über Identity Reporting und Identity Applications konfigurieren, sollten Sie folgende Voraussetzungen beachten:

- Halten Sie den Tomcat-Dienst auf dem Server an, auf dem Identity Applications- und OpenText Identity Manager Reporting-Komponenten ausgeführt werden.
- Vergewissern Sie sich, dass sich der Administrator auf dem OpenText Identity Manager Engine-System bei dem Tool `dxcmd` anmelden kann.

Prozedur

1. Erstellen Sie einen neuen Ordner für FIPS. Beispiel: `C:\fips`
2. Erstellen Sie eine Sicherungskopie der folgenden Dateien im soeben erstellten Ordner:

Dateien	Vorhandener Dateipfad
`idm.jks`	`C:\netiq\idm\apps\tomcat\conf`
`osp.jks`	
`tomcat.ks`	
`encrypt-keys.pkcs12`	
`server.xml`	
`ism-configuration.properties`	
`configupdate.bat`	`C:\netiq\idm\apps\configupdate`
`configupdate.bat.properties`	

3. Navigieren Sie zu `<Einhängeort>\common\osp\misc` und kopieren Sie `osp-tomcat8-pwd-handler-<Version>.jar` in den Ordner `C:\netiq\idm\apps\tomcat\lib`.
4. Navigieren Sie zum Ordner `C:\NetIQ\IDM\apps\tomcat\bin\` und bearbeiten Sie die Datei `setenv.bat` wie folgt:
   - ```
     set JAVA_OPTS= %JAVA_OPTS% -
     Dorg.bouncycastle.fips.approved_only=true -
     Dinternal.osp.framework.fips-password=novell -
     Dorg.bouncycastle.rsa.allow_multi_use=true -
     Djavax.net.ssl.keyStoreType=BCFKS -
     Djavax.net.ssl.trustStoreType=BCFKS -
     Djavax.net.ssl.trustStore=c:\netiq\idm\apps\tomcat\conf\idm.bcfks -
     Djavax.net.ssl.trustStorePassword=novell
     ```
     ```

- `set BCFIPS_JARS=c:\netiq\common\jre\lib\bc-fips-1.0.2.5.jar;c:\netiq\common\jre\lib\bcpkix-fips-1.0.7.jar;c:\netiq\common\jre\lib\bctls-fips-1.0.19.jar`
- `set CLASSPATH=C:\NetIQ\Common\JRE\lib\bc-fips-1.0.2.5.jar;C:\NetIQ\Common\JRE\lib\bcpkix-fips-1.0.7.jar;C:\NetIQ\Common\JRE\lib\bctls-fips-1.0.19.jar;%CLASSPATH%`
- Suchen Sie nach `CATALINA_OPTS` und ändern Sie `encrypt-keys.pkcs12` zu `encrypt-keys.bcfks` sowie `storetype` zu `bcfks`.

HINWEIS: Stellen Sie sicher, dass die Werte `set JAVA_OPTS`, `set BCFIPS_JARS` und `set CLASSPATH` vor `CATALINA_OPTS` stehen.

---

5 Navigieren Sie in der Eingabeaufforderung zu `C:\NETIQ\Commom\JRE\bin` und führen Sie die folgenden Befehle aus:

```
keytool -importkeystore -srckeystore
C:\NetIQ\IDM\apps\tomcat\conf\idm.jks -srcstorepass novell -
srcstoretype PKCS12 -destkeystore
C:\NetIQ\IDM\apps\tomcat\conf\idm.bcfks -deststorepass novell -
deststoretype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
$CLASSPATH
```

```
keytool -importkeystore -srckeystore
C:\NetIQ\IDM\apps\tomcat\conf\tomcat.ks -srcstorepass -srcstoretype
PKCS12 -destkeystore C:\NetIQ\IDM\apps\tomcat\conf\tomcat.bcfks -
deststorepass -deststoretype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
$CLASSPATH
```

```
keytool -importkeystore -srckeystore
C:\NetIQ\IDM\apps\tomcat\conf\idm.jks -srcstorepass novell -
srcstoretype PKCS12 -destkeystore C:\NetIQ\IDM\apps\osp\osp.bcfks -
deststorepass novell -deststoretype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
$CLASSPATH
```

```
keytool -importkeystore -srckeystore
C:\NetIQ\IDM\apps\tomcat\conf\tomcat.ks -srcstorepass changeit -
srcstoretype PKCS12 -destkeystore C:\NetIQ\IDM\apps\osp\osp.bcfks -
deststorepass novell -deststoretype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
$CLASSPATH
```

```
java -jar <mount-location>\common\osp\misc\osp-keymanager-6.7.7.jar -
genkeys -keystore C:\NetIQ\IDM\apps\osp\osp.bcfks -storepass novell -
storetype BCFKS -application idm -providerClass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerPath
C:\NetIQ\Common\JRE\lib\bc-fips-1.0.2.5.jar -keypass novell -use
Encrypting,Signing,TLS
```

```
keytool -importkeystore -srckeystore
C:\NetIQ\IDM\apps\tomcat\conf\encrypt-keys.pkcs12 -srcstorepass
changeit -srcstoretype PKCS12 -destkeystore
C:\NetIQ\IDM\apps\tomcat\conf\encrypt-keys.bcfks -deststorepass
changeit -deststoretype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
$CLASSPATH
```

6 Bearbeiten Sie die Datei `server.xml` wie folgt:

```
<!--Connector port="8543"
protocol="org.apache.coyote.http11.Http11NioProtocol" maxThreads="150"
SSLEnabled="true" scheme="https" secure="true" clientAuth="false"
sslProtocol="TLSv1.3" keystoreFile="conf/tomcat.ks"
keystorePass="changeit" maxHttpHeaderSize="65536"
sslEnabledProtocols="TLSv1.3" /--> <Connector
protocol="com.microfocus.osp.tomcat.http.PasswordHttp11NioProtocol"
port="8543" maxThreads="150" maxHttpHeaderSize="65536"
SSLEnabled="true" scheme="https" secure="true"> <SSLHostConfig
protocol="TLS" protocols="TLSv1.3"
ciphers="TLS_DHE_DSS_WITH_AES_128_GCM_SHA256,TLS_DHE_DSS_WITH_AES_256_
GCM_SHA384,TLS_DHE_DSS_WITH_AES_128_CBC_SHA256,TLS_DHE_DSS_WITH_AES_12
8_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA256,TLS_DHE_DSS_WITH_AES_256
_CBC_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_
GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WIT
H_AES_128_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_EC
DSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECD
HE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_
ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA
_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_CCM,TLS_RSA_WITH_AES_256
_CCM,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_
RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA"
truststoreFile="C:\NetIQ\IDM\apps\osp\osp.bcfks"
truststorePassword="novell" truststoreType="BCFKS" > <Certificate
certificateKeystoreFile="C:\NetIQ\IDM\apps\tomcat\conf\tomcat.bcfks"
certificateKeystorePassword="novell" certificateKeyAlias="ssl
certificatedns" certificateKeystoreType="BCFKS" /> </SSLHostConfig> </
Connector>
```

7 Bearbeiten Sie die Datei `ism-configuration.properties` wie folgt:

```
com.netiq.idm.osp.ssl-keystore.file =
C:\\NetIQ\\IDM\\\\apps\\\\tomcat\\\\conf\\\\tomcat.bcfks

com.netiq.idm.osp.ssl-keystore.type = BCFKS

com.netiq.idm.osp.oauth-keystore.file =
C:\\\\NetIQ\\\\IDM\\\\apps\\\\osp\\\\osp.bcfks

com.netiq.idm.osp.oauth-keystore.type = BCFKS

com.netiq.rpt.ssl-keystore.file =
C:\\NetIQ\\IDM\\apps\\tomcat\\conf\\idm.bcfks

com.netiq.rpt.ssl-keystore.type = BCFKS

DirectoryService/realms/jndi/params/KEYSTORE_PATH =
C:\\NetIQ\\IDM\\apps\\tomcat\\conf\\idm.bcfks
```

```
com.sssw.fw.security.sigcert.truststore.type = BCFKS

com.netiq.idm.osp.oauth-truststore.file =
C:\\\\NetIQ\\\\IDM\\\\apps\\\\tomcat\\\\conf\\\\idm.bcfks

com.netiq.idm.ua.ldap.keystore-type = BCFKS

com.netiq.idm.osp.oauth-key-alias = ssl certificatedns
```

8 Kopieren Sie die folgenden JAR-Dateien in den Ordner `C:\NetIQ\IDM\apps\configupdate\lib`:

- `bc-fips-1.0.2.5.jar`
- `bcpkix-fips-1.0.7.jar`
- `bctls-fips-1.0.19.jar`

9 Bearbeiten Sie Folgendes unter `C:\NetIQ\IDM\apps\configupdate.bat.properties`:

```
master_keystore_type=bcfks
master_keystore=C:\NetIQ\IDM\apps\tomcat\conf\encrypt-keys.bcfks
```

10 Bearbeiten Sie Folgendes in `configupdate.bat`:

```
set "JAVA_OPTS= %JAVA_OPTS% -Dorg.bouncycastle.fips.approved_only=true
-Dinternal.osp.framework.fips-password=novell -
Dorg.bouncycastle.rsa.allow_multi_use=true -
Djavax.net.ssl.keyStoreType=BCFKS -Djavax.net.ssl.trustStoreType=BCFKS
-Djavax.net.ssl.trustStore=c:\netiq\idm\apps\tomcat\conf\idm.bcfks -
Djavax.net.ssl.trustStorePassword=novell  "

set CLASSPATH=C:\NetIQ\Common\JRE\lib\bc-fips-
1.0.2.5.jar;C:\NetIQ\Common\JRE\lib\bcpkix-fips-
1.0.7.jar;C:\NetIQ\Common\JRE\lib\bctls-fips-1.0.19.jar;%CLASSPATH%
```

11 Starten Sie das Dienstprogramm configupdate.

12 Starten Sie Tomcat.

V Installation von Designer

In diesem Abschnitt finden Sie die Schritte für die Installation von Designer für OpenText Identity Manager. Standardmäßig werden die Komponenten vom Installationsprogramm unter `C:\Netiq` installiert.

WICHTIG: Stellen Sie sicher, dass der Name des Verzeichnisses, in dem sich das Designer-Installationsprogramm befindet, kein Leerzeichen aufweist. Benennen Sie das Verzeichnis beispielsweise nicht mit `Designer Install`. Stattdessen wäre `DesignerInstall` richtig.

Wir empfehlen, dass Sie sich vor Beginn der Installation über den Installationsvorgang informieren. Weitere Informationen finden Sie unter Kapitel 10, „Planen der Installation von Designer“, auf Seite 137.

10 Planen der Installation von Designer

In diesem Abschnitt finden Sie die Voraussetzungen, die Überlegungen und die notwendige Systemeinrichtung für die Installation von Designer. Informieren Sie sich zunächst anhand der Checkliste über den Installationsvorgang.

- „Checkliste für die Installation von Designer“, auf Seite 137

Checkliste für die Installation von Designer

Wir empfehlen, vor Beginn der Installation die nachfolgenden Schritte durchzugehen:

	Checkliste
❑	1. Überprüfen Sie die Planungsdaten. Weitere Informationen finden Sie unter Teil II, „Planen der Installation von OpenText Identity Manager“, auf Seite 35.
❑	2. Lesen Sie die Überlegungen zur Installation von Designer, und prüfen Sie, ob der Computer den Voraussetzungen entspricht.
❑	3. Befolgen Sie die Anweisungen zum Installieren von Designer in einem der folgenden Abschnitte: ◆ „Ausführen der ausführbaren Windows-Datei“, auf Seite 139 ◆ „Verwenden der automatischen Installation“, auf Seite 139
❑	4. Installieren Sie die restlichen OpenText Identity Manager-Komponenten.
❑	5. (Optional) Starten Sie ein Projekt für die OpenText Identity Manager-Lösung gemäß den Anweisungen im *Administrationshandbuch zu Designer für OpenText™ Identity Manager CE 24.4 (v4.10)*.

11 Installation von Designer

Je nach Zielcomputer können Sie OpenText Identity Manager Designer wahlweise mit einer ausführbaren Datei, mit einer Binärdatei oder im Textmodus installieren. Auch die automatische Installation ist möglich.

Verschiedene OpenText Identity Manager-Komponenten nutzen Pakete in Designer. Beim Installieren von Designer fügt das Installationsprogramm automatisch bestimmte Pakete in das neue Projekt ein.

- „Ausführen der ausführbaren Windows-Datei“, auf Seite 139
- „Verwenden der automatischen Installation“, auf Seite 139
- „Installieren von Designer in einem anderen Gebietsschema als dem Systemgebietsschema“, auf Seite 140
- „Bearbeiten eines Installationspfads mit Leerzeichen“, auf Seite 141

Ausführen der ausführbaren Windows-Datei

1. Melden Sie sich mit einem Administratorkonto bei dem Computer an, auf dem Designer installiert werden soll.
2. Laden Sie die Datei `Identity_Manager_4.10_Designer_Windows.zip` vom Softwarelizenz- und Download (https://sld.microfocus.com/index)-Portal herunter.
3. Extrahieren Sie die Datei `Identity_Manager_4.10_Designer_Windows.zip`.
4. Navigieren Sie zum Ordner `designer_install`.
5. Führen Sie die Datei `install.exe` aus.
6. Befolgen Sie die Anweisungen im Assistenten, bis die Installation abgeschlossen ist.

Verwenden der automatischen Installation

Mithilfe von Skripten können Sie Designer automatisch installieren, ohne dass der Benutzer eingreifen muss. Mit der Option `-i silent` werden standardmäßige Parameterwerte für die Installation verwendet, sofern Sie nicht die Datei `designerInstaller.properties` bearbeitet haben.

1. Melden Sie sich mit einem Administratorkonto bei dem Computer an, auf dem Designer installiert werden soll.
2. Rufen Sie das Verzeichnis mit dem Installationsprogramm auf.
3. (Optional) Wenn Sie das Installationsverzeichnis und die Sprache für Designer konfigurieren möchten, führen Sie die nachfolgenden Schritte aus.
   - **3a** Öffnen Sie die Datei `designerInstaller.properties` (standardmäßig im Verzeichnis *`Pfad_zur_entpackten_Designer-Datei`*`\designer_install`).
   - **3b** Bearbeiten Sie in der Eigenschaftendatei die Werte für die folgenden Parameter:

USER_INSTALL_DIR

Gibt den Verzeichnispfad für die Installation von Designer an. Beispiel:

```
USER_INSTALL_DIR=C:\designer
```

Wenn Sie einen Pfad angeben, der nicht mit dem Verzeichnis `designer` endet, hängt das Designer-Installationsprogramm ein Verzeichnis `designer` an.

SELECTED_DESIGNER_LOCALE

Legt eine der folgenden Sprachen fest, in denen Designer nach der Installation ausgeführt werden soll:

- `zh_CN` – Chinesisch (vereinfacht)
- `zh_TW` – Chinesisch (traditionell)
- `nl` – Niederländisch
- `en` – Englisch
- `fr` – Französisch
- `de` – Deutsch
- `it` – Italienisch
- `ja` – Japanisch
- `pt_BR` – Portugiesisch (Brasilien)
- `es` – Spanisch

3c Speichern und schließen Sie die Eigenschaftendatei.

4 Führen Sie folgenden Befehl im Verzeichnis der Eigenschaftendatei aus:

```
install -i silent -f designerInstaller.properties
```

Installieren von Designer in einem anderen Gebietsschema als dem Systemgebietsschema

Sie können zusätzliche Eingabeaufforderungen mit der ausführbaren Windows-Datei verwenden, um Designer in einer anderen Sprache als der des Gebietsschemas des Systems zu installieren. Stellen Sie sich folgendes Szenario vor: Das Gebietsschema auf Ihrem Computer ist auf Deutsch festgelegt, Sie möchten Designer jedoch auf Englisch installieren.

Installationsvorgang:

1 Laden Sie die Datei `Identity_Manager_4.10_Designer_Windows.zip` herunter und extrahieren Sie sie.

2 Navigieren Sie im Ordner `Downloads` auf Ihrem Computer zum Ordner **designer_install**.

Beispiel:
`C:\Benutzer\<Benutzername>\Downloads\Identity_Manager_4.10_Designer_Windows\designer_install`

3 Öffnen Sie eine Eingabeaufforderung und führen Sie folgenden Befehl aus:

```
install.exe -i silent -l en_us
```

Mit diesem Befehl wird Designer automatisch im englischen Gebietsschema (USA) installiert. Weitere Gebietsschemata, die von Designer unterstützt werden, finden Sie in Schritt 3b im Abschnitt „Verwenden der automatischen Installation“, auf Seite 139.

Bearbeiten eines Installationspfads mit Leerzeichen

Sie können Designer in einem Verzeichnis installieren, dessen Name ein oder mehrere Leerzeichen enthält. Nach der Installation von Designer müssen Sie allerdings die Dateien `StartDesigner.bat` und `Designer.ini` bearbeiten, damit Designer ordnungsgemäß funktioniert. Ersetzen Sie die Leerzeichen jeweils manuell durch ein Escape-Zeichen („\“). Beispiel:

Änderung

```
C:\designer installation
```

in

```
C:\designer\ installation
```

VI Installation von Analyzer

In diesem Abschnitt finden Sie die Schritte für die Installation von Analyzer für OpenText Identity Manager. Analyzer ist eine Thick-Client-Komponente, die auf einer Arbeitsstation installiert wird. Mit Analyzer untersuchen und bereinigen Sie die Daten in den Systemen, die in Ihre OpenText Identity Manager-Lösung eingebunden werden sollen. Wenn Sie Analyzer in der Planungsphase einsetzen, wird ersichtlich, welche Änderungen auf welche Weise vorgenommen werden müssen.

Standardmäßig werden die Komponenten vom Installationsprogramm unter `C:\NetIQ\Analyzer` installiert.

WICHTIG: Das Analyzer-Tool ist nicht in der ISO für OpenText Identity Manager 4.10 enthalten. Wenn Analyzer bereits installiert ist, aktualisieren Sie ihn auf Version 4.8.5 und verwenden Sie ihn mit OpenText Identity Manager 4.10.

Wir empfehlen, dass Sie sich vor Beginn der Installation über den Installationsvorgang informieren. Weitere Informationen finden Sie unter „Checkliste für die Installation von Analyzer“, auf Seite 145.

12 Planen der Installation von Analyzer

In diesem Abschnitt finden Sie Anweisungen zum Vorbereiten der Installation von Analyzer für OpenText Identity Manager. Wir empfehlen, dass Sie sich vor Beginn der Installation über den Installationsvorgang informieren.

- „Checkliste für die Installation von Analyzer“, auf Seite 145

Checkliste für die Installation von Analyzer

Wir empfehlen, vor Beginn des Installationsprozesses die nachfolgenden Schritte durchzugehen:

	Checkliste
❑	1. Überprüfen Sie die Planungsdaten. Weitere Informationen finden Sie unter Teil II, „Planen der Installation von OpenText Identity Manager“, auf Seite 35.
❑	2. Lesen Sie die Überlegungen zur Installation von Analyzer und prüfen Sie, ob der Computer die Voraussetzungen erfüllt.
❑	3. Befolgen Sie die Anweisungen zum Installieren von Analyzer in einem der folgenden Abschnitte: ◆ Anweisungen zur Verwendung des Installationsassistenten finden Sie in „Ausführen der ausführbaren Windows-Datei“, auf Seite 147 ◆ Anweisungen zur automatischen Installation finden Sie in „Verwenden der automatischen Installation“, auf Seite 147.
❑	4. Informationen zum Aktivieren von Analyzer finden Sie unter Aktivieren von Analyzer im *Überblick und Planungshandbuch zu OpenText™ Identity Manager CE 24.4 (v4.10)*.

13 Installation von Analyzer

In diesem Abschnitt finden Sie die Schritte für die Installation von Analyzer und die Konfiguration Ihrer Umgebung für Analyzer.

- „Ausführen der ausführbaren Windows-Datei“, auf Seite 147
- „Verwenden der automatischen Installation“, auf Seite 147

Ausführen der ausführbaren Windows-Datei

1. Melden Sie sich mit einem Administratorkonto bei dem Computer an, auf dem Analyzer installiert werden soll.
2. Laden Sie die Datei `Identity_Manager_4.8.5_Analyzer_Windows.zip` von der OpenText-Downloads-Website herunter.
3. Extrahieren Sie die Datei `Identity_Manager_4.8.5_Analyzer_Windows.zip`.
4. Navigieren Sie zum Ordner `analyzer_install`.
5. Führen Sie die Datei `install.exe` aus.
6. Befolgen Sie die Anweisungen im Assistenten, bis die Installation abgeschlossen ist.

Verwenden der automatischen Installation

Mithilfe von Skripten kann Designer automatisch installiert werden, ohne dass der Benutzer eingreifen muss. Mit der Option `-i silent` werden standardmäßige Parameterwerte für die Installation verwendet, sofern Sie nicht die Datei `analyzerInstaller.properties` bearbeitet haben.

1. Melden Sie sich mit einem Administratorkonto bei dem Computer an, auf dem Analyzer installiert werden soll.
2. Rufen Sie das Verzeichnis mit dem Installationsprogramm auf.
3. (Optional) Wenn Sie das Installationsverzeichnis und die Sprache für Analyzer konfigurieren möchten, führen Sie folgende Schritte aus.

   3a Öffnen Sie die Datei `analyzerInstaller.properties` (standardmäßig im Verzeichnis *`Pfad_zur_entpackten_Analyzer-Datei`*`\analyzerInstall`).

   3b Bearbeiten Sie in der Eigenschaftendatei die Werte für die folgenden Parameter:

   USER_INSTALL_DIR

   Gibt den Verzeichnispfad für die Installation von Analyzer an. Beispiel:

   ```
   USER_INSTALL_DIR=C:\analyzer
   ```

   Wenn Sie einen Pfad angeben, der nicht mit dem Verzeichnis `analyzer` endet, fügt das Analyzer-Installationsprogramm ein Verzeichnis `analyzer` automatisch an.

SELECTED_ANALYZER_LOCALE

Legt eine der folgenden Sprachen fest, in denen Analyzer nach der Installation gestartet werden soll:

- `zh_CN` – Chinesisch (vereinfacht)
- `zh_TW` – Chinesisch (traditionell)
- `nl` – Niederländisch
- `en` – Englisch
- `fr` – Französisch
- `de` – Deutsch
- `it` – Italienisch
- `ja` – Japanisch
- `pt_BR` – Portugiesisch (Brasilien)
- `es` – Spanisch

3c Speichern und schließen Sie die Eigenschaftendatei.

4 Führen Sie folgenden Befehl im Verzeichnis der Eigenschaftendatei aus:

```
install -i silent -f analyzerInstaller.properties
```

14 Aufgaben nach Abschluss der Installation

Nach der Installation von Identity Manager sollten sie die Treiber konfigurieren, die Sie entsprechend den Richtlinien und Anforderungen, die durch Ihren Geschäftsprozess definiert sind, installiert haben. Zum Erfassen von Revisionsereignissen müssen Sie außerdem Sentinel Log Management für IGA konfigurieren. Zu den Aufgaben nach der Installation gehören in der Regel die folgenden Elemente:

- „Konfigurieren eines verbundenen Systems“, auf Seite 149
- „Erstellen und Konfigurieren eines Treibersatzes“, auf Seite 149
- „Erstellen eines Driver“, auf Seite 152
- „Definieren von Richtlinien“, auf Seite 153
- „Verwalten von Treiberaktivitäten“, auf Seite 153

Konfigurieren eines verbundenen Systems

Identity Manager aktiviert Anwendungen, Verzeichnisse und Datenbanken zur Freigabe von Informationen. Treiberspezifische Konfigurationsanweisungen finden Sie in der Dokumentation zu Identity Manager-Treibern (https://www.netiq.com/documentation/identity-manager-4.10-drivers/).

Erstellen und Konfigurieren eines Treibersatzes

Ein Treibersatz ist ein Container, der Identity Manager-Treiber enthält. Es kann immer nur ein Treibersatz mit einem Server verbunden sein. Ein Treibersatz wird mit dem Designer-Tool erstellt. Wenn ein Server bereits mit einem Treibersatz verbunden ist und Sie den Server dann einem neuen Treibersatz zuweisen, wird der Server aus dem ursprünglichen Treibersatz entfernt.

Identity Manager gibt vor, dass für Treibersätze Passwortrichtlinien vorhanden sind, um die Passwortsynchronisierung mit dem Identitätsdepot zu unterstützen. Dazu wird das Standard-Universalpasswort-Richtlinienpaket in Identity Manager verwendet, oder Sie erstellen eine Passwortrichtlinie basierend auf den Anforderungen Ihrer Organisation. Die Passwortrichtlinie muss jedoch das `DirMXL-PasswordPolicy`-Objekt enthalten. Erstellen sie das Richtlinienobjekt, falls es nicht im Identitätsdepot vorhanden ist.

- „Erstellen von Treibersätzen“, auf Seite 150
- „Zuweisen der Standardpasswortrichtlinie zu Treibersätzen“, auf Seite 150
- „Erstellen des Passwortrichtlinienobjekts im Identitätsdepot“, auf Seite 150
- „Erstellen einer benutzerdefinierten Passwortrichtlinie“, auf Seite 151
- „Erstellen des Standard-Benachrichtigungssammlungs-Objekts im Identitätsdepot“, auf Seite 152

Erstellen von Treibersätzen

Designer für Identity Manager bietet viele Einstellungen zum Erstellen und Konfigurieren von Treibersätzen. Diese Einstellungen ermöglichen die Angabe von globalen Konfigurationswerten, Treibersatzpaketen, Passwörtern für Treibersätze, Protokollstufen, Trace-Stufen und Java-Umgebungsparametern. Weitere Informationen finden Sie unter „Konfigurieren von Treibersätzen“ im *Administrationshandbuch zu Designer für OpenText™ Identity Manager CE 24.4 (v4.10)*.

Zuweisen der Standardpasswortrichtlinie zu Treibersätzen

Sie müssen jedem Treibersatz im Identitätsdepot das DirMXL-Passwortrichtlinienobjekt hinzufügen. Dieses Richtlinienobjekt ist im Standard-Universalpasswort-Richtlinienpaket von Identity Manager enthalten. Die Standardrichtlinie installiert und weist eine Universalpasswortrichtlinie zu, um zu kontrollieren, wie die Identity Manager-Engine automatisch zufällige Passwörter für Treiber generiert.

Alternativ müssen Sie zur Verwendung einer benutzerdefinierten Passwortrichtlinie das Passwortrichtlinienobjekt und die Richtlinie erstellen. Weitere Informationen hierzu finden Sie in „Erstellen des Passwortrichtlinienobjekts im Identitätsdepot“, auf Seite 150 und „Erstellen einer benutzerdefinierten Passwortrichtlinie“, auf Seite 151.

1. Öffnen Sie Ihr Projekt in Designer.
2. Erweitern Sie Ihr Projekt im Bereich „Gliederung“.
3. Erweitern Sie **Paketkatalog > Allgemein** und prüfen Sie, ob das Standardpaket mit den Universalpasswortrichtlinien vorhanden ist.
4. (Bedingt) Führen Sie folgende Schritte durch, wenn das Passwortrichtlinienpaket nicht bereits in Designer aufgelistet ist:
   - **4a** Klicken Sie mit der rechten Maustaste auf **Paketkatalog**.
   - **4b** Wählen Sie **Paket importieren** aus.
   - **4c** Wählen Sie **Standard-Universalpasswortrichtlinie für Identity Manager** aus, und klicken Sie anschließend auf **OK**.

     Sie müssen möglicherweise die Option **Nur Basispaket anzeigen** deaktivieren, um sicherzustellen, dass in der Tabelle alle verfügbaren Pakete angezeigt werden.
5. Wählen Sie jeden Treibersatz aus, und weisen Sie ihm die Passwortrichtlinie zu.

Erstellen des Passwortrichtlinienobjekts im Identitätsdepot

Erstellen Sie das Objekt `DirMXL-PasswordPolicy` im Designer oder mit dem ldapmodify-Dienstprogramm, falls es im Identitätsdepot nicht vorhanden ist. Weitere Informationen zur Vorgehensweise in Designer finden Sie im Abschnitt „Konfigurieren von Treibersätzen“ in *Administrationshandbuch zu Designer für OpenText™ Identity Manager CE 24.4 (v4.10)*. Gehen Sie zur Verwendung des ldapmodify-Dienstprogramms folgendermaßen vor:

1. Erstellen Sie in einem Texteditor eine LDAP-Datenaustauschformat(LDIF)-Datei mit den folgenden Attributen:

```
dn: cn=DirXML-PasswordPolicy,cn=Password Policies,cn=Security
changetype: add
nsimPwdRuleEnforcement: FALSE
nspmSpecialAsLastCharacter: TRUE
nspmSpecialAsFirstCharacter: TRUE
nspmSpecialCharactersAllowed: TRUE
nspmNumericAsLastCharacter: TRUE
nspmNumericAsFirstCharacter: TRUE
nspmNumericCharactersAllowed: TRUE
nspmMaximumLength: 64
nspmConfigurationOptions: 596
passwordUniqueRequired: FALSE
passwordMinimumLength: 1
passwordAllowChange: TRUE
objectClass: nspmPasswordPolicy

dn: cn=DirXML-PasswordPolicy,cn=Password Policies,cn=Security
changetype: modify
add: nsimAssignments
nsimAssignments: <driverset LDAP dn>
```

HINWEIS: Durch Kopieren des unveränderten Inhalts werden in der Datei möglicherweise Sonderzeichen eingefügt. Wenn Sie beim Hinzufügen dieser Attribute zum Identitätsdepot eine `ldif_record() = 17`-Fehlermeldung erhalten, fügen Sie ein zusätzliches Leerzeichen zwischen die beiden DNs ein.

---

2 Möchten Sie dem Identitätsdepot das Objekt DirMXL-PasswordPolicy hinzufügen, importieren Sie die Attribute der Datei, indem Sie `ldapmodify.exe` im Verzeichnis `install/utilities` des OpenText Identity Manager-Installationsdateisatzes ausführen.

Erstellen einer benutzerdefinierten Passwortrichtlinie

Erstellen Sie eine neue Richtlinie basierend auf den Anforderungen Ihres Unternehmens, statt die Standard-Passwortrichtlinie in Identity Manager zu verwenden. Sie können eine Passwortrichtlinie der gesamten Baumstruktur, einem Partitionsstammcontainer, einem Container oder einem bestimmten Benutzer zuweisen. Es empfiehlt sich, Passwortrichtlinien einer möglichst hohen Ebene im Baum zuzuweisen, um die Verwaltung zu vereinfachen. Weitere Informationen finden Sie unter Creating Password Policies im *Administrationshandbuch zur Passwortverwaltung 3.3.2*.

HINWEIS: Sie müssen den Treibersätzen auch das DirXML-Passwortrichtlinienobjekt zuweisen. Weitere Informationen finden Sie unter „Erstellen des Passwortrichtlinienobjekts im Identitätsdepot“, auf Seite 150.

Erstellen des Standard-Benachrichtigungssammlungs-Objekts im Identitätsdepot

Die Standard-Benachrichtigungssammlung ist ein Identitätsdepotobjekt, das einen Satz von Schablonen für Email-Benachrichtigungen enthält, sowie ein Server, der zum Senden von aus Schablonen erstellten Emails verwendet wird. Erstellen Sie das Objekt "Standard-Benachrichtigungssammlung" mit Designer, falls es im Identitätsdepot nicht vorhanden ist.

1. Öffnen Sie Ihr Projekt in Designer.
2. Erweitern Sie Ihr Projekt im Bereich „Gliederung“.
3. Klicken Sie mit der rechten Maustaste auf das Identitätsdepot und anschließend auf **Identitätsdepot-Eigenschaften**.
4. Klicken Sie auf **Pakete** und anschließend auf das Symbol **Pakete hinzufügen**.
5. Wählen Sie alle Pakete mit Benachrichtigungsschablonen aus, und klicken Sie anschließend auf **OK**.
6. Klicken Sie auf **Anwenden**, um die Pakete mit dem Vorgang **Installieren** zu installieren.
7. Stellen Sie die Benachrichtigungsschablonen im Identitätsdepot bereit.

Erstellen eines Driver

Erstellen Sie Treiber mit der Paketverwaltungsfunktion in Designer. Erstellen Sie ein Treiberobjekt und eine Treiberkonfiguration für jeden Identity Manager-Treiber, den Sie verwenden möchten. Das Treiberobjekt enthält Konfigurationsparameter und Richtlinien für diesen Treiber. Installieren Sie im Zuge der Erstellung eines Treiberobjekts die Treiberpakete und bearbeiten Sie dann die Treiberkonfiguration entsprechend Ihrer Umgebung.

Die Treiberpakete enthalten einen Standardsatz von Richtlinien. Diese Richtlinien unterstützen Sie beim Implementieren Ihres Datenfreigabemodells. In den meisten Fällen richten Sie einen Treiber unter Verwendung der zum Lieferumfang gehörenden Standardkonfiguration ein und ändern anschließend die Treiberkonfiguration gemäß den Anforderungen Ihrer Umgebung. Stellen Sie den Treiber nach seiner Erstellung und Konfiguration im Identitätsdepot bereit und starten Sie ihn. Im Allgemeinen werden im Treibererstellungsprozess die folgenden Schritte durchgeführt:

1. Importieren der Treiberpakete
2. Installieren der Treiberpakete
3. Treiberobjekt konfigurieren
4. Bereitstellen des Treiberobjekts
5. Starten des Treiberobjekts

Treiberspezifische und weitere Informationen finden Sie im entsprechenden Handbuch für die Treiberimplementierung auf der Website für Identity Manager-Treiber (https://www.netiq.com/documentation/identity-manager-4.10-drivers/).

Definieren von Richtlinien

Mit Richtlinien können Sie den Informationsfluss in das und aus dem Identitätsdepot an eine bestimmte Umgebung anpassen. Beispielsweise verwendet ein Unternehmen „inetOrgPerson“ als Hauptbenutzerklasse, während in einem anderen Unternehmen „Userr“ als Hauptbenutzerklasse verwendet wird. In diesem Fall wird eine Richtlinie erstellt, die der Identity Manager-Engine mitteilt, welche Benutzerklasse auf dem jeweiligen System aufgerufen wird. OpenText Identity Manager wendet diese Richtlinie immer dann an, wenn Operationen, die sich auf Benutzer beziehen, zwischen verbundenen Systemen übertragen werden.

Außerdem können Sie mithilfe von Richtlinien neue Objekte erstellen, Attributwerte aktualisieren, Schema-Transformationen ausführen, Übereinstimmungskriterien definieren und OpenText Identity Manager-Verknüpfungen verwalten.

Wir empfehlen Ihnen, Richtlinien für Treiber entsprechend Ihrer Geschäftsanforderungen mit dem Designer zu definieren. Detaillierte Informationen zu Richtlinien finden Sie im Handbuch *OpenText™ Identity Manager CE 24.4 (v4.10) – Erstellen von Richtlinien mit Designer* und im *Handbuch über Richtlinien in OpenText™ Identity Manager CE 24.4 (v4.10)*. Informationen zu Dokumenttypdefinitionen (DTD), die Identity Manager verwendet, finden Sie in der Identity Manager DTD-Referenz (https://www.netiq.com/documentation/identity-manager-developer/dtd-documentation.html). Diese Ressourcen umfassen Folgendes:

- Eine detaillierte Beschreibung der zur Verfügung stehenden Richtlinien.
- Ein ausführliches Benutzer- und Referenzhandbuch zum Richtlinien-Builder mit Beispielen und Syntaxbeschreibungen der einzelnen Bedingungen, Aktionen, Nomen und Verben.
- Informationen darüber, wie Sie Richtlinien mithilfe von XSLT-Formatvorlagen erstellen können.

Verwalten von Treiberaktivitäten

Führen Sie Verwaltungs- und Konfigurationsfunktionen von Identity Manager-Treibern mit Designer durch. Diese Funktionen werden im *OpenText™ Identity Manager CE 24.4 (v4.10)-Treiberverwaltungshandbuch* detailliert beschrieben.

VII Aufrüsten von OpenText Identity Manager

In diesem Abschnitt finden Sie Informationen zum Aufrüsten der OpenText Identity Manager-Komponenten. Anweisungen zum Migrieren der vorhandenen Daten auf einen neuen Server finden Sie in Teil VIII, „Migrieren der OpenText Identity Manager-Daten in eine neue Installation“, auf Seite 201. Weitere Informationen zum Unterschied zwischen Aufrüstung und Migration finden Sie in „Erläuterungen zur Aufrüstung und zur Migration“, auf Seite 159.

15 Vorbereiten der Aufrüstung von OpenText Identity Manager

In diesem Abschnitt wird die Vorbereitung Ihrer OpenText Identity Manager-Lösung für die Aufrüstung auf die aktuelle Version beschrieben. Je nach Zielcomputer können Sie den Großteil der OpenText Identity Manager-Komponenten wahlweise mit einer ausführbaren Datei, mit einer Binärdatei oder im Textmodus installieren. Zum Aufrüsten müssen Sie das Installations-Kit für OpenText Identity Manager herunterladen und entpacken.

WARNUNG: Sie müssen sich immer darauf verlassen, dass die Komponenten, die mit OpenText Identity Manager 4.10 installiert werden, über die OpenText Identity Manager Patch Kanäle aktualisiert werden. Andernfalls kann es bei den regelmäßigen OpenText Identity Manager-Patch-Aktualisierungen zu schweren Konflikten kommen.

- „Checkliste für die Aufrüstung von OpenText Identity Manager“, auf Seite 157
- „Erläuterungen zur Aufrüstung und zur Migration“, auf Seite 159
- „Unterstützte Aufrüstungspfade“, auf Seite 160
- „Sichern der aktuellen Konfiguration“, auf Seite 164

Checkliste für die Aufrüstung von OpenText Identity Manager

Wir empfehlen, die Schritte in der nachfolgenden Checkliste für die Aufrüstung auszuführen:

	Checkliste
❑	1. Informieren Sie sich über die Unterschiede zwischen Aufrüstung und Migration. Weitere Informationen finden Sie unter „Erläuterungen zur Aufrüstung und zur Migration“, auf Seite 159.
❑	2. Rüsten Sie auf Identity Manager 4.7.5 auf. Von Versionen vor 4.7.5 können Sie nicht auf Version 4.10 aufrüsten oder migrieren.
❑	3. Stellen Sie sicher, dass das aktuelle Installations-Kit für die Aufrüstung von OpenText Identity Manager vorliegt. Weitere Informationen finden Sie unter Bezugsquellen für OpenText Identity Manager im *Überblick und Planungshandbuch zu OpenText™ Identity Manager CE 24.4 (v4.10)*.
❑	4. Stellen Sie sicher, dass die Computer die Hardware- und Software-Anforderungen für eine höhere Version von OpenText Identity Manager erfüllen.
❑	5. Legen Sie eine Sicherungskopie des aktuellen Treibers, der Treiberkonfiguration und der Datenbanken an. Weitere Informationen finden Sie unter „Sichern der aktuellen Konfiguration“, auf Seite 164.

	Checkliste
❑	6. Installieren Sie die neueste Version von Designer. Weitere Informationen finden Sie unter „Upgrade von Designer“, auf Seite 168.
❑	7. Rüsten Sie OpenText eDirectory auf dem Server, auf dem OpenText Identity Manager ausgeführt wird, auf die aktuelle Version und den aktuellen Patch auf.
❑	8. Halten Sie die Treiber an, die mit dem Server verknüpft sind, auf dem Sie die OpenText Identity Manager-Engine installiert haben. Weitere Informationen finden Sie unter „Anhalten und Starten der OpenText Identity Manager-Treiber“, auf Seite 190.
❑	9. Rüsten Sie die OpenText Identity Manager-Engine auf. Weitere Informationen finden Sie unter „Upgrade der OpenText Identity Manager-Engine“, auf Seite 170. **HINWEIS:** Wenn Sie die OpenText Identity Manager-Engine auf einen neuen Server migrieren, können Sie OpenText eDirectory-Reproduktionen verwenden, die sich auf dem aktuellen OpenText Identity Manager-Server befinden. Weitere Informationen finden Sie unter „Migrieren der OpenText Identity Manager-Engine auf einen neuen Server“, auf Seite 209.
❑	10. (Bedingt) Wenn der Treibersatz für die OpenText Identity Manager-Engine einen Remote Loader-Treiber enthält, rüsten Sie die Remote Loader-Server für jeden Treiber auf. Weitere Informationen finden Sie unter „Aufrüstung von Remote Loader“, auf Seite 172.
❑	11. (Bedingt) Wenn Sie Pakete verwenden, rüsten Sie die Pakete auf die vorhandenen Treiber auf, sodass neue Richtlinien erstellt werden. Weitere Informationen finden Sie unter „Aufrüsten der OpenText Identity Manager-Treiber“, auf Seite 192. Dies ist nur erforderlich, wenn eine neuere Version eines Pakets verfügbar ist und es eine neue Funktion in den Richtlinien für einen Treiber gibt, die Sie zu Ihrem vorhandenen Treiber hinzufügen möchten.
❑	12. (Bedingt) Installieren Sie SSPR, falls nicht bereits installiert. Weitere Informationen finden Sie unter „Installieren von SSPR“, auf Seite 51.
❑	13. Rüsten Sie Identity Applications auf. Weitere Informationen finden Sie unter „Aufrüsten von Identity Applications“, auf Seite 175.
❑	14. Rüsten Sie Identity Reporting auf. Weitere Informationen finden Sie unter „Aufrüsten von Identity Reporting“, auf Seite 184.
❑	15. Starten Sie die Treiber für Identity Applications und die OpenText Identity Manager-Engine. Weitere Informationen finden Sie unter „Anhalten und Starten der OpenText Identity Manager-Treiber“, auf Seite 190.
❑	16. (Bedingt) Wenn Sie die OpenText Identity Manager-Engine oder Identity Applications auf einen neuen Server migriert haben, fügen Sie diesen neuen Server zum Treibersatz hinzu. Weitere Informationen finden Sie unter „Hinzufügen von neuen Servern zum Treibersatz“, auf Seite 194.
❑	17. (Bedingt) Wenn Sie benutzerdefinierte Richtlinien und Regeln verwenden, stellen Sie die benutzerdefinierten Einstellungen wieder her. Weitere Informationen finden Sie unter „Wiederherstellen der benutzerdefinierten Richtlinien und Regeln für den Treiber“, auf Seite 195.
❑	18. Aktivieren Sie die aufgerüstete OpenText Identity Manager-Lösung. Weitere Informationen finden Sie unter „OpenText Identity Manager aktivieren“, auf Seite 119.

Erläuterungen zur Aufrüstung und zur Migration

Wenn Sie eine neuere Version einer vorhandenen OpenText Identity Manager-Installation installieren möchten, nehmen Sie in der Regel eine **Aufrüstung** vor. Wenn die neue Version von OpenText Identity Manager jedoch keinen direkten Aufrüstungspfad von der bestehenden Version unterstützt, müssen Sie zunächst auf eine Version aufrüsten, von der aus eine Aufrüstung auf Version 4.10 möglich ist. Alternativ können Sie eine Migration auf einen neuen Computer durchführen. Wir definieren die **Migration** als Vorgang, bei dem OpenText Identity Manager auf einem neuen Server installiert wird und anschließend die vorhandenen Daten auf diesen neuen Server migriert werden.

Während der Produktevaluierung oder nach Aktivierung der Advanced Edition möchten Sie möglicherweise auf die Standard Edition **umstellen**, wenn Sie die Funktionen der Advanced Edition für Ihre Umgebung nicht benötigen. Mit OpenText Identity Manager können Sie in einigen einfachen Schritten von der Advanced Edition zur Standard Edition wechseln.

Aufrüsten

Im Allgemeinen lassen sich die Identity Manager 4.9 Standard und Advanced Edition problemlos aufrüsten.

- **Identity Manager 4.9 Standard Edition:** Wenn aktuell Identity Manager 4.9 Standard Edition installiert ist, können Sie sie direkt zu OpenText Identity Manager 4.10 Standard Edition aufrüsten. Weitere Informationen finden Sie in der Kurzanleitung für die Installation und Aufrüstung von OpenText™ Identity Manager CE 24.4 (v4.10) Standard Edition.

  Wählen Sie für die Aufrüstung von Identity Manager 4.9 Standard Edition zu OpenText Identity Manager 4.10 Advanced Edition eine der folgenden Methoden:

  - Rüsten Sie von Identity Manager 4.9 Standard Edition auf OpenText Identity Manager 4.10 Standard Edition auf und führen Sie dann die Aufrüstung auf OpenText Identity Manager 4.10 Advanced Edition durch.
  - Rüsten Sie von Identity Manager 4.9 Standard Edition auf Identity Manager 4.9 Advanced Edition auf und führen Sie dann die Aufrüstung auf OpenText Identity Manager 4.10 Advanced Edition durch.
- **Identity Manager 4.9 Advanced Edition:** Wenn aktuell Identity Manager 4.9 Advanced Edition installiert ist, können Sie sie direkt zu OpenText Identity Manager 4.10 Advanced Edition aufrüsten. Weitere Informationen finden Sie unter „Checkliste für die Aufrüstung von OpenText Identity Manager“, auf Seite 157.

Migration

In bestimmten Fällen ist keine direkte Aufrüstung möglich. In diesen Szenarien ist die Migration vorzuziehen. Wenn beispielsweise OpenText Identity Manager auf einem Server installiert ist, auf dem ein mittlerweile nicht mehr unterstütztes Betriebssystem ausgeführt wird, ist eine Migration anstelle einer Aufrüstung erforderlich

Wenn Sie mehrere Server mit einem Treibersatz verknüpft haben, können Sie eine Aufrüstung oder eine Migration nur auf einem Server gleichzeitig durchführen. Wenn Sie nicht genügend Zeit haben, um die Server zum gleichen Zeitpunkt aufzurüsten, arbeiten die Treiber weiterhin mit den verschiedenen Versionen von OpenText Identity Manager, bis die Upgrades für jeden Server abgeschlossen werden können.

WICHTIG: Wenn Sie Funktionen für Treiber aktivieren, die nur unter OpenText Identity Manager 4.10 oder höher unterstützt werden, arbeiten die Treiber nicht mehr auf den Servern mit gemischten Versionen. Die älteren Engines können die neue Funktionalität nicht verarbeiten. Dies deaktiviert die Treiber, bis alle Server auf OpenText Identity Manager 4.10 oder höher aufgerüstet wurden.

Wechseln von der Advanced Edition zur Standard Edition

In OpenText Identity Manager können Sie während des Produkttestzeitraums oder nach dem Aktivieren der Advanced Edition von der Advanced Edition zur Standard Edition wechseln.

WICHTIG: Sollten Sie die Advanced Edition bereits aktiviert haben, müssen Sie nicht auf die Standard Edition umstellen, da die Advanced Edition alle Funktionen der Standard Edition enthält. Sie müssen nur dann auf die Standard Edition umstellen, wenn Sie keinerlei Funktionen der Advanced Edition für Ihre Umgebung wünschen und die Bereitstellung von OpenText Identity Manager einschränken möchten. Weitere Informationen finden Sie unter Kapitel 17, „Wechseln von der Advanced Edition zur Standard Edition“, auf Seite 199.

Unterstützte Aufrüstungspfade

Von Identity Manager 4.7.x und 4.8.x kann auf 4.9 aufgerüstet werden. OpenText empfiehlt, vor dem Starten der Aufrüstung die Informationen in den Versionshinweisen zu Ihrer aktuellen Version zu lesen.

- „Aufrüsten von Identity Manager 4.7.5.“, auf Seite 160
- „Aufrüsten von Identity Manager 4.8.x“, auf Seite 162

Aufrüsten von Identity Manager 4.7.5.

Wenn Sie Identity Manager 4.7.5 http installiert hatten, müssen Sie auf Identity Manager 4.7.5 https aktualisieren. Vergewissern Sie sich, dass `tomcat.ks` und `idm.jks` verfügbar sind. Wie Sie sie erstellen, erfahren Sie im Abschnitt Verwendung von SSL für die sichere Kommunikation in OpenText™ Identity Manager CE 24.4 (v4.10) – Administratorhandbuch zu Identity Applications.

Die nachfolgende Tabelle zeigt die komponentenweisen Upgrade-Pfade für Identity Manager 4.7.5.

Komponente	Basisversion	Aufgerüstete Version
OpenText Identity Manager-Engine	4.7.5	1. Rüsten Sie das Betriebssystem auf eine unterstützte Version auf. 2. Rüsten Sie das Identitätsdepot auf Version 9.3 auf 3. Rüsten Sie die OpenText Identity Manager-Engine auf Version 4.10 auf
Remote Loader/Fan-out-Agent	4.7.5	Installieren Sie den Remote Loader/Fan-out-Agent 4.10.
Designer		Installieren Sie Designer 4.10

Komponente	Basisversion	Aufgerüstete Version
Analyzer		Installieren Sie Analyzer 4.8.5
Identity Applications	4.7.5	Bevor Sie Identity Applications aufrüsten, müssen das Identitätsdepot auf Version 9.3 und die OpenText Identity Manager-Engine auf Version 4.10 aufgerüstet werden. 1. Rüsten Sie das Betriebssystem auf eine unterstützte Version auf. 2. Rüsten Sie das Betriebssystem auf eine unterstützte Version auf. Informationen zu den unterstützten Datenbankversionen finden Sie auf der Website für technische Informationen zu OpenText Identity Manager (https://www.microfocus.com/en-us/products/netiq-identity-manager/specs). 3. (Bedingt) Wenn SSPR auf einem separaten Server installiert ist, rüsten Sie die Komponente auf Version 4.10 auf. 4. Aktualisieren Sie die Benutzeranwendungstreiber- sowie die Rollen- und Ressourcentreiberpakete. 5. Rüsten Sie Identity Applications auf Version 4.10 auf. 6. Halten Sie Tomcat an. **HINWEIS:** Nach dem Aufrüsten werden die alten JRE-Dateien nicht in das Sicherungsverzeichnis verschoben, sondern bleiben an diesem Speicherort: `C:\NetIQ\idm\apps\jre`

Komponente	Basisversion	Aufgerüstete Version
Identity Reporting	4.7.5	1. Rüsten Sie das Betriebssystem auf eine unterstützte Version auf. 2. Rüsten Sie das Betriebssystem auf eine unterstützte Version auf. Weitere Informationen zu den unterstützten Datenbankversionen finden Sie in den Systemanforderungen für OpenText™ Identity Manager CE 24.4 (v4.10). 3. Rüsten Sie SLM für IGA auf eine unterstützte Version auf. 4. Aufrüsten von Identity Reporting zu 7.4.0 5. (Bedingt) Erstellen Sie eine Datensynchronisierungsrichtlinie auf der Seite des OpenText Identity Manager-Datenerfassungsdiensts.

Wir empfehlen, vor dem Starten der Aufrüstung die Informationen in den Versionshinweisen zu Ihrer Version zu lesen. Sie befinden sich auf der Seite der OpenText Identity Manager-Dokumentation (https://www.netiq.com/documentation/identity-manager-4.10/).

HINWEIS: Vergewissern Sie sich nach dem Aufrüsten, dass `tomcat.ks` und `idm.jks` verfügbar sind. Wie Sie sie erstellen, erfahren Sie im Abschnitt Verwendung von SSL für die sichere Kommunikation in OpenText™ Identity Manager CE 24.4 (v4.10) – Administratorhandbuch zu Identity Applications.

Aufrüsten von Identity Manager 4.8.x

Die nachfolgende Tabelle zeigt die komponentenweisen Aufrüstungspfade für Identity Manager 4.8.x:

Komponente	Basisversion	Aufgerüstete Version
OpenText Identity Manager-Engine	4.8.x	1. Rüsten Sie das Betriebssystem auf eine unterstützte Version auf. 2. Rüsten Sie das Identitätsdepot auf Version 9.3 auf 3. Rüsten Sie die OpenText Identity Manager-Engine auf Version 4.10 auf
Remote Loader/Fan-out-Agent	4.8.x	Installieren Sie den Remote Loader/Fan-out-Agent 4.10.
Designer		Installieren Sie Designer 4.10
Analyzer		Installieren Sie Analyzer 4.8.5.

Komponente	Basisversion	Aufgerüstete Version
Identity Applications	4.8.x	Bevor Sie Identity Applications aufrüsten, müssen das Identitätsdepot auf Version 9.3 und die OpenText Identity Manager-Engine auf Version 4.10 aufgerüstet werden. 1. Rüsten Sie das Betriebssystem auf eine unterstützte Version auf. 2. Rüsten Sie das Betriebssystem auf eine unterstützte Version auf. Informationen zu den unterstützten Datenbankversionen finden Sie auf der Website für technische Informationen zu OpenText Identity Manager (https://www.netiq.com/products/identity-manager/advanced/technical-information/). 3. (Bedingt) Wenn SSPR auf einem separaten Server installiert ist, rüsten Sie die Komponente auf Version 4.10 auf. 4. Aktualisieren Sie die Benutzeranwendungstreiber- sowie die Rollen- und Ressourcentreiberpakete. 5. Rüsten Sie Identity Applications auf Version 4.10 auf 6. Halten Sie Tomcat an.

Komponente	Basisversion	Aufgerüstete Version
Identity Reporting	4.8.x	1. Rüsten Sie das Betriebssystem auf eine unterstützte Version auf. 2. Rüsten Sie das Betriebssystem auf eine unterstützte Version auf. Weitere Informationen zu den unterstützten Datenbankversionen finden Sie in den Systemanforderungen für OpenText™ Identity Manager CE 24.4 (v4.10). 3. Rüsten Sie SLM für IGA auf eine unterstützte Version auf (die Installation wird nur auf Linux-Rechnern unterstützt). 4. Rüsten Sie das Data Collection Services-Treiberpaket und das Treiberpaket „Verwaltetes System – Gateway“ auf. 5. Rüsten Sie Identity Reporting 7.4.0 auf 6. (Bedingt) Erstellen Sie eine Datensynchronisierungsrichtlinie auf der Seite des OpenText Identity Manager-Datenerfassungsdiensts.

Wir empfehlen, vor dem Starten der Aufrüstung die Informationen in den Versionshinweisen zu Ihrer Version zu lesen. Sie befinden sich auf der Seite der OpenText Identity Manager-Dokumentation (https://www.netiq.com/documentation/identity-manager-4.10/).

Sichern der aktuellen Konfiguration

Wir empfehlen, vor dem Aufrüsten die aktuelle Konfiguration Ihrer OpenText Identity Manager-Lösung zu sichern. Für das Sichern der Benutzeranwendung sind keine weiteren Schritte erforderlich. Die gesamte Konfiguration der Benutzeranwendung wird im Benutzeranwendungstreiber gespeichert. Sie können die Sicherung wie folgt anlegen:

- „Exportieren des Designer-Projekts“, auf Seite 164
- „Exportieren der Treiberkonfiguration“, auf Seite 166

Exportieren des Designer-Projekts

Ein Designer-Projekt enthält das Schema und alle Treiberkonfigurationsinformationen. Wenn Sie ein Projekt Ihrer OpenText Identity Manager-Lösung erstellen, können Sie alle Treiber in einem Schritt exportieren, statt einzelne Exportdateien für jeden Treiber erstellen zu müssen.

- „Exportieren des aktuellen Projekts“, auf Seite 165
- „Erstellen eines neuen Projekts aus dem Identitätsdepot“, auf Seite 165

Exportieren des aktuellen Projekts

Wenn Sie bereits ein Designer-Projekt haben, vergewissern Sie sich, dass die Informationen in diesem Projekt mit denen im Identitätsdepot synchron sind:

1. Öffnen Sie Ihr Projekt in Designer.
2. Klicken Sie im Modellierer mit der rechten Maustaste auf das Identitätsdepot und wählen Sie anschließend **Live > Vergleichen**.
3. Werten Sie das Projekt aus, gleichen Sie mögliche Unterschiede ab und klicken Sie anschließend auf **OK**.

   Weitere Informationen finden Sie unter „Verwenden der Vergleichsfunktion beim Bereitstellen“ im *Administrationshandbuch zu Designer für OpenText™ Identity Manager CE 24.4 (v4.10)*.
4. Wählen Sie in der Symbolleiste **Projekt > Exportieren**.
5. Klicken Sie auf **Alle markieren**, um alle zu exportierenden Ressourcen auszuwählen.
6. Wählen Sie, wo und in welchem Format das Projekt gespeichert werden soll, und klicken Sie anschließend auf **Fertig stellen**.

   Speichern Sie das Projekt an einem beliebigen Speicherort außer im aktuellen Arbeitsbereich. Wenn Sie auf Designer aufrüsten, müssen Sie einen neuen Speicherort für den Arbeitsbereich erstellen. Weitere Informationen finden Sie unter „Exportieren von Projekten“ im *Administrationshandbuch zu Designer für OpenText™ Identity Manager CE 24.4 (v4.10)*.

Erstellen eines neuen Projekts aus dem Identitätsdepot

Wenn Ihnen kein Designer-Projekt Ihrer aktuellen OpenText Identity Manager-Lösung vorliegt, müssen Sie ein Projekt zur Sicherung Ihrer aktuellen Lösung erstellen.

1. Installieren Sie Designer.
2. Starten Sie Designer und geben Sie einen Speicherort für Ihren Arbeitsbereich an.
3. Wählen Sie aus, ob Sie auf Online-Updates prüfen möchten, und klicken Sie anschließend auf **OK**.
4. Klicken Sie in der Begrüßungsseite auf **Designer ausführen**.
5. Wählen Sie in der Symbolleiste **Projekt > Projekt importieren > Identitätsdepot**.
6. Geben Sie einen Namen für das Projekt an und verwenden Sie anschließend entweder den Standardspeicherort für Ihr Projekt oder wählen Sie einen anderen Speicherort aus.
7. Klicken Sie auf **Weiter**.
8. Stellen Sie mit den folgenden Werten eine Verbindung zum Identitätsdepot her:
   - **Hostname:** IP-Adresse oder DNS-Name des Identitätsdepot-Servers
   - **Benutzername:** DN des Benutzers, mit dem die Authentifizierung beim Identitätsdepot erfolgt
   - **Passwort:** Passwort des Authentifizierungsbenutzers
9. Klicken Sie auf **Weiter**.
10. Lassen Sie die Optionen „Identitätsdepot - Schema“ und „Standard-Benachrichtigungssammlung“ ausgewählt.

11 Erweitern Sie die Standard-Benachrichtigungssammlung, und heben Sie die Auswahl der nicht benötigten Sprachen auf.

   Die Standard-Benachrichtigungssammlungen sind in viele unterschiedliche Sprachen übersetzt. Sie können alle Sprachen importieren oder nur die Sprachen auswählen, die Sie verwenden.

12 Klicken Sie auf **Durchsuchen**, suchen Sie das Verzeichnis und wählen Sie einen Treibersatz aus, den Sie importieren möchten.

13 Wiederholen Sie Schritt 12 für jeden Treibersatz in diesem Identitätsdepot und klicken Sie anschließend auf **Fertig stellen**.

14 Klicken Sie auf **OK**, nachdem das Projekt importiert wurde.

15 Wenn Sie nur ein Identitätsdepot haben, sind Sie fertig. Wenn Sie mehrere Identitätsdepots haben, fahren Sie mit Schritt 16 fort.

16 Klicken Sie in der Symbolleiste auf **Live > Importieren**.

17 Wiederholen Sie Schritt 8 bis Schritt 14 für jedes weitere Identitätsdepot.

Exportieren der Treiberkonfiguration

Beim Exportieren der Treiberdaten wird ein Backup Ihrer aktuellen Konfiguration erstellt. Designer unterstützt jedoch momentan nicht die Erstellung von Backups der Treiber und Richtlinien der rollenbasierten Berechtigungen.

Exportieren der Treiberkonfigurationen mit Designer

1 Stellen Sie sicher, dass Ihr Projekt in Designer über die aktuellste Treiberversion verfügt. Weitere Informationen finden Sie unter „Importieren einer Bibliothek, eines Treibersatzes oder eines Treibers vom Identitätsdepot“ im *Administrationshandbuch zu Designer OpenText™ Identity Manager CE 24.4 (v4.10)*.

2 Klicken Sie im Modellierer mit der rechten Maustaste auf die Linie des aufzurüstenden Treibers.

3 Wählen Sie **In Konfigurationsdatei exportieren**.

4 Wählen Sie den Speicherort für die Konfigurationsdatei und klicken Sie anschließend auf **Speichern**.

5 Klicken Sie auf der Ergebnisseite auf **OK**.

6 Führen Sie Schritt 1 bis Schritt 5 für alle Treiber aus.

16 Aufrüsten der OpenText Identity Manager-Komponenten

In diesem Abschnitt finden Sie Informationen zum Aufrüsten einzelner Komponenten in OpenText Identity Manager. Dieser Abschnitt enthält außerdem einige Schritte, die unter Umständen nach einer Aufrüstung anfallen.

- „Überlegungen für das Upgrade“, auf Seite 167
- „Upgrade-Reihenfolge“, auf Seite 168
- „Upgrade von Designer“, auf Seite 168
- „Aufrüsten der OpenText Identity Manager-Engine-Komponenten“, auf Seite 169
- „Aufrüsten von Identity Applications“, auf Seite 175
- „Aufrüsten von Identity Reporting“, auf Seite 184
- „Aufrüsten von Analyzer“, auf Seite 188
- „Arbeitsschritte nach der Aktualisierung“, auf Seite 188
- „Aufgaben nach dem Upgrade im FIPS-aktivierten Modus“, auf Seite 189
- „Anhalten und Starten der OpenText Identity Manager-Treiber“, auf Seite 190
- „Aufrüsten der OpenText Identity Manager-Treiber“, auf Seite 192
- „Hinzufügen von neuen Servern zum Treibersatz“, auf Seite 194
- „Wiederherstellen der benutzerdefinierten Richtlinien und Regeln für den Treiber“, auf Seite 195

Überlegungen für das Upgrade

- Ab Identity Manager 4.9 wird SecretStore nicht mehr unterstützt. Nachdem Sie ein Upgrade auf das neueste UAD-Paket durchgeführt und Tomcat neu gestartet haben, werden alle bestehenden Passwörter im SecretStore Repository automatisch in das Attribut `notfSMTPMailPassword` migriert. Die Migration von Passwörtern wird über die Eigenschaft `com.netiq.idm.migrate.secretstore` gesteuert, die in der Datei `ism-configuration.properties` verfügbar ist. Standardmäßig ist diese Eigenschaft auf `true` festgelegt. Nach der Migration wird die Eigenschaft automatisch wieder auf „false“ festgelegt und bleibt in diesem Zustand.
- Beim Upgrade von 4.9 auf 4.10 wird der Benutzer nicht zur Eingabe des Master-Keystore-Passworts aufgefordert. Es wird das zuvor gespeicherte Passwort aus der `ism-sensitive.properties`-Datei verwendet. Beim Upgrade von 4.7.5 und 4.8.x auf 4.10 wird der Benutzer jedoch nicht zur Eingabe des Master-Keystore-Passworts (encrypt-keys.pkcs12)

aufgefordert. Führen Sie die unter Storing Configupdate Ultity Password (Speichern des Passworts für das Configupdate-Dienstprogramm) beschriebenen Schritte aus, um das Passwort zu ändern oder erneut zu verschlüsseln.

- Wenn Sie Identity Applications-Komponente von Identity Manager 4.7.5 auf 4.10 aufrüsten, exportieren Sie die Daten mit dem Workflow-Migrationswerkzeug aus der Identity Applications-Datenbank (`idmuserappdb`) in die Workflow-Engine-Datenbank (`igaworkflowdb`). Weitere Informationen finden Sie unter *Migrating Data from Identity Applications Database into Workflow Engine Database* (Migrieren von Daten aus der Identity Applications-Datenbank in die Workflow-Engine-Datenbank) in OpenText™ Identity Manager CE 24.4 (v4.10) – Administratorhandbuch zu Identity Applications.

Upgrade-Reihenfolge

Sie müssen die Komponenten des OpenText Identity Manager in folgender Reihenfolge aufrüsten:

1. Designer
2. Sentinel Log Management für IGA (kann nur auf Linux-Rechnern installiert werden)
3. Identitätsdepot
4. OpenText Identity Manager-Engine
5. Remote Loader
6. Fan-out-Agent
7. Identity Applications (Advanced Edition)
8. Identity Reporting
9. Analyzer
10. Zurücksetzen von Passwörtern per Selbstbedienung

Upgrade von Designer

HINWEIS: Diese Version unterstützt kein Upgrade von Designer von einer früheren Version. Wenn Sie also eine ältere Version installiert haben, müssen Sie diese vor der Installation von Designer 4.10 deinstallieren. Außerdem können die integrierten Funktionen für automatische Updates und Offline-Updates nicht für ein Upgrade auf Designer 4.10 verwendet werden.

1. Melden Sie sich als Administrator an dem Server an, auf dem Designer installiert ist.
2. Legen Sie eine Sicherungskopie Ihrer Projekte an. Exportieren Sie hierzu die Projekte.

   Weitere Informationen zum Exportieren finden Sie unter „Exportieren von Projekten“ im *Administrationshandbuch zu Designer für OpenText™ Identity Manager CE 24.4 (v4.10)*.
3. Zur Deinstallation schließen Sie zunächst Designer. Anschließend deinstallieren Sie Designer je nach Betriebssystem:

   Öffnen Sie die Option „Software“ in der Systemsteuerung. Unter Windows Server 2008 klicken Sie beispielsweise auf **Programme und Funktionen**. Klicken Sie mit der rechten Maustaste auf **Designer für OpenText Identity Manager**, und klicken Sie auf **Deinstallieren**.

4 Starten Sie das Installationsprogramm für Designer von der Datei `Identity_Manager_4.10_Designer_Windows.zip`. (`<Speicherort der extrahierten ZIP-Datei für Designer>\designer_install\install.exe`)

5 Befolgen Sie die Anweisungen im Assistenten, bis die Installation abgeschlossen ist.

6 Nach der Installation von Designer 4.10 müssen Sie alle Designer-Projekte aus der älteren Version importieren. Zu Beginn des Importvorgangs führt Designer den Projektkonvertierer-Assistenten aus, mit dem die älteren Projekte in die aktuelle Version konvertiert werden. Wählen Sie im Assistenten die Option **Projekt in den Arbeitsbereich kopieren**. Weitere Informationen zum Projektkonvertierer finden Sie unter Konvertieren früherer Projekte im *Administrationshandbuch zu Designer für OpenText™ Identity Manager CE 24.4 (v4.10)*.

Aufrüsten der OpenText Identity Manager-Engine-Komponenten

Vor dem Aufrüsten der OpenText Identity Manager-Engine muss das Identitätsdepot aufgerüstet werden. Im Rahmen des Aufrüstungsvorgangs für die OpenText Identity Manager-Engine werden die Dateien des Treiberschnittstellenmoduls aktualisiert, die im Dateisystem des Hostcomputers gespeichert sind.

Upgrade des Identitätsdepots

1 Laden Sie die `Identity_Manager_4.10.0_Windows.iso` entsprechend der Anweisungen in Bezugsquellen für OpenText Identity Manager im *Überblick und Planungshandbuch zu OpenText™ Identity Manager CE 24.4 (v4.10)* herunter.

2 Hängen Sie die heruntergeladene `.iso`-Datei ein.

3 Navigieren Sie zum Verzeichnis `<Speicherort der eingehängten ISO-Datei>\IdentityManagerServer\products\eDirectory\x64`.

4 Führen Sie die Datei `eDirectory_930_Windows_x86_x64.exe` aus.

5 Geben Sie auf der Registerkarte **Basis** die folgenden Details an:

- Geben Sie die folgenden Details an, wenn Sie **Neuer Baum** auswählen:
  - **Baumname:** Geben Sie einen Baumnamen für das Identitätsdepot an.
  - **Server-FDN:** Geben Sie einen Server-FDN an.

    HINWEIS: Auch wenn das Identitätsdepot zulässt, dass der vollständige eindeutige Name (FDN) des NCP-Serverobjekts bis zu 256 Zeichen lang sein kann, empfehlen wir, die Variable auf einen viel niedrigeren Wert zu beschränken, da vom Identitätsdepot andere längere Objekte erstellt werden, die auf der Länge dieses Objekts basieren.
  - **Baum-Admin:** Geben Sie einen Administratornamen für das Identitätsdepot an.
  - **Admin-Passwort:** Geben Sie das Administrator-Passwort an.
- Geben Sie die folgenden Details an, wenn Sie **Vorhandener Baum** auswählen:
  - **IP-Adresse:** Geben Sie die IP-Adresse des vorhandenen Baums für das Identitätsdepot an.
  - **Port-Nummer:** Geben Sie die Port-Nummer für den vorhandenen Baum an. Der Standardwert ist 524.

- **Server-FDN:** Geben Sie einen Server-FDN an.
- **Baum-Admin:** Geben Sie den vorhandenen Administratornamen für das Identitätsdepot an.
- **Admin-Passwort:** Geben Sie das Administrator-Passwort an.

6 (Bedingt) Geben Sie auf der Registerkarte **Erweitert** die folgenden Details an:

- Damit IPv6-Adressen auf dem Identitätsdepotserver verwendet werden, wählen Sie **IPv6 aktivieren** aus.

  HINWEIS: Wir empfehlen, diese Option zu aktivieren. Wenn die IPv6-Adressen nach erfolgter Installation aktiviert werden sollen, müssen Sie das Setup-Programm erneut ausführen.

- Zum Aktivieren von Enhanced Background Authentication (EBA) wählen Sie **EBA aktivieren** aus.
- Geben Sie den Klartext und die sicheren Ports für HTTP an. Die Standardwerte lauten 8028 bzw. 8030.
- Geben Sie den Klartext und die sicheren Ports für LDAP an. Die Standardwerte lauten 389 bzw. 636.

7 Geben Sie im Feld **Installationsordner** den Speicherort an, an dem das Identitätsdepot installiert ist.

8 Geben Sie im Feld **DIB-Verzeichnis** den Speicherort an, an dem sich die DIB-Dateien befinden.

9 Klicken Sie auf **Aufrüsten** und fahren Sie mit dem Aufrüstungsvorgang fort.

Upgrade der OpenText Identity Manager-Engine

Stellen Sie sicher, dass alle Treiber angehalten wurden. Weitere Informationen finden Sie unter „Anhalten der Treiber“, auf Seite 190.

Führen Sie das Upgrade der OpenText Identity Manager-Engine wie folgt aus:

1 Laden Sie die Datei `Identity_Manager_4.10.0_Windows.iso` von der OpenText-Downloads-Website herunter.

2 Stellen Sie die heruntergeladene `.iso`-Datei bereit.

3 Navigieren Sie zum Ordner `<Speicherort der installierten ISO-Datei>\IdentityManagerServer` und führen Sie die Datei `install.exe` aus.

4 Wählen Sie die Sprache für die Installation aus und klicken Sie auf **OK**.

5 Klicken Sie auf der Einführungsseite auf **Weiter**.

6 Lesen und akzeptieren Sie die Lizenzvereinbarung und klicken Sie dann auf **Weiter**.

Die installierten Komponenten und deren Versionen werden angezeigt.

7 Wählen Sie **OpenText Identity Manager-Engine** aus und klicken Sie auf **Weiter**.

8 Geben Sie die folgenden Informationen ein:

Identitätsdepot-Administrator: Geben Sie den Namen des Identitätsdepot-Administrators an.

Identitätsdepot-Administratorpasswort: Geben Sie das Passwort des Identitätsdepot-Administrators an.

9 Wählen Sie aus der folgenden Liste die Edition des OpenText Identity Managers aus, die Sie installieren möchten:

- Standard Edition
- Advanced Edition

HINWEIS: Wählen Sie unbedingt die gleiche Edition wie in der vorherigen Version.

---

10 Geben Sie die Konfigurationseinstellungen für die OpenText Identity Manager-Engine an. Weitere Informationen finden Sie unter „Arbeitsblatt für die Konfiguration der OpenText Identity Manager-Engine“, auf Seite 52.

11 Lesen Sie auf der Seite der Zusammenfassung vor der Aufrüstung die Einstellungen und klicken Sie auf **Aufrüsten**.

Arbeiten mit MapDB 3.0.9

Zusätzlich zur OpenText Identity Manager-Engine wird MapDB von folgenden OpenText Identity Manager-Treibern verwendet:

- Datenerfassungsdienste
- JDBC
- LDAP
- Verwaltetes System – Gateway
- Office 365 und Azure Active Directory
- Salesforce

Wenn Sie einige dieser Treiber verwenden, müssen Sie vor dem Upgrade der Treiber folgende Abschnitte lesen:

- „Erläuterungen zur Unterstützung der Treiberversionen durch die OpenText Identity Manager 4.10-Engine“, auf Seite 171
- „Manuelles Entfernen der MapDB-Cache-Dateien“, auf Seite 172

Erläuterungen zur Unterstützung der Treiberversionen durch die OpenText Identity Manager 4.10-Engine

Lesen Sie die folgenden Überlegungen, bevor Sie einen OpenText Identity Manager-Treiber aufrüsten, der MapDB verwendet:

- Die im Lieferumfang von OpenText Identity Manager 4.10 enthaltenen Treiber sind kompatibel mit der Engine oder dem Remote Loader von OpenText Identity Manager 4.10. Sie müssen die Schritte für das Upgrade der Treiber ausführen, die im jeweiligen Implementierungshandbuch der Treiber genannt sind.
- Die im Lieferumfang einer Version älter als OpenText Identity Manager 4.10 enthaltenen Treiber sind nicht kompatibel mit der Engine oder dem Remote Loader von OpenText Identity Manager 4.10.

- Die im Lieferumfang von Identity Manager 4.10 enthaltenen Treiber sind nicht rückwärts kompatibel mit der Engine oder dem Remote Loader von OpenText Identity Manager 4.8.x.
- Die im Lieferumfang von Identity Manager 4.10 enthaltenen Treiber sind nicht rückwärts kompatibel mit der Engine oder dem Remote Loader von OpenText Identity Manager 4.7.x.

Manuelles Entfernen der MapDB-Cache-Dateien

Bei der Aufrüstung der OpenText Identity Manager-Engine verbleiben einige der bestehenden MapDB-Cache-Dateien (dx*) im DIB-Verzeichnis des Identitätsdepots. Nach dem Upgrade des Treibers müssen Sie die vorhandenen MapDB-Cache-Dateien für den Treiber manuell entfernen. Durch diese Aktion wird sichergestellt, dass Ihr Treiber mit der OpenText Identity Manager 4.10-Engine korrekt funktioniert.

In der folgenden Tabelle sind die MapDB-Cache-Dateien aufgelistet, die entfernt werden müssen:

OpenText Identity Manager-Treiber	Zu entfernende MapDB-Status-Cache-Datei
Datenerfassungsdienste	DCSDriver_<Treiberinstanz-GUID>-* <Treiberinstanz-GUID>-*
JDBC	jdbc_<Treiberinstanz-GUID>_*
LDAP	ldap_<Treiberinstanz-GUID>*
Verwaltetes System – Gateway	MSGW-<Treiberinstanz-GUID>.*
Office 365 und Azure Active Directory	<Name des Azure-Treibers>_obj.db.*
Salesforce	<Name des Salesforce-Treibers>.* <Name des Salesforce-Treibers>

wobei ***** den Namen der MapDB-Status-Cache-Datei bezeichnet. Im Fall eines Salesforce-Treibers sind die MapDB-Status-Cache-Dateien ebenfalls im Treibernamen angegeben. Nachfolgend sehen Sie einige Beispiele zu diesen Dateien.

- DCSDriver_<Treiberinstanz-GUID>-0.t, <Treiberinstanz-GUID>-1.p
- jdbc_<Treiberinstanz-GUID>_0.t, jdbc_<Treiberinstanz-GUID>_1
- ldap_<Treiberinstanz-GUID>b, ldap_<Treiberinstanz-GUID>b.p
- MSGW-<Treiberinstanz-GUID>.p, MSGW-<Treiberinstanz-GUID>.t
- <Name des Azure-Treibers>_obj.db.t, <Name des Azure-Treibers>_obj.db.p
- <Name des Salesforce-Treibers>.p, <Name des Salesforce-Treibers>.t, Salesforce driver1

Aufrüstung von Remote Loader

Wenn Sie den Remote Loader ausführen, müssen die Remote Loader-Dateien aufgerüstet werden.

HINWEIS: Stellen Sie vor der Aufrüstung von *.NET* Remote Loader sicher, dass zuvor alle Windows-Updates erfolgreich im System installiert wurden.

1. Erstellen Sie eine Sicherung der Remote Loader-Konfigurationsdateien. Standardmäßig wird die Datei unter dem Pfad `C:\...\RemoteLoader\Name_des_Remote_Loader-config.txt` abgelegt.
2. Stellen Sie sicher, dass alle Treiber angehalten wurden. Anweisungen hierzu finden Sie unter Stoppen, Starten oder Neustarten eines Treibers in Designer im *Verwaltungshandbuch für OpenText™ Identity Manager CE 24.4 (v4.10)-Treiber*.
3. Halten Sie den Remote Loader-Service bzw. den Daemon für jeden Treiber an.

   Wählen Sie in der Remote Loader-Konsole die Remote Loader-Instanz aus, und klicken Sie anschließend auf **Anhalten**.
4. Stoppen Sie den `cache`-Vorgang mit dem Windows-Task-Manager.
5. Laden Sie die Datei `Identity_Manager_4.10.0_Windows.iso` von der OpenText-Downloads-Website herunter.
6. Stellen Sie die heruntergeladene `.iso`-Datei bereit.
7. Navigieren Sie zum Ordner `<Speicherort der installierten ISO-Datei>\IdentityManagerServer` und führen Sie die Datei `install.exe` aus.
8. Wählen Sie die Sprache für die Installation aus und klicken Sie auf **OK**.
9. Klicken Sie auf der Einführungsseite auf **Weiter**.
10. Lesen und akzeptieren Sie die Lizenzvereinbarung und klicken Sie dann auf **Weiter**.

    Die installierten Komponenten und deren Versionen werden angezeigt.
11. Wählen Sie **Remote Loader-Service** aus und klicken Sie auf **Weiter**.
12. Klicken Sie auf der Seite mit der Zusammenfassung vor der Aufrüstung auf **Aufrüsten**.
13. Überprüfen Sie nach der Aktualisierung, ob Ihre Konfigurationsdateien die Informationen Ihrer Umgebung enthalten.
14. (Bedingt) Falls ein Problem mit der Konfigurationsdatei auftritt, kopieren Sie die Sicherungsdatei, die Sie in Schritt 1 erstellt haben. Fahren Sie andernfalls mit dem nächsten Schritt fort.
15. Starten Sie den Remote Loader-Service bzw. den Daemon für jeden Treiber.

WICHTIG: Wenn Ihr Treiber MapDB verwendet, müssen Sie die bestehenden MapDB-Status-Cache-Dateien für den Treiber nach der Aufrüstung des Treibers manuell entfernen. Dies ist erforderlich, weil beim Upgrade der OpenText Identity Manager-Engine nicht alle dieser Dateien aus dem DIB-Verzeichnis des Identitätsdepots entfernt werden. Weitere Informationen finden Sie unter „Arbeiten mit MapDB 3.0.9“, auf Seite 171.

Aufrüstung des Java Remote Loader

1. Erstellen Sie eine Sicherung der Remote Loader-Konfigurationsdateien. Standardmäßig wird die Datei unter dem Pfad `C:\...\RemoteLoader\Name_des_Remote_Loader-config.txt` abgelegt.
2. Stellen Sie sicher, dass alle Treiber angehalten wurden. Anweisungen hierzu finden Sie unter Stoppen, Starten oder Neustarten eines Treibers in Designer im *Verwaltungshandbuch für OpenText™ Identity Manager CE 24.4 (v4.10)-Treiber*.
3. Halten Sie den Remote Loader-Service bzw. den Daemon für jeden Treiber an.

   Wählen Sie in der Remote Loader-Konsole die Remote Loader-Instanz aus, und klicken Sie anschließend auf **Anhalten**.
4. Stoppen Sie den `lcache`-Vorgang mit dem Windows-Task-Manager.
5. Laden Sie die Datei `Identity_Manager_4.10.0_Windows.iso` von der OpenText-Downloads-Website herunter.
6. Stellen Sie die heruntergeladene `.iso`-Datei bereit.
7. Navigieren Sie zum Ordner `<Speicherort der installierten ISO-Datei>\IdentityManagerServer\products\IDM\java_remoteloader`.
8. Kopieren und ersetzen Sie die Datei `dirxml_jremote_dev.tar.gz` im bestehenden Verzeichnis, in dem Remote Loader installiert ist.
9. Entsprechend der in der bestehenden Einrichtung vorhandenen Datei müssen Sie eine der folgenden Dateien im bestehenden Verzeichnis, in dem Java Remote Loader installiert ist, kopieren und ersetzen:
   - `dirxml_jremote.tar.gz`
   - `dirxml_jremote_mvs.tar`
10. Extrahieren Sie die Dateien, die Sie in Schritt 8 und 9 kopiert haben.

    Dekomprimieren Sie die `.tar.gz`-Datei mit Z-zip oder einer unterstützten Software.
11. (Bedingt) Falls ein Problem mit der Konfigurationsdatei auftritt, kopieren Sie die Sicherungsdatei, die Sie in Schritt 1 erstellt haben. Fahren Sie andernfalls mit dem nächsten Schritt fort.

    HINWEIS: Vergewissern Sie sich anhand der Datei `version.txt`, dass Sie die neueste Version von Java Remote Loader installiert haben.

    ---
12. Starten Sie den Remote Loader-Service bzw. den Daemon für jeden Treiber.

Aufrüsten des Fan-out-Agent

Stellen Sie sicher, dass alle Treiber angehalten wurden. Weitere Informationen finden Sie unter „Anhalten der Treiber“, auf Seite 190.

Führen Sie das Upgrade der OpenText Identity Manager-Engine wie folgt aus:

1. Laden Sie die Datei `Identity_Manager_4.10.0_Windows.iso` von der OpenText-Downloads-Website herunter.
2. Stellen Sie die heruntergeladene `.iso`-Datei bereit.
3. Navigieren Sie zum Ordner `<Speicherort der installierten ISO-Datei>\IdentityManagerServer` und führen Sie die Datei `install.exe` aus.
4. Wählen Sie die Sprache für die Installation aus und klicken Sie auf **OK**.
5. Klicken Sie auf der Einführungsseite auf **Weiter**.
6. Lesen und akzeptieren Sie die Lizenzvereinbarung und klicken Sie dann auf **Weiter**.

   Die installierten Komponenten und deren Versionen werden angezeigt.
7. Wählen Sie **Fan-out-Agent** aus und klicken Sie auf **Weiter**.
8. Lesen Sie auf der Seite der Zusammenfassung vor der Aufrüstung die Einstellungen und klicken Sie auf **Aufrüsten**.
9. Starten Sie den Fan-out-Agent-Service.

Aufrüsten von Identity Applications

In diesem Abschnitt finden Sie Informationen zur Aufrüstung der Identity Applications und unterstützenden Software, wozu die Aktualisierung der folgenden Komponenten gehört:

- OpenText Identity Manager-Benutzeranwendung
- One SSO Provider (OSP)
- Self-Service Password Reset (SSPR)
- Tomcat, JDK und ActiveMQ

Nach der Aufrüstung sind folgende Komponentenversionen installiert:

- Tomcat – `9.0.95.0-1`
- ActiveMQ – `5.18.4.0-1`
- Java – `11.76.21.1`
- One SSO-Anbieter – `6.7.7.0`
- Self-Service-Funktionen für die Passwortrücksetzung – `4.8.0.1`
- Identity Applications – `4.10.0`
- Identity Reporting – `7.4.0`

Dieser Abschnitt enthält Informationen zu folgenden Themen:

- „Erläuterungen zum Aufrüstungsprogramm“, auf Seite 176
- „Voraussetzungen für die Aufrüstung“, auf Seite 176

- „Systemanforderungen“, auf Seite 176
- „Aufrüsten der PostgreSQL-Datenbank“, auf Seite 176
- „Upgrade der Treiberpakete für Identity Applications“, auf Seite 179
- „Aufrüsten von Identity Applications“, auf Seite 179
- „Aufgaben nach der Aufrüstung für Identity Applications“, auf Seite 180

Erläuterungen zum Aufrüstungsprogramm

Im Rahmen des Aufrüstungsvorgangs werden die Konfigurationswerte der vorhandenen Komponenten gelesen. Hierzu gehören die Dateien `ism-configuration.properties`, `server.xml`, SSPR`Configuration.xml` und weitere Konfigurationsdateien. Beim Aufrufen dieser Konfigurationsdateien wird intern das Aufrüstungsprogramm für die zugehörigen Komponenten gestartet. Darüber hinaus erstellt dieses Programm eine Sicherung der aktuellen Installation.

Voraussetzungen für die Aufrüstung

Wenn Ihre Datenbank über SSL konfiguriert ist, ersetzen Sie in der Datei `server.xml`, die sich im Pfad `C:\NetIQ\idm\apps\tomcat\conf` befindet, `ssl=true` durch `sslmode=require`.

Ändern Sie beispielsweise

```
jdbc:postgresql://<postgres db>:5432/idmuserappdb?ssl=true
```

in

```
jdbc:postgresql://<postgres db>:5432/idmuserappdb?sslmode=require
```

Systemanforderungen

Im Rahmen des Aufrüstungsvorgangs wird eine Sicherung der aktuellen Konfiguration für die installierten Komponenten erstellt. Auf Ihrem Server muss ausreichend freier Speicherplatz für die Sicherung vorhanden sein sowie weiterer freier Speicherplatz für die Aufrüstung.

Aufrüsten der PostgreSQL-Datenbank

WICHTIG: Die Aufrüstung kann je nach Größe der Datenbank einige Zeit in Anspruch nehmen. Planen Sie die Aufrüstung daher entsprechend.

1. Halten Sie den PostgreSQL-Dienst an, der auf dem Server ausgeführt wird.
2. Benennen Sie das Verzeichnis `postgres` unter `C:\Netiq\idm\` um.

   Benennen Sie `postgres` beispielsweise in `postgresql_old` um.
3. Entfernen Sie den alten Dienst, indem Sie den folgenden Befehl ausführen:

   `sc delete „<postgres-Dienstname>”`
4. Installieren Sie eine von Ihrem Betriebssystem unterstützte PostgreSQL-Version.

Sie müssen einen Speicherort auswählen, der nicht dem aktuellen Installationsort von PostgreSQL entspricht.

4a Stellen Sie die Image-Datei `Identity_Manager_4.10.0_Windows.iso` bereit und navigieren Sie zum Verzeichnis `\common\postgres_tomcat`.

4b Führen Sie die Datei `TomcatPostgreSQL.exe` aus.

Wählen Sie für die Installation nur die Option **PostgreSQL** aus.

HINWEIS

- Die Optionen **Datenbank-Anmeldekonto erstellen** und **Leere Datenbank erstellen** sind standardmäßig deaktiviert.
- Stellen Sie sicher, dass Sie über Administratorberechtigungen für das alte und neue PostgreSQL -Installationsverzeichnis verfügen.

---

5 Halten Sie den neu installierten PostgreSQL-Dienst an. Navigieren Sie zu **Services**, suchen Sie nach dem Service *<PostgreSQL-Versionsnummer>* und stoppen Sie den Service.

HINWEIS: Benutzer mit entsprechenden Rechten können Dienste nach entsprechender Authentifizierung anhalten.

---

6 Ändern Sie die Rechte für das neu erstellte PostgreSQL-Verzeichnis wie folgt:

Erstellen Sie einen `postgres`-Benutzer:

1. Navigieren Sie zu **Systemsteuerung > Benutzerkonten > Benutzerkonten > Konten verwalten**.
2. Klicken Sie auf **Benutzerkonto hinzufügen**.
3. Geben Sie auf der Seite für das Hinzufügen von Benutzern `postgres` als Benutzernamen an und legen Sie ein Passwort fest.

Weisen Sie dem Benutzer `postgres` Rechte für die bestehenden und neuen PostgreSQL-Verzeichnisse zu:

1. Klicken Sie mit der rechten Maustaste auf das PostgreSQL-Verzeichnis und navigieren Sie zu **Eigenschaften > Sicherheit > Bearbeiten**.
2. Wählen Sie **Vollzugriff** für den Benutzer aus, um uneingeschränkte Rechte bereitzustellen.
3. Klicken Sie auf **Anwenden**.

7 Führen Sie vor der Anmeldung als Postgres-Benutzer diese Schritte aus, um den Benutzer zur Liste der rdp-zulässigen Benutzer hinzuzufügen.

1. Öffnen Sie die Anwendung „Computer-Management“.
2. Navigieren Sie zu **System Tools > Local Users and Groups > Groups** (Systemprogramme > Lokale Benutzer und Gruppen > Gruppen).
3. Doppelklicken Sie auf **Remote Desktop Users** (Remote-Desktop-Benutzer).
4. Klicken Sie im Popup-Fenster „Remote Desktop Users Properties“ (Eigenschaften von Remote Desktop-Benutzern) auf **Add** (Hinzufügen).
5. Geben Sie den Postgres-Benutzer ein und schließen Sie alle geöffneten Postgres-Verzeichnisse.

8 Greifen Sie als Benutzer `postgres` auf das PostgreSQL-Verzeichnis zu.

1. Melden Sie sich als `postgres`-Benutzer am Server an.

Stellen Sie vor der Anmeldung sicher, dass `postgres` sich mit dem Windows-Server verbinden kann, indem Sie prüfen, ob der Benutzer Remote-Verbindungen vornehmen darf.

2. Löschen Sie das Datenverzeichnis aus dem neuen Postgres-Installationsverzeichnis. Beispiel: `C:\NetIQ\idm\apps\postgres\data`
3. Öffnen Sie eine Eingabeaufforderung und legen Sie mithilfe des folgenden Befehls PGPASSWORD fest:

   ```
   set PGPASSWORD=<your pg password>
   ```

4. Wechseln Sie zum neu erstellten PostgreSQL-„bin“-Verzeichnis.

   Beispiel: `C:\NetIQ\IDM\apps\postgres\bin`

5. Führen Sie `initdb` als `postgres`-Datenbankbenutzer aus.

   ```
   initdb.exe -D <neues_Datenverzeichnis> -E WIN1252 -U postgres
   ```

   Beispiel:

   ```
   initdb.exe -D C:\NetIQ\idm\apps\postgres\data -E WIN1252 -U postgres
   ```

9 Führen Sie über das neue PostgreSQL-`bin`-Verzeichnis die PostgreSQL-Aufrüstung durch. Führen Sie den folgenden Befehl aus und klicken Sie auf **Eingabe**.

HINWEIS: Stellen Sie sicher, dass Sie den **Methode**-Typ in `pg_hba.conf` im Verzeichnis `C:\NetIQ\idm\apps\postgres\data\` von `md5` in `trust` ändern.

```
pg_upgrade.exe --old-datadir "C:\NetIQ\idm\postgres_old\data" --new-
datadir "C:\NetIQ\idm\apps\postgres\data" --old-bindir
"C:\NetIQ\idm\postgres_old\bin" --new-bindir
"C:\NetIQ\idm\apps\postgres\bin"
```

10 Ersetzen Sie nach einem erfolgreichen Upgrade die Dateien `pg_hba.conf` und `postgresql.conf` im neuen Postgres-Datenverzeichnis (`C:\NetIQ\idm\apps\postgres\data`) durch die Dateien aus dem alten Postgres-Verzeichnis.

11 Starten Sie den aufgerüsteten PostgreSQL-Datenbankdienst.

Navigieren Sie zu **Services**, suchen Sie nach dem Service *<PostgreSQL-Versionsnummer>* und starten Sie den Service.

HINWEIS: Benutzer mit entsprechenden Rechten können Dienste nach einer Authentifizierung starten.

---

12 (Optional) Nachdem bestätigt wurde, dass die migrierte Datenbank ordnungsgemäß funktioniert, können die ursprünglichen Datendateien gelöscht werden. Führen Sie die folgenden Schritte aus, um die ursprünglichen Datendateien zu löschen:

1. Melden Sie sich als Benutzer `postgres` an.
2. Navigieren Sie zum bin-Verzeichnis im neu erstellten Postgres und führen Sie die Dateien `analyze_new_cluster.bat` und `delete_old_cluster.bat` aus.

   Beispiel: `C:\NetIQ\idm\apps\postgresql\bin`

HINWEIS: Diesen Schritt müssen Sie nur durchführen, wenn Sie alte Datendateien löschen möchten.

Upgrade der Treiberpakete für Identity Applications

Sie müssen Tomcat beenden und die Pakete für den Benutzeranwendungstreiber und den Rollen- und Ressourcenservice-Treiber auf die neueste Version aktualisieren. Informationen zum Upgrade der Pakete auf die aktuelle Version finden Sie unter Upgrade der installierten Pakete im *Administrationshandbuch zu Designer für OpenText™ Identity Manager CE 24.4 (v4.10)*.

Nach dem Upgrade der Treiberpakete für die Benutzeranwendung müssen Sie das Paket mit den Workflow-Vorlagen manuell hinzufügen:

1. Navigieren Sie in Designer zu **Benutzeranwendungstreiber** > **Eigenschaften**.
2. Klicken Sie auf „Pakete“ und dann auf .
3. Wählen Sie **Workflow-Vorlagen erstellen** aus.
4. Klicken Sie auf **OK** und dann auf **Fertig stellen**, um die Installation abzuschließen.
5. Stellen Sie den Benutzeranwendungstreiber bereit.

WICHTIG: Wenn eine Vorlage für E-Mail-Benachrichtigungen installiert ist oder im Rahmen des Upgrades des Benutzeranwendungstreibers aktualisiert wird, müssen Sie das Objekt **Standard-Benachrichtigungssammlung** bereitstellen.

Aufrüsten von Identity Applications

Im folgenden Vorgang wird die Vorgehensweise zur Aufrüstung der folgenden Komponenten beschrieben:

- Identity Applications
- OSP
- Tomcat
- PostgreSQL
- SSPR (falls auf demselben Computer installiert wie Identity Applications)
- ActiveMQ

Führen Sie zum Aufrüsten von Identity Applications die folgenden Schritte aus:

1. Laden Sie die Datei `Identity_Manager_4.10.0_Windows.iso` von der OpenText-Downloads-Website herunter.
2. Stellen Sie die heruntergeladene `.iso`-Datei bereit.
3. Navigieren Sie zum Ordner `<Speicherort der installierten ISO-Datei>\IdentityApplications` und führen Sie die Datei `install.exe` aus.
4. Wählen Sie die Sprache für die Installation aus und klicken Sie auf **OK**.
5. Klicken Sie auf der Einführungsseite auf **Weiter**.
6. Lesen und akzeptieren Sie die Lizenzvereinbarung und klicken Sie dann auf **Weiter**.

Die installierten Komponenten und deren Versionen werden angezeigt.

7 Wählen Sie **Identity Applications** aus und klicken Sie auf **Weiter**.

8 Geben Sie die Konfigurationseinstellungen für Identity Applications an. Weitere Informationen finden Sie unter „Arbeitsblatt zur Konfiguration von Identity Applications“, auf Seite 54.

HINWEIS

- Wir empfehlen, die Workflow-Datenbank mit dem OpenText Identity Manager-Installationsprogramm zu erstellen, wenn Sie die PostgreSQL-Datenbank auf dem gleichen Server wie Identity Applications installiert haben.
- Während der Aufrüstung müssen Sie die JDBC-JAR-Datei der Datenbank manuell angeben. Wenn Sie beispielsweise die PostgreSQL-Datenbank verwenden, müssen Sie den Speicherort der Datenbank-JAR angeben, die sich außerhalb des Ordners `tomcat\lib` befindet.

---

9 Lesen Sie auf der Seite der Zusammenfassung vor der Aufrüstung die Einstellungen und klicken Sie auf **Aufrüsten**.

Abhängig davon, wo Sie die Komponenten installiert haben, wird das Sicherungsverzeichnis in diesem Verzeichnis erstellt und ein Zeitstempel (mit der Uhrzeit der Sicherung) wird an das gesicherte Verzeichnis angehängt.

Beispiel:

- Tomcat – `C:\NetIQ\idm\apps\tomcat_backup_02262018_033634`
- OSP und SSPR – `C:\NetIQ\idm\apps\osp_sspr_backup_02262018_033634`
- ActiveMQ – `C:\NetIQ\idm\apps\activemq_backup_02262018_033634`
- Benutzeranwendung – `C:\NetIQ\idm\apps\UserApplication_backup_02262018_033634`
- Identity Reporting – `C:\NetIQ\idm\apps\IdentityReporting_backup_02262018_033634`

Aufgaben nach der Aufrüstung für Identity Applications

Nach dem Aufrüsten von OpenText Identity Manager von 4.7.5 auf 4.10 wird der Typ des Schlüsselspeichers im Dienstprogramm für die Konfigurationsaktualisierung automatisch zu pkcs12 geändert. Stellen Sie sicher, dass Sie den Typ der Schlüsselspeicherdateien im Dienstprogramm für die Konfigurationsaktualisierung von pkcs12 zu jks ändern, die vor dem Aufrüsten für die folgenden Einträge in jks vorliegen:

- Identitätsdepot-Zertifikate
- Authentifizierungsserver
- Authentifizierungsschlüssel
- RBPM

Führen Sie nach dem Aufrüsten von Identity Applications von 4.7.5 auf 4.10 die folgenden Schritte aus:

1. Wenn Sie Identity Applications in einer verteilten Einrichtung installiert haben, bearbeiten Sie configupdate.properties und ändern Sie die Edition zu Advanced.
2. Nehmen Sie in der Datei configupdate die folgenden Änderungen vor:
   - Geben Sie den korrekten OSP-Port an.
   - Stellen Sie sicher, dass alle Registerkarten für TLS-Einträge korrigiert sind.
3. Aktualisieren Sie die folgenden ism-configuration.properties:

   ```
   com.netiq.idm.osp.oauth-truststore.file =
   C:\\\\NetIQ\\\\IDM\\\\apps\\\\tomcat\\\\conf\\\\idm.jks

   com.netiq.idm.osp.oauth-truststore.pwd._attr_obscurity = ENCRYPT

   com.netiq.idm.osp.oauth-truststore.pwd = GqJVxLBPwgWLK1/
   ULnOb4A==:JoxqTICngaIQtU3z/u7v/w==:2jk5gzsEca+kaz6x7xjE6g==
   ```

4. Starten Sie den Tomcat-Service neu.

Wenn Sie Identity Applications in einer Cluster-Umgebung aktualisieren, kopieren Sie die folgenden Dateien vom primären Knoten auf alle Knoten der Benutzeranwendungen:

- `ism-sensitive.properties`
- `ism-configuration.properties`
- `encrypt-keys.pkcs12`

Wenn Sie Identity Applications und SSPR auf verschiedenen Servern installiert haben, müssen Sie das vertrauenswürdige SSPR-Zertifikat mit dem CN „Identity Applications“ in die Datei `cacerts` des Identity Applications-Servers importieren.

Sie müssen außerdem die benutzerdefinierten Einstellungen für Tomcat, SSPR, OSP oder Identity Applications manuell wiederherstellen.

Führen Sie die nach der Aufrüstung vorzunehmenden Schritte für die erforderlichen Komponenten durch:

- „Java“, auf Seite 181
- „Tomcat“, auf Seite 182
- „Identity Applications“, auf Seite 183
- „One SSO-Anbieter“, auf Seite 183
- „Self-Service Password Reset“, auf Seite 183
- „Kerberos“, auf Seite 184

Java

Überprüfen Sie die Zertifikate am aufgerüsteten JRE-Speicherort: `jre\lib\security\cacerts` im Vergleich zu Ihrem alten JRE-Speicherort. Importieren Sie die fehlenden Zertifikate manuell in `cacerts`.

1 Importieren Sie `java cacerts` mit dem Befehl `keytool`:

```
keytool -import -trustcacerts -file Certificate_Path -alias ALIAS_NAME
-keystore cacerts
```

HINWEIS: Nach der Aufrüstung ist JRE im Installationsverzeichnis der Identity Applications gespeichert. Beispiel: `C:\NetIQ\idm\apps\jre`

2 Starten Sie das Identitätsdepot neu.

3 Stellen Sie sicher, dass der JRE-Startort `tomcat\bin\setenv.bat` ist.

4 Starten Sie das **Konfigurationsaktualisierungsprogramm** und prüfen Sie den Pfad der `cacerts`.

Tomcat

1 (Bedingt) Möchten Sie benutzerdefinierte Dateien aus der zuvor im Rahmen der Aufrüstung erstellten Sicherung wiederherstellen, gehen Sie wie folgt vor:

- Stellen Sie benutzerdefinierte https-Zertifikate wieder her. Kopieren Sie zur Wiederherstellung der Zertifikate den Inhalt der Java Secure Socket Extension (JSSE) aus der gesicherten `server.xml`-Datei zur neuen `server.xml` -Datei im Verzeichnis `\tomcat\conf`.
- Kopieren Sie nicht die Konfigurationsdateien vom gesicherten Tomcat-Verzeichnis in das neue Tomcat-Verzeichnis. Starten Sie mit der Standardkonfiguration der neuen Version und nehmen Sie die erforderlichen Änderungen vor. Weitere Informationen finden Sie auf der Apache-Website.

  Stellen Sie sicher, dass die neue Datei `server.xml` folgende Einträge aufweist:

```
<Connector port="8543" protocol="HTTP/1.1"
       maxThreads="150" SSLEnabled="true" scheme="https"
secure="true"
       clientAuth="false" sslProtocol="TLS"
       keystoreFile="path_to_keystore_file"
       keystorePass="keystore_password" />
<!--
      <Cluster
className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>
 -->
```

  Alternativ:

```
<Connector port="8543"
protocol="org.apache.coyote.http11.Http11NioProtocol"
       maxThreads="150" SSLEnabled="true" scheme="https"
secure="true"
       clientAuth="false" sslProtocol="TLS"
       keystoreFile="path_to_keystore_file"
       keystorePass="keystore_password" />
<!--
      <Cluster
className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>
 -->
```

HINWEIS: In einer Cluster-Umgebung kommentieren Sie das Tag `Cluster` in `server.xml` manuell aus und kopieren Sie `osp.jks` auf alle Knoten vom ersten Knoten unter `C:\netiq\idm\apps\osp_backup_<Datum>`.

- Wenn Ihnen benutzerdefinierte Keystore-Dateien vorliegen, fügen Sie den korrekten Pfad der neuen `server.xml`-Datei hinzu.
- Importieren Sie die Zertifikate der Identity Applications in das Identitätsdepot unter / `C:\NetIQ\eDirectory\jre\lib\security\cacerts`.

  Sie können die Zertifikate beispielsweise mit dem folgenden „keytool“-Befehl in das Identitätsdepot importieren:

  ```
  keytool -importkeystore -alias <User Application certificate alias>
  -srckeystore <backup cacert> -srcstorepass changeit -destkeystore
  C:\NetIQ\eDirectory\jre\lib\security\cacerts
  ```

2 (Bedingt) Navigieren Sie zur Benutzeranwendung und stellen Sie die benutzerdefinierten Einstellungen manuell wieder her. Lesen Sie hierzu die gesicherte Konfiguration wieder ein.

Identity Applications

Beim Upgrade der Identity Applications von 4.7.5 auf 4.10 müssen Sie sicherstellen, dass der Parameter `Dcom.novell.afw.wf.engine-id=IDMProv` in der Datei `setenv` im Ordner `tomcat/bin` vorhanden ist. Falls dieser Parameter nach dem Upgrade der Identity Applications fehlt, müssen Sie ihn manuell in der Datei `setenv` hinzufügen und den Tomcat-Server neu starten.

One SSO-Anbieter

Standardmäßig ist der Eintrag `LogHost` in der Datei `logevent.conf` auf `localhost` eingestellt.

Zum Bearbeiten des Eintrags `LogHost` stellen Sie die benutzerdefinierten OSP-Konfigurationen manuell anhand der Sicherung wieder her, die im Rahmen des Aufrüstungsvorgangs erstellt wurde.

Self-Service Password Reset

Aktualisieren Sie nach der Aufrüstung von SSPR den SSO-Client-Parameter mit dem Konfigurationsaktualisierungsprogramm. Weitere Informationen finden Sie unter „Parameter für SSO-Clients“, auf Seite 93.

Aktualisieren Sie die SSPR-Konfigurationsdetails mit den folgenden Schritten:

1 Melden Sie sich beim SSPR-Portal als Administrator an.

2 Aktualisieren Sie die Audit-Serverdetails:

  2a Navigieren Sie zu **Ihre ID > Konfigurationseditor** und geben Sie das Konfigurationspasswort an.

  2b Wählen Sie **Einstellungen > Revision > Audit-Weiterleitung > Syslog-Audit Server-Zertifikate** aus.

  2c Importieren Sie diese Zertifikate vom Server und klicken Sie auf **Speichern**.

3 Importieren Sie die **LocalDB** in SSPR:

   3a Navigieren Sie im Dropdown-Menü zu **IhreID > Konfigurationsmanager**.

   3b Klicken Sie auf **LocalDB**.

   3c Klicken Sie auf **LocalDB-Archivdatei importieren (hochladen)**.

4 (Bedingt) So schränken Sie die Konfiguration für SSPR ein:

   4a Navigieren Sie in der Liste zu **IhreID > Konfigurationsmanager**.

   4b Klicken Sie auf **Konfiguration einschränken**.

5 Konfigurieren Sie die Administratorberechtigungen für SSPR (siehe „Schritte nach der Installation“, auf Seite 60).

Starten Sie die aufgerüsteten Komponenten, um zu prüfen, ob die Aufrüstung erfolgreich war.

Starten Sie beispielsweise das OpenText Identity Manager-Dashboard und klicken Sie auf **Info**. Prüfen Sie, ob die Anwendung die neue Version anzeigt, zum Beispiel **4.10.0**.

Kerberos

Das Aufrüstungsprogramm erstellt einen neuen Tomcat-Ordner auf dem Computer. Falls sich Kerberos-Dateien (z. B. `keytab` und `Kerberos_login.config`) im bisherigen Tomcat-Ordner befinden, kopieren Sie diese Dateien aus dem gesicherten Ordner in den neuen Tomcat-Ordner.

Aufrüsten von Identity Reporting

Identity Reporting umfasst zwei Treiber. Unter Umständen müssen Sie auch Inhalte aus dem OpenText Event Auditing Service (EAS) zu Sentinel Log Management für IGA migrieren. Nehmen Sie die Aufrüstung in der nachstehenden Reihenfolge vor:

1. Rüsten Sie Sentinel Log Management für IGA auf. Weitere Informationen finden Sie unter Aufrüsten von Sentinel Log Management für IGA im Einrichtungshandbuch zu OpenText™ Identity Manager CE 24.4 (v4.10) für Linux.
2. Rüsten Sie Identity Reporting auf.

Voraussetzungen für die Aufrüstung

Wenn Ihre Datenbank über SSL konfiguriert ist, ersetzen Sie in der Datei `server.xml`, die sich im Pfad `C:\NetIQ\idm\apps\tomcat\conf` befindet, `ssl=true` durch `sslmode=require`.

Ändern Sie beispielsweise

```
jdbc:postgresql://<postgres db>:5432/idmrptdb?ssl=true
```

in

```
jdbc:postgresql://<postgres db>:5432/idmrptdb?sslmode=require
```

Aufrüsten von Identity Reporting

Vor der Aufrüstung von Identity Reporting müssen Sie zunächst Identity Applications und SLM for IGA aufrüsten. Zum Aufrüsten von Identity Reporting installieren Sie die neue Version über die bisherige Version.

Führen Sie zum Aufrüsten von Identity Reporting die folgenden Schritte aus:

1. Laden Sie die Datei `Identity_Manager_4.10.0_Windows.iso` vom Softwarelizenz- und Download-Portal (https://sld.microfocus.com) herunter.
2. Stellen Sie die heruntergeladene `.iso`-Datei bereit.
3. Navigieren Sie zum Ordner <`Speicherort der installierten ISO-Datei`>`\IdentityReporting` und führen Sie die Datei `install.exe` aus.
4. Wählen Sie die Sprache für die Installation aus und klicken Sie auf **OK**.
5. Klicken Sie auf der Einführungsseite auf **Weiter**.
6. Lesen und akzeptieren Sie die Lizenzvereinbarung und klicken Sie dann auf **Weiter**.

   Die installierten Komponenten und deren Versionen werden angezeigt.
7. Wählen Sie **Identity Reporting** aus und klicken Sie auf **Weiter**.
8. Geben Sie die Konfigurationseinstellungen für Identity Reporting an. Weitere Informationen finden Sie unter „Arbeitsblatt zur Konfiguration von Identity Reporting“, auf Seite 57.
9. Lesen Sie auf der Seite der Zusammenfassung vor der Aufrüstung die Einstellungen und klicken Sie auf **Aufrüsten**.

   Melden Sie sich nach dem erfolgreichen Upgrade von Identity Reporting bei der Reporting-Benutzeroberfläche an und prüfen Sie die Version. Weitere Informationen finden Sie unter „Überprüfen der Aufrüstung für Identity Reporting“, auf Seite 187.

HINWEIS

- Die Eigenschaft `com.netiq.rpt.ssl-keystore.type` in der Datei `ism-configuration.properties` behält den Wert (JKS/PKCS12), der vor dem Aufrüsten festgelegt wurde.
- Wenn Sie Identity Reporting von 4.8.7 auf 4.10 aufrüsten, wird der Java 8-basierte Tomcat an folgendem Speicherort gesichert: `c:\netiq\idm\apps\tomcat\conf`.

Schritte nach der Aufrüstung für Reporting

Wenn Sie während der Aufrüstung bei der Aufforderung, `ein Schema für Identity Reporting zu erstellen`, die Option "Start" oder "Datei" wählen, müssen Sie die Datenquelle manuell über die Benutzeroberfläche von Identity Reporting hinzufügen. Navigieren Sie zum

Hinzufügen zu der Option **Datenquellen**, klicken Sie auf **Hinzufügen** und wählen Sie dann `IDMDCSDataSource` aus der Liste aus. Starten Sie außerdem Tomcat neu, nachdem Sie ihn einmal gestartet haben, um sicherzustellen, dass die verfügbare Datenbank ordnungsgemäß läuft.

Nach dem Aufrüsten von Identity Reporting auf Version 4.9 navigieren Sie zur Datei `ism-configuration.properties`, die sich im Verzeichnis `/opt/netiq/idm/apps/tomcat/conf/` befindet, und führen Sie die folgenden Aktionen aus:

- Ändern Sie den Wert der Eigenschaft `com.netiq.rpt.landing.url` wie folgt:

  ```
  com.netiq.rpt.landing.url = ${com.netiq.idm.osp.url.host}/idmdash/#/landing
  ```

- Ändern Sie den Wert der Eigenschaft `com.netiq.idmdcs.landing.url` wie folgt:

  ```
  com.netiq.idmdcs.landing.url = ${com.netiq.idm.osp.url.host}/idmdash/#/landing
  ```

- Geben Sie den Wert für die Eigenschaft `com.netiq.rpt.redirect.url` im folgenden Format an: `https:<Hostname>:<Port>/path`

  Beispiel: `com.netiq.rpt.redirect.url = https://192.168.0.1:8543/IDMRPT/oauth.html`

Nach dem Aufrüsten von OpenText Identity Manager von 4.7.5 auf 4.10 wird der Typ des Schlüsselspeichers im Dienstprogramm für die Konfigurationsaktualisierung automatisch zu pkcs12 geändert. Stellen Sie sicher, dass Sie den Typ der Schlüsselspeicherdateien im Dienstprogramm für die Konfigurationsaktualisierung von pkcs12 zu jks ändern, die vor dem Aufrüsten für die folgenden Einträge in jks vorliegen:

- Identitätsdepot-Zertifikate
- Authentifizierungsserver
- Authentifizierungsschlüssel
- RBPM

Führen Sie nach dem Aufrüsten von Identity Reporting von 4.7.5 auf 4.9 die folgenden Schritte aus:

1. (Bedingt) Wenn Sie Identity Applications in einer verteilten Einrichtung installiert haben, bearbeiten Sie configupdate.properties und ändern Sie die Edition zu Advanced.
2. Nehmen Sie in der Datei configupdate die folgenden Änderungen vor:
   - Geben Sie den korrekten OSP-Port an.
   - Stellen Sie sicher, dass alle Registerkarten für TLS-Einträge korrigiert sind.
3. Aktualisieren Sie die folgenden ism-configuration.properties:

   ```
   com.netiq.rpt.authserver.url = https://apps.<example>.com:8543
   ```

   ```
   com.netiq.rpt.ssl-keystore.file =
   C:\\\\NetIQ\\\\IDM\\\\apps\\\\tomcat\\\\conf\\\\idm.jks
   ```

   ```
   com.netiq.rpt.ssl-keystore.pwd._attr_obscurity = ENCRYPT
   ```

   ```
   com.netiq.rpt.ssl-keystore.pwd = GqJVxLBPwgWLK1/
   ULnOb4A==:JoxqTICngaIQtU3z/u7v/w==:2jk5gzsEca+kaz6x7xjE6g==
   ```

   ```
   com.netiq.rpt.ssl-keystore.type = JKS/PKCS12
   ```

```
com.netiq.idm.osp.oauth-truststore.file =
C:\\\\NetIQ\\\\IDM\\\\apps\\\\tomcat\\\\conf\\\\idm.jks

com.netiq.idm.osp.oauth-truststore.pwd._attr_obscurity = ENCRYPT

com.netiq.idm.osp.oauth-truststore.pwd = GqJVxLBPwgWLK1/
ULnOb4A==:JoxqTICngaIQtU3z/u7v/w==:2jk5gzsEca+kaz6x7xjE6g==
```

4. Starten Sie den Tomcat-Service neu.

Ändern der Verweise auf reportRunner in der Datenbank

Aktualisieren Sie die Verweise auf reportRunner in der Datenbank, nachdem Sie Identity Reporting aufgerüstet und Tomcat zum ersten Mal gestartet haben.

1 Halten Sie Tomcat an.

2 Navigieren Sie zum Installationsverzeichnis von Identity Reporting und benennen Sie den Ordner `reportContent` in `ORG-reportContent` um.

Beispiel: `C:\NetIQ\idm\apps\IdentityReporting`

3 Löschen Sie den Inhalt der temporären Verzeichnisse und Arbeitsverzeichnisse im Tomcat-Ordner.

4 Melden Sie sich bei der PostgreSQL-Datenbank an.

4a Suchen Sie die reportRunner-Verweise in den folgenden Tabellen:

- `idm_rpt_cfg.idmrpt_rpt_params`
- `idm_rpt_cfg.idmrpt_definition`

4b Geben Sie die folgenden Löschanweisungen aus:

```
DELETE FROM idm_rpt_cfg.idmrpt_rpt_params WHERE
rpt_def_id='com.novell.content.reportRunner';

DELETE FROM idm_rpt_cfg.idmrpt_definition WHERE
def_id='com.novell.content.reportRunner';
```

5 Starten Sie Tomcat.

Sehen Sie sich in den Protokollen an, ob die Berichte mit dem korrekten reportRunner aktualisiert wurden.

6 Melden Sie sich bei Identity Reporting an und führen Sie die Berichte aus.

Überprüfen der Aufrüstung für Identity Reporting

1 Starten Sie Identity Reporting.

2 Überprüfen Sie, ob alte und neue Berichte im Werkzeug angezeigt werden.

3 Überprüfen Sie im **Kalender**, ob die geplanten Berichte aufgeführt sind.

4 Überprüfen Sie, ob die Seite **Einstellungen** die bisherigen Einstellungen für verwaltete und nicht verwaltete Anwendungen enthält.

5 Überprüfen Sie, ob alle anderen Einstellungen fehlerfrei sind.

6 Überprüfen Sie, ob die abgeschlossenen Berichte in der Anwendung aufgelistet sind.

Aufrüsten von Analyzer

Für die Aufrüstung von Analyzer stellen wir Patch-Dateien im `.zip`-Format bereit. Stellen Sie vor dem Aufrüsten von Analyzer sicher, dass der Computer den Voraussetzungen und Systemanforderungen entspricht. Weitere Informationen finden Sie in den Versionshinweisen für die Aktualisierung.

WICHTIG: Das Analyzer-Tool ist nicht in der ISO für OpenText Identity Manager 24.4 (v4.10) enthalten. Wenn Analyzer bereits installiert ist, aktualisieren Sie ihn auf Version 4.8.5 und verwenden Sie ihn mit OpenText Identity Manager 24.4 (v4.10).

---

1. Laden Sie die Patch-Datei, z. B. `Identity_Manager_4.8.5_Analyzer_Windows.zips`, von der Seite Software und Lizenz (https://sld.microfocus.com/) herunter.
2. Extrahieren Sie die `.zip`-Datei in das Verzeichnis, in dem sich die Analyzer-Installationsdateien befinden (z. B. die Plugins, das Deinstallationsskript und andere Analyzer-Dateien).
3. Starten Sie Analyzer neu.
4. Überprüfen Sie mit den folgenden Schritten, ob der neue Patch erfolgreich angewendet wurde:
   - **4a** Starten Sie Analyzer.
   - **4b** Klicken Sie auf **Hilfe > Info**.
   - **4c** Überprüfen Sie, ob die neue Version angezeigt wird, z. B. **4.6 Update 1** und Build-ID **20121128**.

Arbeitsschritte nach der Aktualisierung

Führen Sie nach der Aufrüstung die folgenden Aktion aus:

HINWEIS: Stellen Sie nach der Aufrüstung von Identity Applications und Identity Reporting die während der Installation verwendeten JAR-Dateien – entweder `ojdbc8.jar` für Oracle oder `mssql-jdbc-9.2.1.jre8.jar` für MSSQL – basierend auf der verwendeten Datenbank im Verzeichnis `tomcat/lib` wieder her. Starten Sie dann die Tomcat-Dienste neu.

Konfigurieren von TLSv1.3 für Tomcat-Dienste

Führen Sie die folgenden Schritte aus, um TLSv1.3 zu konfigurieren:

1. Navigieren Sie zum Verzeichnis `C:\NetIQ\IDM\apps\tomcat\conf` und fügen Sie die folgenden Einträge zur `server.xml`-Datei hinzu.

   ```
   useServerCipherSuitesOrder="true"
   ```

   ```
   ciphers="TLS_AES_256_GCM_SHA384,TLS_CHACHA20_POLY1305_SHA256,TLS_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
   ```

   ```
   sslEnabledProtocols="TLSv1.2+TLSv1.3"
   ```

   Beispiel:

```
<Connector port="8543" protocol="HTTP/1.1" URIEncoding="UTF-8"
maxThreads="200" enableLookups="true" scheme="https" secure="true"
maxHttpHeaderSize="65536" SSLEnabled="true" sslProtocol="TLS"
disableUploadTimeout="true" keystoreFile="conf/tomcat.ks"
keystorePass="novell" useServerCipherSuitesOrder="true"
ciphers="TLS_AES_256_GCM_SHA384,TLS_CHACHA20_POLY1305_SHA256,TLS_AES_1
28_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WI
TH_AES_256_CBC_SHA384" sslEnabledProtocols="TLSv1.2+TLSv1.3" />
```

2. Öffnen Sie die Datei `ism-configuration.properties` und bearbeiten Sie den folgenden Eintrag, der von TLSv1.2 zu TLSv1.3 geändert wird:

   ```
   com.netiq.idm.sslProtocol = TLSv1.3
   ```

3. Starten Sie die Tomcat-Dienste neu.

HINWEIS: Wenn in der OpenText Identity Manager-Umgebung eine Diskrepanz in der SSPR- und Tomcat-TLS-Konfiguration besteht, hat die Tomcat-TLS-Konfiguration, die in `ism-configuration.properties` auf 1.3 gesetzt ist, Vorrang – unabhängig davon, ob die SSPR-TLS-Konfiguration auf 1.2 gesetzt ist.

Aufgaben nach dem Upgrade im FIPS-aktivierten Modus

Nach dem Upgrade von OpenText Identity Manager im FIPS-aktivierten Modus:

- Stellen Sie sicher, dass Java-Keystores im JKS-Format in das BCFKS-Format konvertiert werden.

  Ändern Sie beispielsweise in der Datei `ism-configuration.properties` die folgenden Eigenschaften von JKS in das BCFKS-Format:

  ```
  com.sssw.fw.security.sigcert.truststore.path = /opt/netiq/idm/apps/
  tomcat/conf/idm.bcfkscom.netiq.idm.ua.ldap.edit.keystore-type =
  BCFKScom.netiq.idm.ua.ldap.edit.keystore-type.other =
  BCFKScom.netiq.idm.osp.oauth-truststore.file = /opt/netiq/idm/apps/
  tomcat/conf/idm.bcfksDirectoryService/realms/jndi/params/KEYSTORE_PATH
  = /opt/netiq/idm/apps/tomcat/conf/idm.bcfkscom.netiq.rpt.ssl-
  keystore.file = /opt/netiq/idm/apps/tomcat/conf/idm.bcfks
  ```

- Stellen Sie sicher, dass Sie die Anpassung in der Datei `java.security` im Ordner `<jre-root>\conf\security` aktualisieren, indem Sie die folgenden Schritte ausführen:

  1. Suchen Sie nach der Zeichenkette Liste der Anbieter und ihrer Präferenzordnung, kommentieren Sie alle vorhandenen Anbieter aus und fügen Sie die folgenden Einträge hinzu:

     ```
     security.provider.1=BCFIPS
     security.provider.2=BCJSSE
     security.provider.3=SunJSSE
     security.provider.4=SUN
     security.provider.5=SunJCE
     ```

  2. Suchen Sie nach der Zeichenkette `ssl.KeyManagerFactory.algorithm=SunX509`, kommentieren Sie sie aus und fügen Sie dann Folgendes hinzu:

     ```
     ssl.KeyManagerFactory.algorithm=PKIX
     ```

3. Suchen Sie nach der Zeichenkette `keystore.type`, kommentieren Sie sie aus und fügen Sie dann Folgendes hinzu:

   ```
   keystore.type=bcfks
   ```

Anhalten und Starten der OpenText Identity Manager-Treiber

Unter Umständen müssen die OpenText Identity Manager-Treiber gestartet oder gestoppt werden, damit die richtigen Dateien im Rahmen einer Installation oder Aufrüstung geändert oder ersetzt werden können. In diesem Abschnitt werden die folgenden Vorgänge beschrieben:

- „Anhalten der Treiber“, auf Seite 190
- „Starten der Treiber“, auf Seite 191

Anhalten der Treiber

Vor dem Ändern von Dateien für einen Treiber muss der entsprechende Treiber angehalten werden.

- „Anhalten der Treiber mithilfe von Designer“, auf Seite 190
- „Anhalten der Treiber mit der OpenText Identity Console“, auf Seite 190

Anhalten der Treiber mithilfe von Designer

1 Wählen Sie in Designer das Objekt „Identitätsdepot“ in der Registerkarte **Gliederung**.

2 Klicken Sie in der Symbolleiste „Modellierer“ auf das Symbol **Alle Treiber anhalten** .

   Alle im Projekt verwendeten Treiber werden angehalten.

3 Wählen Sie für die Treiber die manuelle Startoption aus, um zu vermeiden, dass die Treiber vor Abschluss der Aufrüstung starten:

   3a Doppelklicken Sie auf das Treibersymbol in der Registerkarte **Gliederung**.

   3b Wählen Sie **Treiberkonfiguration > Startoption**.

   3c Wählen Sie **Manuell** und klicken Sie dann auf **OK**.

   3d Führen Sie Schritt 3a bis Schritt 3c für alle Treiber aus.

Anhalten der Treiber mit der OpenText Identity Console

1 Wählen Sie in der Identity Console den Punkt **OpenText Identity Manager-Verwaltung**.

2 Klicken Sie im **Aktionsmenü** auf das Treibersatzobjekt.

3 Klicken Sie auf **Alle Treiber anhalten**.

4 Führen Sie die Schritte 1 bis 3 für alle Treibersatzobjekte aus.

5 Wählen Sie für die Treiber die manuelle Startoption aus, um zu vermeiden, dass die Treiber vor Abschluss der Aufrüstung starten:

   5a Wählen Sie in der Identity Console den Punkt **OpenText Identity Manager-Verwaltung**.

   5b Klicken Sie auf das Treibersatzobjekt.

5c Klicken Sie in der oberen rechten Ecke des Treibersymbols auf **Aktionsmenü** und wählen Sie **Startoptionen**.

5d Wählen Sie **Manuell** und klicken Sie dann auf **OK**.

5e Führen Sie Schritt 5a auf Seite 190 bis Schritt 5d auf Seite 191 für alle Treiber in Ihrer Baumstruktur aus.

Starten der Treiber

Nach dem Aktualisieren aller OpenText Identity Manager-Komponenten starten Sie die Treiber neu. Wir empfehlen, die gestarteten Treiber nach dem Ausführen zu testen, ob noch alle Richtlinien funktionieren.

- „Starten der Treiber mithilfe von Designer“, auf Seite 191
- „Starten der Treiber mit der OpenText Identity Console“, auf Seite 191

Starten der Treiber mithilfe von Designer

1. Wählen Sie in Designer das Objekt „Identitätsdepot“ in der Registerkarte **Gliederung**.
2. Klicken Sie in der „Modellierer“-Symbolleiste auf das Symbol **Alle Treiber starten** . Alle Treiber im Projekt werden gestartet.
3. Legen Sie die Treiber-Startoptionen fest:
   - **3a** Doppelklicken Sie auf das Treibersymbol in der Registerkarte **Gliederung**.
   - **3b** Wählen Sie **Treiberkonfiguration > Startoption**.
   - **3c** Wählen Sie **Autom. starten** bzw. die gewünschte Methode für den Start des Treibers aus. Klicken Sie anschließend auf **OK**.
   - **3d** Führen Sie Schritt 3a bis Schritt 3c für alle Treiber aus.
4. Testen Sie die Treiber, um sicherzustellen, dass die die Richtlinien wie gewünscht funktionieren. Weitere Informationen zum Testen der Richtlinien finden Sie unter „Testen von Richtlinien mit dem Richtliniensimulator“ im Handbuch *OpenText™ Identity Manager CE 24.4 (v4.10) – Erstellen von Richtlinien mit Designer*.

Starten der Treiber mit der OpenText Identity Console

1. Wählen Sie in der Identity Console den Punkt **OpenText Identity Manager-Übersicht**.
2. Klicken Sie im Treibersatzobjekt auf das **Aktionsmenü**-Symbol .
3. Klicken Sie auf **Alle Treiber starten**.
4. Wenn Sie mehrere Treiber haben, wiederholen Sie die Schritte 1 bis 3 für alle Treibersatzobjekte.
5. Legen Sie die Treiber-Startoptionen fest:
   - **5a** Wählen Sie in der Identity Console den Punkt **OpenText Identity Manager-Verwaltung**.
   - **5b** Klicken Sie auf das Treibersatzobjekt.
   - **5c** Klicken Sie in der oberen rechten Ecke des Treibersymbols auf **Aktionsmenü** und wählen Sie **Startoptionen**.

5d Wählen Sie **Manuell** und klicken Sie dann auf **OK**.

5e Wiederholen Sie Schritt 5a auf Seite 191 und Schritt 5d auf Seite 192 für jeden Treiber.

6 Testen Sie die Treiber, um sicherzustellen, dass die die Richtlinien wie gewünscht funktionieren.

Aufrüsten der OpenText Identity Manager-Treiber

Wir stellen neue Inhalte nicht mehr über Treiberkonfigurationsdateien, sondern über **Pakete** bereit. Die Pakete verwalten und erstellen Sie in Designer. Weitere Informationen zum Verwalten von Paketen finden Sie unter „Erläuterungen zu Paketen“ im *Administrationshandbuch zu Designer für OpenText™ Identity Manager CE 24.4 (v4.10)*.

Sie können die Treiber wie folgt auf Pakete aufrüsten:

- „Einen neuen Treiber erstellen“, auf Seite 192
- „Vorhandene Inhalte durch Inhalte aus Paketen ersetzen“, auf Seite 192
- „Aktuelle Inhalte beibehalten und neue Inhalte über Pakete hinzufügen“, auf Seite 193

WICHTIG: Wenn Ihr Treiber MapDB verwendet, müssen Sie die bestehenden MapDB-Status-Cache-Dateien für den Treiber nach der Aufrüstung des Treibers manuell entfernen. Dies ist erforderlich, weil im Aufrüstungsvorgang der OpenText Identity Manager-Engine nicht alle dieser Dateien gelöscht werden. Weitere Informationen finden Sie unter „Arbeiten mit MapDB 3.0.9“, auf Seite 171.

Einen neuen Treiber erstellen

Die einfachste und sauberste Methode, um Pakete zu Treibern aufzurüsten, besteht darin, den vorhandenen Treiber zu löschen und einen neuen Treiber mithilfe von Paketen zu erstellen. Statten Sie den neuen Treiber mit allen gewünschten Funktionen aus. Die Schritte hierfür sind bei jedem Treiber unterschiedlich. Anweisungen finden Sie in den einzelnen Treiberhandbüchern auf der Website zur OpenText Identity Manager-Treiberdokumentation (https://www.netiq.com/documentation/identity-manager-4.10-drivers/). Der Treiber funktioniert nun wie vorher, seine Inhalte stammen aber aus Paketen und nicht aus einer Treiberkonfigurationsdatei.

Vorhandene Inhalte durch Inhalte aus Paketen ersetzen

Wenn die vom Treiber erstellten Verknüpfungen beibehalten werden müssen, entfällt das Löschen und Neuerstellen des Treibers. Sie können die Verknüpfungen beibehalten und den Treiberinhalt durch Pakete ersetzen.

So ersetzen Sie vorhandene Inhalte durch Inhalte aus Paketen:

1 Erstellen Sie eine Sicherung des Treibers und aller seiner angepassten Inhalte.

Eine Anleitung dazu finden Sie in „Exportieren der Treiberkonfiguration“, auf Seite 166.

2 Löschen Sie in Designer alle im Treiber gespeicherten Objekte. Löschen die Richtlinien, Filter, Berechtigungen und alle anderen im Treiber gespeicherten Elemente.

HINWEIS: Designer bietet eine Funktion zum automatischen Importieren der aktuellen Pakete. Sie müssen die Treiberpakete nicht manuell in den Treiberkatalog importieren.

Weitere Informationen finden Sie unter „Importieren von Paketen in den Paketkatalog“ im *Administrationshandbuch zu Designer OpenText™ Identity Manager CE 24.4 (v4.10)*.

3 Installieren Sie die aktuellen Pakete im Treiber.

Diese Schritte sind bei jedem Treiber unterschiedlich. Anweisungen finden Sie im jeweiligen Treiberhandbuch auf der Website zur OpenText Identity Manager-Treiberdokumentation (https://www.netiq.com/documentation/identity-manager-4.10-drivers/).

4 Stellen Sie alle benutzerdefinierten Richtlinien und Regeln für den Treiber wieder her. Eine Anleitung dazu finden Sie in „Wiederherstellen der benutzerdefinierten Richtlinien und Regeln für den Treiber“, auf Seite 195.

Aktuelle Inhalte beibehalten und neue Inhalte über Pakete hinzufügen

Sie können den Treiber im aktuellen Zustand belassen und mithilfe der Pakete um neue Funktionen erweitern, solange keine Überschneidung zwischen den Funktionen in den Paketen und den aktuellen Funktionen des Treibers besteht.

Bevor Sie ein Paket erstellen, legen Sie eine Sicherungskopie der Treiberkonfigurationsdatei an. Wenn Sie ein Paket installieren, werden unter Umständen vorhandene Richtlinien überschrieben, sodass der Treiber nicht mehr funktioniert. Wenn eine Richtlinie überschrieben wird, können Sie die gesicherte Konfigurationsdatei des Treibers importieren und die Richtlinie wiederherstellen.

Stellen Sie zunächst sicher, dass die Namen der benutzerdefinierten Richtlinien nicht mit denen der Standardrichtlinien übereinstimmen. Wenn eine Treiberkonfiguration mit einer neuen Treiberdatei überlagert wird, werden die vorhandenen Richtlinien jeweils überschrieben. Benutzerdefinierte Richtlinien ohne eindeutigen Namen werden verworfen.

So fügen Sie mithilfe von Paketen neue Inhalte zum Treiber hinzu:

1 Erstellen Sie eine Sicherung des Treibers und aller seiner angepassten Inhalte.

Eine Anleitung dazu finden Sie in „Exportieren der Treiberkonfiguration“, auf Seite 166.

HINWEIS: Designer bietet eine Funktion zum automatischen Importieren der aktuellen Pakete. Sie müssen die Treiberpakete nicht manuell in den Treiberkatalog importieren.

Weitere Informationen finden Sie unter „Importieren von Paketen in den Paketkatalog“ im *Administrationshandbuch zu Designer OpenText™ Identity Manager CE 24.4 (v4.10)*.

2 Installieren Sie die Pakete im Treiber.

Anweisungen finden Sie im jeweiligen Treiberhandbuch auf der Website zur OpenText Identity Manager-Treiberdokumentation (https://www.netiq.com/documentation/identity-manager-4.10-drivers/).

3 Fügen Sie die gewünschten Pakete zum Treiber hinzu. Diese Schritte sind bei jedem Treiber unterschiedlich.

Weitere Informationen finden Sie auf der Website der OpenText Identity Manager-Treiberdokumentation (https://www.netiq.com/documentation/identity-manager-4.10-drivers/).

Der Treiber enthält nun die über die Pakete hinzugefügten neuen Funktionen.

Hinzufügen von neuen Servern zum Treibersatz

Beim Aufrüsten oder Migrieren von OpenText Identity Manager auf neue Server müssen Sie die Treibersatzinformationen aktualisieren. In diesem Abschnitt werden die anfallenden Schritte beschrieben. Sie können den Treibersatz wahlweise mit Designer oder mit der OpenText Identity Console aktualisieren.

Hinzufügen des neuen Servers zum Treibersatz

Wenn Sie die OpenText Identity Console verwenden, müssen Sie den neuen Server zum Treibersatz hinzufügen. Designer enthält einen Migrationsassistenten für den Server, der diesen Schritt für Sie durchführt. Wenn Sie Designer verwenden, fahren Sie mit „Kopieren der serverspezifischen Informationen in Designer“, auf Seite 207 fort. Wenn Sie die OpenText Identity Console verwenden, führen Sie die folgenden Schritte aus:

1. Klicken Sie in der OpenText Identity Console auf **IDM-Verwaltung**.
2. Wählen Sie den Treibersatz aus.
3. Klicken Sie auf .
4. Klicken Sie auf **Server hinzufügen**.
5. Suchen Sie den neuen OpenText Identity Manager -Server, wählen Sie ihn aus, und klicken Sie anschließend auf **OK**.

Entfernen des alten Servers aus dem Treibersatz

Sobald auf dem neuen Server alle Treiber ausgeführt werden, können Sie den bisherigen Server aus dem Treibersatz entfernen.

- „Mithilfe von Designer den alten Server aus dem Treibersatz entfernen“, auf Seite 194
- „Entfernen des alten Servers aus dem Treibersatz mit der OpenText Identity Console“, auf Seite 195
- „Stilllegen des alten Servers“, auf Seite 195

Mithilfe von Designer den alten Server aus dem Treibersatz entfernen

1. Öffnen Sie Ihr Projekt in Designer.
2. Klicken Sie im Modellierer mit der rechten Maustaste auf den Treibersatz und wählen Sie anschließend **Eigenschaften**.
3. Wählen Sie **Serverliste**.
4. Wählen Sie den bisherigen OpenText Identity Manager-Server in der Liste **Server auswählen** aus, und klicken Sie auf **<**. Der Server wird aus der Liste **Server auswählen** entfernt.
5. Klicken Sie zum Speichern der Änderungen auf **OK**.

6 Stellen Sie die Änderung im Identitätsdepot bereit.

Weitere Informationen finden Sie unter „Bereitstellen eines Treibersatzes in einem Identitätsdepot“ im *Administrationshandbuch zu Designer für OpenText™ Identity Manager CE 24.4 (v4.10)*.

Entfernen des alten Servers aus dem Treibersatz mit der OpenText Identity Console

1 Klicken Sie in der OpenText Identity Console auf **IDM-Verwaltung**.

2 Wählen Sie den Treibersatz aus.

3 Klicken Sie auf .

4 Klicken Sie auf **Server entfernen**.

5 Suchen Sie den neuen OpenText Identity Manager -Server, wählen Sie ihn aus, und klicken Sie anschließend auf **OK**.

Stilllegen des alten Servers

Zu diesem Zeitpunkt hostet der alte Server keine Treiber mehr. Wenn Sie diesen Server nicht mehr benötigen, müssen Sie zusätzliche Schritte durchführen, um ihn stillzulegen:

1 Entfernen Sie die OpenText eDirectory-Reproduktionen von diesem Server.

Weitere Informationen finden Sie unter Löschen einer Reproduktion im NetIQ eDirectory-Administrationshandbuch.

2 Entfernen Sie OpenText eDirectory von diesem Server.

Weitere Informationen finden Sie im Artikel TID 10056593, "Dauerhaftes Entfernen eines Servers aus einem NDS-Baum" (https://support.microfocus.com/kb/doc.php?id=10056593) (Sie müssen sich möglicherweise anmelden).

Wiederherstellen der benutzerdefinierten Richtlinien und Regeln für den Treiber

Nach dem Installieren neuer Pakete für die Treiber bzw. nach dem Aufrüsten auf diese neuen Pakete müssen Sie zunächst die Überlagerung mit der neuen Treiberkonfigurationsdatei vornehmen und dann die benutzerdefinierten Richtlinien oder Regeln (soweit vorhanden) für den Treiber wiederherstellen. Wenn diese Richtlinien andere Namen haben, sind sie noch im Treiber gespeichert, aber die Links sind kaputt und müssen erneuert werden.

- „Wiederherstellen benutzerdefinierter Richtlinien und Regeln für den Treiber mithilfe von Designer“, auf Seite 196
- „Wiederherstellen benutzerdefinierter Richtlinien und Regeln für den Treiber mit der OpenText Identity Console“, auf Seite 196

Wiederherstellen benutzerdefinierter Richtlinien und Regeln für den Treiber mithilfe von Designer

Sie können Richtlinien zum Richtliniensatz hinzufügen. Diese Schritte sollten Sie zunächst in einer Testumgebung durchführen, bevor Sie den aktualisierten Treiber in Ihre Produktionsumgebung verschieben.

1. Wählen Sie in der **Gliederungsansicht** den aufgerüsteten Treiber aus, und klicken Sie anschließend auf das Symbol **Richtlinienfluss anzeigen** .
2. Klicken Sie mit der rechten Maustaste auf den Richtliniensatz, dessen benutzerdefinierte Richtlinie Sie wiederherstellen möchten, und wählen Sie anschließend **Richtlinie hinzufügen > Vorhandene kopieren**.
3. Wechseln Sie zur benutzerdefinierten Richtlinie und markieren Sie sie. Klicken Sie anschließend auf **OK**.
4. Geben Sie den Namen für die neue benutzerdefinierte Richtlinie an und klicken Sie dann auf **OK**.
5. Klicken Sie zum Speichern des Projekts in der Dateikonfliktmeldung auf **Ja**.
6. Wenn der Richtlinien-Builder die Richtlinie geöffnet hat, stellen Sie sicher, dass die Informationen in der kopierten Richtlinie richtig sind.
7. Wiederholen Sie Schritt 2 bis Schritt 6 für alle benutzerdefinierten Richtlinien, die für den Treiber wiederhergestellt werden sollen.
8. Starten Sie den Treiber und testen Sie ihn.

   Weitere Informationen zum Starten des Treibers finden Sie unter Stoppen, Starten oder Neustarten eines Treibers in Designer im *Verwaltungshandbuch für OpenText™ Identity Manager CE 24.4 (v4.10)-Treiber*. Weitere Informationen zum Testen des Treibers finden Sie unter „Testen von Richtlinien mit dem Richtliniensimulator“ im Handbuch *OpenText™ Identity Manager CE 24.4 (v4.10) – Erstellen von Richtlinien mit Designer*.
9. Wenn Sie überprüft haben, dass die Richtlinien funktionieren, können Sie den Treiber in der Produktionsumgebung einsetzen.

Wiederherstellen benutzerdefinierter Richtlinien und Regeln für den Treiber mit der OpenText Identity Console

Führen Sie diese Schritte in einer Testumgebung durch, bevor Sie den aktualisierten Treiber in Ihre Produktionsumgebung verschieben.

1. Gehen Sie in der Identity Console zu **OpenText Identity Manager-Verwaltung**.
2. Klicken Sie auf das Treibersatzobjekt, das den aufgerüsteten Treiber enthält.
3. Klicken Sie auf das Treibersymbol.
4. Gehen Sie zu **Datenumwandlung und -synchronisierung > Richtlinien** und wählen Sie dann den Richtliniensatz aus, in dem Sie die angepasste Richtlinie wiederherstellen möchten.
5. Klicken Sie auf **Richtlinie einfügen**.
6. Suchen Sie im Popupfenster **Vorhandene Richtlinie verwenden** die benutzerdefinierte Richtlinie und wählen Sie sie aus.
7. Klicken Sie auf **Speichern**.

8 Wiederholen Sie Schritt 2 bis Schritt 7 für alle benutzerdefinierten Richtlinien, die für den Treiber wiederhergestellt werden sollen.

9 Starten Sie den Treiber und testen Sie ihn.

Weitere Informationen zum Starten des Treibers finden Sie unter Stoppen, Starten oder Neustarten eines Treibers in Designer im *Verwaltungshandbuch für OpenText™ Identity Manager CE 24.4 (v4.10)-Treiber*. In der OpenText Identity Console gibt es keinen Richtliniensimulator. Lösen Sie zum Testen der Richtlinien Ereignisse aus, durch die die Richtlinien ausgeführt werden. Sie können z. B. einen Benutzer erstellen, ändern oder löschen.

10 Wenn Sie überprüft haben, dass die Richtlinien funktionieren, können Sie den Treiber in der Produktionsumgebung einsetzen.

17 Wechseln von der Advanced Edition zur Standard Edition

Sie sollten nur dann auf die Standard Edition umstellen, wenn Sie keinerlei Funktionen der Advanced Edition für Ihre Umgebung wünschen und die Bereitstellung von OpenText Identity Manager einschränken möchten.

1. (Bedingt) Falls Sie die Advanced Edition bereits aktiviert haben, heben Sie die Aktivierung wieder auf.
2. (Bedingt) Wechseln Sie mit den folgenden Schritten zum Standard Edition-Testmodus:
   - **2a** Navigieren Sie zum Identitätsdepotverzeichnis `dib` unter `C:\Novell\NDS\DIBFiles`.
   - **2b** Erstellen Sie eine neue Datei, geben Sie den Namen `.idme` ein und tragen Sie die Zahl 2 in die Datei ein.
   - **2c** Starten Sie OpenText eDirectory neu.
   - **2d** Fahren Sie mit Schritt 4 fort.
3. (Bedingt) Falls Sie bereits eine Standard Edition-Aktivierung erworben haben, aktivieren Sie die Edition.
4. Halten Sie Tomcat an.
5. Löschen Sie folgende WAR-Dateien und Webapps-Ordner aus dem Verzeichnis `C:\NetIQ\idm\apps\tomcat\webapps`:
   - `IDMProv*`
   - `IDMRPT*`
   - `dash*`
   - `idmdash*`
   - `landing*`
   - `rra*`
   - `rptdoc*`
6. Verschieben Sie die folgenden vorhandenen Ordner in ein Sicherungsverzeichnis:
   - `IDMReporting`
   - `UserApplication`
7. Kopieren Sie die Datei `ism-configuration.properties` aus dem Verzeichnis `C:\NetIQ\IDM\apps\tomcat\conf` in ein Sicherungsverzeichnis.
8. Installieren Sie Identity Reporting von der ISO-Datei für OpenText Identity Manager 4.10.
9. Starten Sie `configupdate.bat` im Verzeichnis *<Berichterstellungs-Installationsordner>*`/bin` und geben Sie Werte für die folgenden Parameter an:

   Registerkarte „Berichterstellung“: Geben Sie die Einstellungen in den folgenden Abschnitten an:

   - Identitätsdepot

- Identitätsdepot-Benutzeridentität
- Berichtadministratoren
  - **Container-DN der Berichtsadministratorrolle**. Beispiel: `ou=sa,o=data`
  - **Berichtadministratoren**. Beispiel: `cn=uaadmin,ou=sa,o=data`

Registerkarte „Authentifizierung“: Geben Sie die Einstellungen in den folgenden Abschnitten an:

- Beglaubigungsserver
  - **Hostkennung für OAuth-Server**. Beispiel: IP-Adresse oder DNS-Name des Authentifizierungsservers, z. B. `192.99.17.22`
  - **TCP-Port für OAuth-Server**
  - **OAuth-Server verwendet TLS/SSL**
- Authentifizierungskonfiguration
  - **OAuth-Keystore-Datei**. Beispiel: `C:\NetIQ\idm\apps\osp\osp.jks`
  - **Schlüsselalias für Schlüssel für OAuth**
  - **Schlüsselpasswort für Schlüssel für OAuth**
  - **Sitzungszeitüberschreitung (Minuten)**. Beispiel: 60 Minuten.

Registerkarte „SSO-Clients“: Geben Sie die Einstellungen in den folgenden Abschnitten an:

- Berichte
  - **URL-Link zur Portalseite**. Beispiel: `http://192.168.0.1:8180/IDMRPT`
- Zurücksetzen von Passwörtern per Selbstbedienung
  - **OAuth-Client-ID**. Beispiel: *sspr*
  - OAuth-Client-Geheimnis. Beispiel: *<SSPR-Client-Geheimnis>*
  - **OSP-OAuth-Umleitungs-URL**. Beispiel: `http://192.168.0.2:8180/sspr/public/oauth`

Weitere Informationen zum Konfigurationsprogramm finden Sie in „Ausführen des Konfigurationsprogramms der Identity Applications“, auf Seite 74.

10 Speichern Sie die Änderungen und schließen Sie das Konfigurationsprogramm.

11 Starten Sie Tomcat.

VIII Migrieren der OpenText Identity Manager-Daten in eine neue Installation

In diesem Abschnitt wird die Migration vorhandener Daten aus den OpenText Identity Manager-Komponenten in eine neue Installation beschrieben. Der Großteil der Migrationsaufgaben befasst sich mit Identity Applications. Anweisungen zum Aufrüsten der OpenText Identity Manager-Komponenten finden Sie unter Teil VII, „Aufrüsten von OpenText Identity Manager“, auf Seite 155. Weitere Informationen zum Unterschied zwischen Aufrüstung und Migration finden Sie in „Erläuterungen zur Aufrüstung und zur Migration“, auf Seite 159.

18 Vorbereiten der Migration von OpenText Identity Manager

In diesem Abschnitt wird die Vorbereitung Ihrer OpenText Identity Manager-Lösung auf die Migration in die neue Installation beschrieben.

Checkliste für die Migration

Wir empfehlen, die Schritte in der nachfolgenden Checkliste für die Migration auszuführen.

	Checkliste
❑	1. Stellen Sie sicher, dass das aktuelle Installations-Kit für die Migration der OpenText Identity Manager-Daten vorliegt.
❑	2. Stellen Sie sicher, dass die Computer die Hardware- und Software-Anforderungen für eine höhere Version von OpenText Identity Manager erfüllen.
❑	3. Rüsten Sie das Identitätsdepot auf die neueste unterstützte Version auf.
❑	4. Fügen Sie dem neuen Server die OpenText eDirectory-Reproduktionen hinzu, die sich auf dem aktuellen OpenText Identity Manager-Server befinden. Weitere Informationen finden Sie unter Abschnitt 19, „Migrieren von OpenText Identity Manager auf einen neuen Server“, auf Seite 205.
❑	5. Installieren Sie OpenText Identity Manager auf dem neuen Server. Weitere Informationen finden Sie unter „Planen der Installation von OpenText Identity Manager“, auf Seite 35.
❑	6. (Bedingt) Wenn der Treibersatz einen Remote Loader-Treiber enthält, rüsten Sie den Remote Loader-Server für jeden Treiber auf. Weitere Informationen finden Sie unter „Aufrüstung von Remote Loader“, auf Seite 172.
❑	7. (Bedingt) Wenn die Benutzeranwendung auf dem bisherigen Server ausgeführt wird, aktualisieren Sie diese Komponente und die zugehörigen Treiber. Weitere Informationen finden Sie unter „Checkliste für die Migration von OpenText Identity Manager“, auf Seite 205.
❑	8. Fügen Sie den neuen Server zum Treibersatz hinzu. Weitere Informationen finden Sie unter „Hinzufügen des neuen Servers zum Treibersatz“, auf Seite 194.
❑	9. Ändern Sie die serverspezifischen Informationen für jeden Treiber. Weitere Informationen finden Sie unter „Kopieren der serverspezifischen Informationen in Designer“, auf Seite 207.
❑	10. (Bedingt) Wenn Sie RBPM verwenden, aktualisieren Sie die serverspezifischen Informationen des bisherigen Servers auf den neuen Server für die Benutzeranwendung. Weitere Informationen finden Sie in „Kopieren von serverspezifischen Informationen für den Treibersatz“, auf Seite 207

	Checkliste
❑	11. Aktualisieren Sie die Treiber auf das Paketformat. Weitere Informationen finden Sie unter „Aufrüsten der OpenText Identity Manager-Treiber“, auf Seite 192.
❑	12. (Bedingt) Wenn Sie benutzerdefinierte Richtlinien und Regeln verwenden, stellen Sie die angepassten Einstellungen wieder her. Weitere Informationen finden Sie unter „Wiederherstellen der benutzerdefinierten Richtlinien und Regeln für den Treiber“, auf Seite 195.
❑	13. Entfernen Sie den alten Server aus dem Treibersatz. Weitere Informationen finden Sie unter „Entfernen des alten Servers aus dem Treibersatz“, auf Seite 194.
❑	14. Aktivieren Sie die aufgerüstete OpenText Identity Manager-Lösung. Weitere Informationen finden Sie unter „OpenText Identity Manager aktivieren“, auf Seite 119.

19 Migrieren von OpenText Identity Manager auf einen neuen Server

In diesem Abschnitt wird die Migration von der Benutzeranwendung auf Identity Applications auf dem neuen Server beschrieben. Eine Migration kann außerdem dann anfallen, wenn Sie eine vorhandene Installation nicht aufrüsten können. Dieser Abschnitt enthält die nachfolgenden Verfahren:

- „Checkliste für die Migration von OpenText Identity Manager“, auf Seite 205
- „Vorbereiten des Designer-Projekts auf die Migration“, auf Seite 206
- „Kopieren von serverspezifischen Informationen für den Treibersatz“, auf Seite 207
- „Migrieren der OpenText Identity Manager-Engine auf einen neuen Server“, auf Seite 209
- „Migrieren des Benutzeranwendungstreibers“, auf Seite 209
- „Aufrüsten der Identity Applications“, auf Seite 211
- „Migrieren von Identity Applications“, auf Seite 211
- „Abschließen der Migration der Identity Applications“, auf Seite 213

Checkliste für die Migration von OpenText Identity Manager

Wir empfehlen, die Schritte in der nachfolgenden Checkliste auszuführen.

	Checkliste
❑	1. Sichern Sie die Verzeichnisse und Datenbanken in Ihrer OpenText Identity Manager-Lösung.
❑	2. Stellen Sie sicher, dass jeweils die aktuelle Version der OpenText Identity Manager-Komponenten installiert ist (außer Identity Applications). **HINWEIS:** Soll die aktuelle Datenbank der Benutzeranwendung weiterhin genutzt werden, wählen Sie im Installationsprogramm die Option **Vorhandene Datenbank.**
❑	3. Führen Sie eine Zustandsüberprüfung des Identitätsdepots aus, damit gewährleistet ist, dass das Schema ordnungsgemäß erweitert wird. Verwenden Sie TID 3564075 zum Durchführen der Zustandsüberprüfung.
❑	4. Importieren Sie die vorhandenen Benutzeranwendungstreiber in Designer.
❑	5. Archivieren Sie das Designer-Projekt. Hiermit wird der Zustand des Treibers vor der Migration festgehalten. Weitere Informationen finden Sie unter „Vorbereiten des Designer-Projekts auf die Migration“, auf Seite 206.

	Checkliste
❑	6. (Bedingt) Soll die OpenText Identity Manager-Engine auf einen neuen Server migriert werden, kopieren Sie die OpenText eDirectory-Reproduktionen auf den neuen Server. Weitere Informationen finden Sie unter „Migrieren der OpenText Identity Manager-Engine auf einen neuen Server“, auf Seite 209.
❑	7. Erstellen Sie zur Vorbereitung der Migration ein neues Designer-Projekt mit der aktuellen Version von Designer, und importieren Sie den Benutzeranwendungstreiber.
❑	8. Migrieren Sie den Benutzeranwendungstreiber. Weitere Informationen finden Sie unter „Migrieren des Benutzeranwendungstreibers“, auf Seite 209.
❑	9. Stellen Sie die beiden Treiber im Identitätsdepot bereit.
❑	10. Rüsten Sie Identity Applications auf. Weitere Informationen finden Sie unter „Aufrüsten von Identity Applications“, auf Seite 175.
❑	11. Stellen Sie sicher, dass die Browser keine Inhalte aus früheren Versionen von OpenText Identity Manager enthalten. Weitere Informationen finden Sie unter „Leeren des Browsercache“, auf Seite 214.
❑	12. (Bedingt) Stellen Sie Ihre benutzerdefinierten Einstellungen für das SharedPagePortlet wieder her. Weitere Informationen finden Sie unter „Aktualisieren der Einstellung für die maximale Zeitüberschreitung für das SharedPagePortlet“, auf Seite 215.
❑	13. Stellen Sie sicher, dass mit der Suchoption für Gruppen erst dann Informationen angezeigt werden, wenn der Benutzer Filterparameter festlegt. Weitere Informationen finden Sie unter „Deaktivieren der Einstellung für automatische Abfragen für Gruppen“, auf Seite 215.

Vorbereiten des Designer-Projekts auf die Migration

Bevor Sie den Treiber migrieren, müssen Sie das Designer-Projekt mit einigen Schritten auf die Migration vorbereiten.

HINWEIS: Wenn kein zu migrierendes Designer-Projekt vorliegt, erstellen Sie ein neues Projekt mit **Datei > Importieren > Projekt (aus Identitätsdepot)**.

1. Starten Sie Designer.
2. (Bedingt) Wenn ein Designer-Projekt vorhanden ist, das die zu migrierende Benutzeranwendung enthält, sichern Sie das Projekt:
   - **2a** Klicken Sie in der Projektansicht mit der rechten Maustaste auf das Projekt, und wählen Sie **Projekt kopieren**.
   - **2b** Geben Sie einen Namen für das Projekt an, und klicken Sie auf **OK**.
3. Aktualisieren Sie das Schema für das vorhandene Projekt mit den folgenden Schritten:
   - **3a** Wählen Sie in der Modellierer-Ansicht das Identitätsdepot aus.
   - **3b** Wählen Sie **Live > Schema > Importieren**.

4 (Optional) Überprüfen Sie mit den folgenden Schritten, ob das Projekt die richtige Versionsnummer für OpenText Identity Manager enthält:

4a Wählen Sie in der Modellierer-Ansicht das Identitätsdepot aus, und klicken Sie auf **Eigenschaften**.

4b Wählen Sie im linken Navigationsmenü den Eintrag **Serverliste**.

4c Wählen Sie einen Server aus, und klicken Sie auf **Bearbeiten**.

Im Feld **Identity Manager-Version** sollte die aktuelle Version angezeigt werden.

Kopieren von serverspezifischen Informationen für den Treibersatz

Sie müssen alle serverspezifischen Informationen, die in den einzelnen Treibern und Treibersätzen gespeichert sind, in die Informationen des neuen Servers kopieren. Hierzu gehören auch Globalkonfigurationswerte und andere Daten im Treibersatz, die auf dem neuen Server nicht vorhanden sind und daher kopiert werden müssen. Die serverspezifischen Informationen sind enthalten in:

- Globalkonfigurationswerte
- Engine-Steuerungswerte
- Benannte Passwörter
- Treiberauthentifizierungsinformationen
- Treiber-Startoptionen
- Treiberparameter
- Treibersatz-Daten

Dies erfolgt in Designer oder in der OpenText Identity Console. Wenn Sie Designer verwenden, ist es ein automatisierter Prozess. Wenn Sie die OpenText Identity Console verwenden, ist es ein manueller Prozess. Die Migration eines OpenText Identity Manager-Servers vor Version 3.5 auf einen OpenText Identity Manager-Server mit Version 3.5 oder höher sollten Sie mit der OpenText Identity Console vornehmen. Bei allen anderen unterstützten Migrationspfaden können Sie Designer verwenden.

- „Kopieren der serverspezifischen Informationen in Designer“, auf Seite 207
- „Ändern der serverspezifischen Informationen in der OpenText Identity Console“, auf Seite 208
- „Ändern der serverspezifischen Informationen für die Benutzeranwendung“, auf Seite 209

Kopieren der serverspezifischen Informationen in Designer

Dieses Verfahren betrifft alle Treiber, die im Treibersatz gespeichert sind.

1 Öffnen Sie Ihr Projekt in Designer.

2 Klicken Sie in der Registerkarte **Gliederung** mit der rechten Maustaste auf den Server und wählen Sie anschließend **Migrieren**.

3 Lesen Sie den Überblick, damit Sie sehen, welche Elemente auf den neuen Server migriert werden, und klicken Sie anschließend auf **Weiter**.

4 Wählen Sie den Zielserver aus der Liste der verfügbaren Server aus, und klicken Sie anschließend auf **Weiter**.

   Es werden nur die Server aufgelistet, die momentan nicht mit einem Treibersatz verknüpft sind und deren Version gleich der oder neuer als die Version des OpenText Identity Manager-Ursprungsservers ist.

5 Wählen Sie eine der folgenden Optionen aus:

   - **Zielserver aktiv machen:** Kopiert die Einstellungen vom Ursprungsserver auf den Zielserver und deaktiviert die Treiber auf dem Ursprungsserver. Die Verwendung dieser Option wird empfohlen.
   - **Ursprungsserver aktiv lassen:** Kopiert die Einstellungen nicht und deaktiviert alle Treiber auf dem Zielserver.
   - **Ziel- und Ursprungsserver aktiv machen:** Kopiert die Einstellungen vom Ursprungsserver auf den Zielserver, ohne die Treiber auf dem Ursprungs- oder Zielserver zu deaktivieren. Diese Option wird nicht empfohlen. Wenn beide Treiber gestartet werden, werden die gleichen Informationen in zwei verschiedene Warteschlangen geschrieben, was zu Beschädigungen führen kann.

6 Klicken Sie auf **Migrieren**.

7 Stellen Sie die geänderten Treiber im Identitätsdepot bereit.

   Weitere Informationen finden Sie unter „Bereitstellen eines Treibers in einem Identitätsdepot“ im *Administrationshandbuch zu Designer für OpenText™ Identity Manager CE 24.4 (v4.10)*.

8 Starten Sie die Treiber.

   Weitere Informationen finden Sie unter Stoppen, Starten oder Neustarten eines Treibers in Designer im *Verwaltungshandbuch für OpenText™ Identity Manager CE 24.4 (v4.10)-Treiber*.

Ändern der serverspezifischen Informationen in der OpenText Identity Console

1 Gehen Sie in der Identity Console zu **OpenText Identity Manager-Verwaltung**.

2 Klicken Sie auf das Treibersatzobjekt, das die erforderlichen Treiber enthält.

3 Klicken Sie im Aktionsmenü auf das Symbol und dann auf **Treiber anhalten**.

4 Klicken Sie auf das Treibersymbol.

5 Gehen Sie zu **Konfiguration**. Tabulator.

6 Kopieren oder migrieren Sie alle serverspezifischen Treiberparameter, Globalkonfigurationswerte, Engine-Steuerungswerte, benannten Passwörter, Treiberauthentifizierungsdaten und Treiber-Startoptionen, die die Informationen des alten Servers enthalten, in die Informationen des neuen Servers. Globalkonfigurationswerte und andere Parameter des Treibersatzes, z. B. die max. Heap-Größe, die Java-Einstellungen usw., müssen mit den Werten des alten Servers übereinstimmen.

7 Klicken Sie auf **Speichern**, um alle Änderungen zu speichern und die Seite zu verlassen.

8 Klicken Sie auf das Aktionsmenü und dann auf **Treiber starten**.

9 Wiederholen Sie Schritt 3 bis Schritt 8 auf Seite 208 für jeden Treiber im Treibersatz.

Ändern der serverspezifischen Informationen für die Benutzeranwendung

Sie müssen die Benutzeranwendung neu konfigurieren, damit der neue Server erkannt wird. Führen Sie `configupdate.bat` aus.

1. Navigieren Sie zum Konfigurationsprogramm für die Aktualisierung (standardmäßig im Installationsunterverzeichnis der Benutzeranwendung).
2. Starten Sie das Konfigurations-Aktualisierungsprogramm (`configupdate.bat`) über die Befehlszeile.
3. Geben Sie die Werte aus „Konfigurieren der Einstellungen für Identity Applications“, auf Seite 74 an.

Migrieren der OpenText Identity Manager-Engine auf einen neuen Server

Wenn Sie die OpenText Identity Manager-Engine auf einen neuen Server migrieren, können Sie die OpenText eDirectory-Reproduktionen beibehalten, die derzeit auf dem bisherigen OpenText Identity Manager-Server verwendet werden.

1. Installieren Sie eine unterstützte Version von OpenText eDirectory auf dem neuen Server.
2. Kopieren Sie die OpenText eDirectory-Reproduktionen, die sich auf dem aktuellen OpenText Identity Manager-Server befinden, auf den neuen Server.

   Weitere Informationen finden Sie unter „Administering Replicas“ (https://www.netiq.com/documentation/edirectory-93/edir_admin/data/fbgciaad.html) (Verwalten von Reproduktionen) im *OpenText eDirectory-Administrationshandbuch* (https://www.netiq.com/documentation/edirectory-93/).
3. Installieren Sie die OpenText Identity Manager-Engine auf dem neuen Server.

Migrieren des Benutzeranwendungstreibers

Beim Aufrüsten auf eine neue Version von OpenText Identity Manager oder beim Migrieren auf einen anderen Server müssen Sie unter Umständen ein neues Basispaket für den Benutzeranwendungstreiber importieren oder das vorhandene Paket aufrüsten. Beispiel: **Benutzeranwendungsbasis-Version 2.2.0.20120516011608**.

Wenn Sie die Arbeit an einem neuen OpenText Identity Manager-Projekt beginnen, fordert Designer Sie automatisch dazu auf, neue Pakete in das Projekt zu importieren. Zu diesem Zeitpunkt können Sie das Paket auch manuell importieren.

Importieren eines neuen Basispakets

1. Öffnen Sie Ihr Projekt in Designer.
2. Klicken Sie mit der rechten Maustaste auf **Paketkatalog > Paket importieren**, und wählen Sie das entsprechende Paket aus.

3 (Bedingt)·Wenn·das·Benutzeranwendungs-Basispaket·nicht·im·Dialogfeld·„Paket importieren“ aufgeführt wird, führen Sie die folgenden Schritte aus:

   3a Klicken Sie auf die Schaltfläche „Durchsuchen“.

   3b Navigieren Sie zu *designer_root*/packages/eclipse/plugins/NOVLUABASE_*Version_des_aktuellen_Pakets*.jar.

   3c Klicken Sie auf **OK**.

4 Klicken Sie auf **OK**.

Aufrüsten eines vorhandenen Basispakets

1 Öffnen Sie Ihr Projekt in Designer.

2 Klicken Sie mit der rechten Maustaste auf den Benutzeranwendungstreiber.

3 Klicken Sie auf **Treiber > Eigenschaften > Pakete**.

   Wenn das Basispaket aufgerüstet werden kann, wird in der Spalte **Upgrades** ein Häkchen angezeigt.

4 Klicken Sie für das Paket, für das ein Upgrade verfügbar ist, auf **Operation auswählen**.

5 Klicken Sie in der Dropdown-Liste auf **Upgrade**.

6 Wählen Sie die aufzurüstende Version aus. Klicken Sie anschließend auf **OK**.

7 Klicken Sie auf **Anwenden**.

8 Tragen Sie die erforderlichen Angaben zum Aufrüsten des Pakets in die Felder ein. Klicken Sie anschließend auf **Weiter**.

9 Lesen Sie die Installationsübersicht. Klicken Sie anschließend auf **Fertig stellen**.

10 Schließen Sie die Seite „Paketverwaltung“.

11 Deaktivieren Sie die Option **Nur zutreffende Paketversionen anzeigen**.

Bereitstellen des migrierten Treibers

Die Treibermigration ist erst dann abgeschlossen, wenn Sie den Benutzeranwendungstreiber im Identitätsdepot bereitstellen. Nach der Migration befindet sich das Projekt in einem Zustand, in dem nur die gesamte migrierte Konfiguration bereitgestellt werden kann. Es ist nicht möglich, Definitionen in die migrierte Konfiguration zu importieren. Sobald die gesamte Migrationskonfiguration bereitgestellt wurde, wird diese Einschränkung wieder aufgehoben, und Sie können wie gewohnt einzelne Objekte bereitstellen und Definitionen importieren.

1 Öffnen Sie das Projekt in Designer, und führen Sie die Projektprüfung für die migrierten Objekte aus.

   Weitere Informationen hierzu finden Sie unter „Validieren der Bereitstellungsobjekte“ im *OpenText™ Identity Manager CE 24.4 (v4.10) – Administratorhandbuch zur Entwicklung von Identity Applications*. Falls Validierungsfehler in der Konfiguration festgestellt werden, so werden Sie über die Fehler informiert. Diese Fehler müssen behoben werden, bevor Sie den Treiber bereitstellen können.

2 Klicken Sie in der Ansicht **Gliederung** mit der rechten Maustaste auf den Benutzeranwendungstreiber.

3 Wählen Sie **Bereitstellen**.

4 Wiederholen Sie diesen Vorgang für alle Benutzeranwendungstreiber im Treibersatz.

Aufrüsten der Identity Applications

Wenn Sie das Aufrüstungsprogramm für Identity Applications ausführen, beachten Sie die folgenden Überlegungen:

- Verwenden Sie dieselbe Datenbank wie für die bisherige Benutzeranwendung. (Dies ist die Installation, von der aus Sie die Migration vornehmen.) Wählen Sie im Installationsprogramm als Datenbanktyp die Option **Vorhandene Datenbank**.
- Sie können einen anderen Namen für den Kontext für die Benutzeranwendung angeben.
- Legen Sie einen Installationsspeicherort fest, der nicht mit dem Speicherort der bisherigen Installation übereinstimmt.
- Verweisen Sie auf eine unterstützte Tomcat-Version.
- Verwenden Sie für Ihre Datenbank keine Sortierung, bei der zwischen Groß- und Kleinschreibung unterschieden wird. Die Sortierung, bei der zwischen Groß- und Kleinschreibung unterschieden wird, wird nicht unterstützt. Die Sortierung, bei der nicht zwischen Groß- und Kleinschreibung unterschieden wird, könnte bei der Migration Fehler aufgrund doppelter Schlüssel verursachen. Wenn ein Fehler durch doppelte Schlüssel auftritt, müssen Sie die Sortierung überprüfen und korrigieren. Installieren Sie anschließend Identity Applications erneut. Die einzige unterstützte Sortierung ist SQL_Latin1_General_CP1_CI_AS.

Weitere Informationen zum Aufrüsten der Identity Applications finden Sie in „Aufrüsten von Identity Applications“, auf Seite 175.

Migrieren von Identity Applications

Verwenden Sie für Ihre Datenbank keine Sortierung, bei der zwischen Groß- und Kleinschreibung unterschieden wird. Die Sortierung, bei der zwischen Groß- und Kleinschreibung unterschieden wird, wird nicht unterstützt. Die Sortierung, bei der zwischen Groß- und Kleinschreibung unterschieden wird, könnte bei der Migration Fehler aufgrund doppelter Schlüssel verursachen. Wenn ein Fehler durch doppelte Schlüssel auftritt, müssen Sie die Sortierung überprüfen und korrigieren. Installieren Sie anschließend Identity Applications erneut. Die einzige unterstützte Sortierung ist SQL_Latin1_General_CP1_CI_AS.

Bevor Sie Identity Applications migrieren, müssen Sie die Bibliotheken libssl.so.1.0.0 und libcrypto.so.1.0.0 aus dem Verzeichnis /opt/netiq/common/openssl/lib64/ installieren.

Die Migration von Identity Applications umfasst Folgendes:

- „Migrieren der Datenbank zum neuen Server“, auf Seite 212
- „Installieren von Identity Applications auf dem neuen Server“, auf Seite 213

Migrieren der Datenbank zum neuen Server

Wenn sich Ihre Benutzeranwendungsdatenbank auf PostgreSQL befindet, führen Sie folgende Schritte aus:

1. Melden Sie sich bei dem Server an, auf dem PostgreSQL installiert ist.
2. Öffnen Sie die Eingabeaufforderung, navigieren Sie zum Verzeichnis `postgres bin` und exportieren Sie die Daten in eine `.sql`-Datei.

   Beispiel: `pg_dumpall -U postgres > dump.sql`
3. Melden Sie sich am neuen Server an, auf dem PostgreSQL installiert werden soll.
4. Installieren Sie PostgreSQL wie unten beschrieben:
   - **4a** Laden Sie die Datei `Identity_Manager_4.10.x_Windows.iso` vom Softwarelizenz- und Download (https://sldlogin.microfocus.com/)-Portal herunter und hängen Sie sie ein.
   - **4b** Navigieren Sie zu dem Speicherort, an dem Sie die Datei `Identity_Manager_4.10_Windows.iso` eingehängt haben.
   - **4c** Navigieren Sie zu: `<Einhänge-Speicherort>\common\packages\postgres\directory.`
   - **4d** Führen Sie das `PostgreSQL`-Installationsprogramm aus.
5. Navigieren Sie zu `C:\NetIQ\IDM\postgres` und löschen Sie das Datenverzeichnis.
6. Erstellen Sie ein Datenverzeichnis am Installationsort von PostgreSQL und stellen Sie sicher, dass der Benutzer `postgres` Zugriffsrechte auf das Verzeichnis hat.
7. Öffnen Sie die Eingabeaufforderung, navigieren Sie zum Verzeichnis `postgres bin` und initialisieren Sie die Datenbank wie unten gezeigt:

   Beispiel: `initdb.exe -D C:\NetIQ\IDM\postgres\data -E WIN1252 -U postgres.`
8. Vergewissern Sie sich, dass unter `C:\NetIQ\IDM\postgres\data` in der Datei `pg_hba.conf` die folgenden Einträge vorhanden sind.

   # IPv6 lokale Verbindungen:

   `host all all ::1/128 trust`

   `host all all 0.0.0.0/0 trust`
9. Vergewissern Sie sich, dass in der Datei `postgresql.conf` Folgendes auskommentiert ist:

   listen_addresses = '*'

   port=5432
10. Starten Sie die `postgres`-Dienste neu und führen Sie dazu `services.msc` über `Ausführen` aus.
11. Öffnen Sie die Eingabeaufforderung, navigieren Sie zum Verzeichnis `postgres bin` und importieren Sie die Daten in die neue PostgreSQL-Datenbank. Verwenden Sie dann den gesammelten Dump wie in Schritt 2 beschrieben.

    Beispiel: `psql -U postgres < dump.sql.`

Installieren von Identity Applications auf dem neuen Server

Im folgenden Verfahren wird die Installation von Identity Applications auf dem neuen Server erläutert:

1. Laden Sie die Datei `Identity_Manager_4.10.x_Windows.iso` von der OpenText-Downloads-Website (https://dl.netiq.com/) herunter.
2. Hängen Sie die `.iso`-Datei ein.
3. Navigieren Sie zum Verzeichnis `Identity apps`, installieren Sie **Identity Applications** und überspringen Sie die Bereitstellung der Benutzeranwendung und des Treibers für den Rollen- und Ressourcendienst.
   - **3a** Wählen Sie den Modus "Benutzerdefinierte Installation".
   - **3b** Geben Sie die Details des Identitätsdepots ein.
   - **3c** Deaktivieren Sie die Option **Identity Applications-Treiber bereitstellen**.
4. Wählen Sie **Vorhandener PostgreSQL**-Server, geben Sie die erforderlichen Details an und fahren Sie mit der Installation fort.

Abschließen der Migration der Identity Applications

Nach dem Aufrüsten oder Migrieren der Identity Applications schließen Sie den Migrationsvorgang ab.

Vorbereiten einer Oracle-Datenbank für die SQL-Datei

Während des Installationsvorgangs haben Sie ggf. angegeben, dass eine SQL-Datei zum Aktualisieren der Datenbank der Identity Applications geschrieben werden soll. Wenn Ihre Datenbank auf einer Oracle-Plattform ausgeführt wird, sind weitere Schritte erforderlich, bevor Sie die SQL-Datei ausführen können.

1. Führen Sie in der Datenbank die folgenden SQL-Anweisungen aus:

```
ALTER TABLE DATABASECHANGELOG ADD ORDEREXECUTED INT;
UPDATE DATABASECHANGELOG SET ORDEREXECUTED = -1;
ALTER TABLE DATABASECHANGELOG MODIFY ORDEREXECUTED INT NOT NULL;
ALTER TABLE DATABASECHANGELOG ADD EXECTYPE VARCHAR(10);
UPDATE DATABASECHANGELOG SET EXECTYPE = 'EXECUTED';
ALTER TABLE DATABASECHANGELOG MODIFY EXECTYPE VARCHAR(10) NOT NULL;
```

2. Führen Sie den folgenden `updateSQL`-Befehl aus:

```
C:\NetIQ\idm\jre\bin\java -Xms256m -Xmx256m -Dwar.context.name=IDMProv
-
Ddriver.dn="cn=User Application Driver,cn=driverset1,o=system" -
Duser.container="o=data" -jar C:\NetIQ\idm\jre\liquibase.jar --
databaseClass=liquibase.database.core.PostgresDatabase --
driver=org.postgresql.Driver --
classpath=C:\NetIQ\idm\apps\postgresql\postgresql-9.4.1212jdbc42.jar
C:\NetIQ\idm\apps\UserApplication\IDMProv.war --
changeLogFile=DatabaseChangeLog.xml --url="jdbc:postgresql://
localhost:5432/
idmuserappdb" --contexts="prov,newdb" --logLevel=info --
logFile=C:\NetIQ\idm\apps\UserApplication\db.out --username******** --
password******** update
```

3 Öffnen Sie die SQL-Datei (standardmäßig im Verzeichnis *\Installationspfad*\userapp\sql) in einem Texteditor.

4 Fügen Sie einen umgekehrten Schrägstrich (/) nach der Definition der Funktion CONCAT_BLOB ein. Beispiel

```
  -- Changeset icfg-data-load.xml::700::IDMRBPM
CREATE OR REPLACE FUNCTION CONCAT_BLOB(A IN BLOB, B IN BLOB) RETURN BLOB
AS
                C BLOB;
            BEGIN
                DBMS_LOB.CREATETEMPORARY(C, TRUE);
                DBMS_LOB.APPEND(C, A);
                DBMS_LOB.APPEND(C, B);
                RETURN c;
            END;
/
```

5 Führen Sie die SQL-Datei aus.

Weitere Informationen zum Ausführen der SQL-Datei finden Sie in „Manuelles Erstellen der Datenbank“, auf Seite 99.

HINWEIS: Führen Sie die SQL-Datei nicht mit SQL*Plus aus. Die Zeilen in der Datei sind länger als 4000 Zeichen.

Leeren des Browsercache

Bevor Sie sich bei den Identity Applications anmelden, leeren Sie den Cache des Browsers. Wenn Sie den Cache nicht leeren, können einige Laufzeitfehler auftreten.

Aktualisieren der Einstellung für die maximale Zeitüberschreitung für das SharedPagePortlet

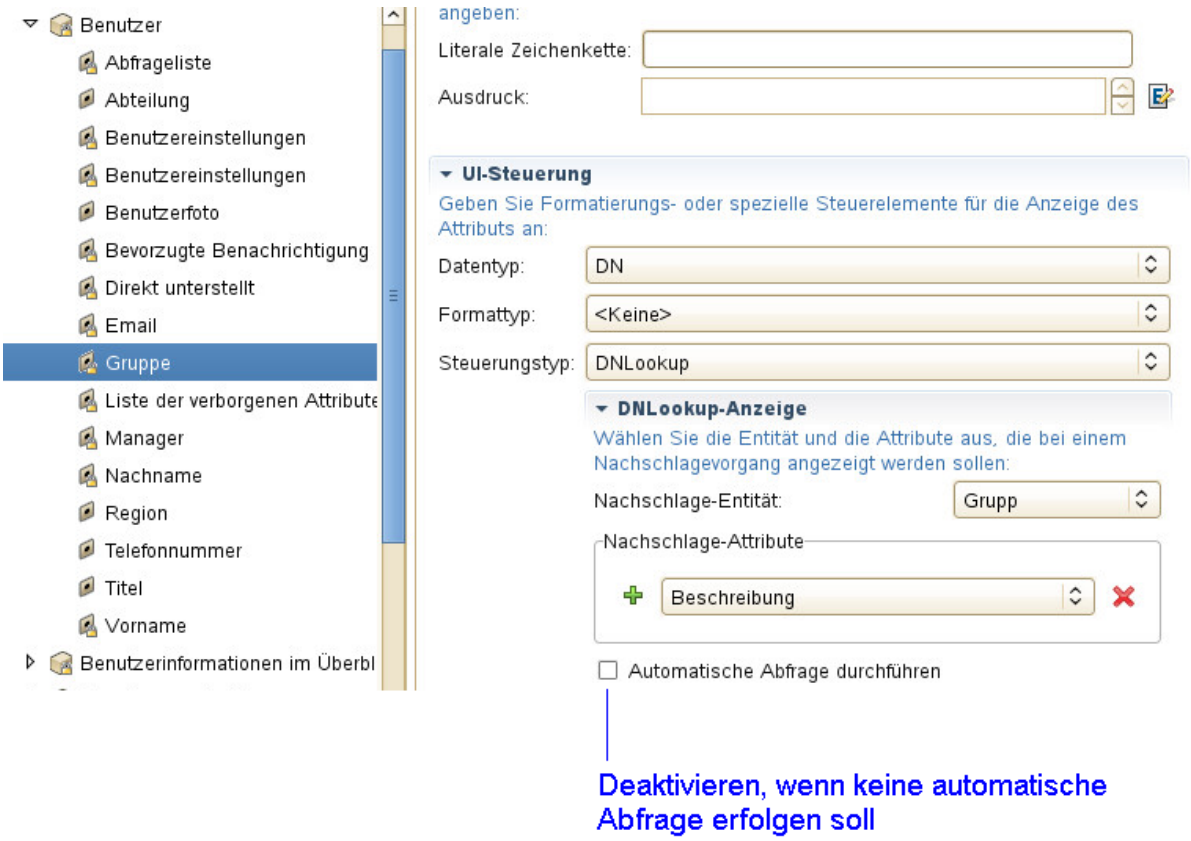
Falls Sie die Standardeinstellungen für das SharedPagePortlet angepasst haben, wurden diese Änderungen in der Datenbank gespeichert, und diese Einstellung wird überschrieben. Wenn Sie zur Registerkarte „Identitätsselbstbedienung“ navigieren, wird daher unter Umständen nicht die richtige freigegebene Seite hervorgehoben. Führen Sie die folgenden Schritte aus, damit dieses Problem nicht auftritt:

1. Melden Sie sich als Benutzeranwendungsadministrator an.
2. Navigieren Sie zu **Administration > Portletadministration**.
3. Erweitern Sie den Eintrag **Navigation für die freigegebene Seite**.
4. Klicken Sie links im Portlet-Baum auf **Navigation für die freigegebene Seite**.
5. Klicken Sie rechts auf der Seite auf **Einstellungen**.
6. Die Einstellung **Maximale Zeitüberschreitung** muss 0 lauten.
7. Klicken Sie auf **Einstellungen speichern**.

Deaktivieren der Einstellung für automatische Abfragen für Gruppen

Standardmäßig ist die DNLookup-Anzeige für die Gruppenentität in der Verzeichnisabstraktionsschicht aktiviert. Sobald also die Objektauswahl für eine Gruppenzuweisung geöffnet wird, werden standardmäßig alle Gruppen angezeigt, ohne dass Sie nach den Gruppen suchen müssen. Sie können diese Einstellung ändern, da das Fenster für die Gruppensuche erst dann Ergebnisse zeigen sollte, wenn der Benutzer die Suchkriterien festgelegt hat.

Zum Ändern dieser Einstellung deaktivieren Sie in Designer die Option **Automatische Abfrage durchführen**:


Benutzer
Abfrageliste
Abteilung
Benutzereinstellungen
Benutzereinstellungen
Benutzerfoto
Bevorzugte Benachrichtigung
Direkt unterstellt
Email
Gruppe
Liste der verborgenen Attribute
Manager
Nachname
Region
Telefonnummer
Titel
Vorname
Benutzerinformationen im Überbl
angeben:
Literale Zeichenkette:
Ausdruck:
UI-Steuerung
Geben Sie Formatierungs- oder spezielle Steuerelemente für die Anzeige des Attributs an:
Datentyp:
DN
Formattyp:
<Keine>
Steuerungstyp:
DNLookup
DNLookup-Anzeige
Wählen Sie die Entität und die Attribute aus, die bei einem Nachschlagevorgang angezeigt werden sollen:
Nachschlage-Entität:
Grupp
Nachschlage-Attribute
Beschreibung
Automatische Abfrage durchführen
Deaktivieren, wenn keine automatische Abfrage erfolgen soll

IX Bereitstellen von OpenText Identity Manager in Microsoft Azure

In diesem Abschnitt wird erläutert, wie OpenText Identity Manager in der Microsoft Azure-Cloud geplant und implementiert wird.

- Kapitel 20, „Planung und Implementierung von OpenText Identity Manager in Microsoft Azure“, auf Seite 219
- Kapitel 21, „Beispielszenarien für Hybrid OpenText Identity Manager“, auf Seite 231

20 Planung und Implementierung von OpenText Identity Manager in Microsoft Azure

OpenText Identity Manager unterstützt die Bereitstellung der folgenden OpenText Identity Manager-Komponenten in Microsoft Azure.

- OpenText Identity Manager-Engine
- OpenText Identity Manager-Treiber und Remote Loader
- Designer
- Identity Applications
- Identity Reporting

HINWEIS: Die Bereitstellung von Sentinel Log Management wird in Microsoft Azure nicht unterstützt.

Voraussetzungen

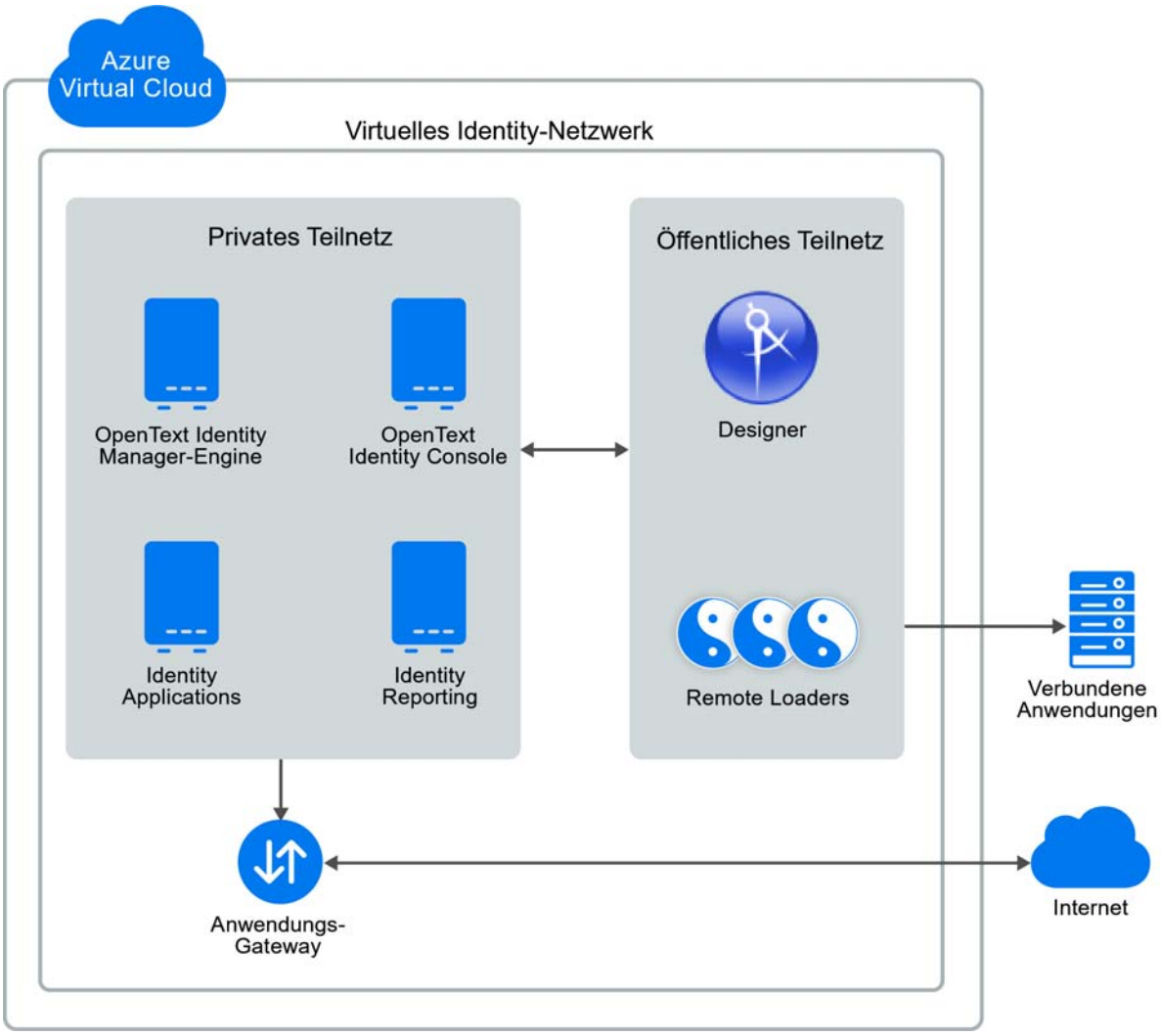
Zusätzlich zu den Systemanforderungen für die OpenText Identity Manager-Komponenten müssen Sie auch die folgenden Voraussetzungen erfüllen:

- Ein Verwaltungskonto in Microsoft Azure.
- `Identity_Manager_4.10.0_Windows.iso` und Designer sind heruntergeladen und extrahiert und stehen in den Instanzen der OpenText Identity Manager-Komponenten zur Verfügung.
- Remote-Desktop zur Herstellung einer Verbindung zu den Azure VM-Instanzen von Ihrem lokalen Client-Computer aus.

Bereitstellungsverfahren

OpenText Identity Manager-Komponenten können je nach Bedarf in einem privaten oder einem öffentlichen Netzwerk bereitgestellt werden. Abbildung 20-1 veranschaulicht ein Beispiel einer Bereitstellung, das in den folgenden Abschnitten herangezogen wird.

Abbildung 20-1 *Bereitstellung von OpenText Identity Manager unter Microsoft Azure*



OpenText Identity Manager-Komponenten können in unterschiedlichen Kombinationen unter Microsoft Azure bereitgestellt werden. Es hängt davon ab, wie die Komponenten auf verschiedenen Servern verteilt sind. Der Bereitstellungsvorgang ist jedoch für alle Szenarien gleich.

Das Bereitstellungsverfahren umfasst die folgenden Schritte:

- „Erstellen einer Ressourcengruppe“, auf Seite 221
- „Erstellen eines virtuellen Netzwerks und Teilnetzes“, auf Seite 221
- „Erstellen eines Anwendungs-Gateways“, auf Seite 222
- „Erstellen einer VM-Instanz“, auf Seite 224
- „Aktualisieren von Host-Einträgen in der VM“, auf Seite 225
- „Einrichten von Designer“, auf Seite 226
- „Konfigurieren des Anwendungs-Gateways“, auf Seite 226

Erstellen einer Ressourcengruppe

Wir empfehlen, eine Ressourcengruppe zu erstellen und die erforderlichen Ressourcen zur Gruppe hinzuzufügen, um sie mit OpenText Identity Manager zu verwenden. Führen Sie zum Erstellen einer neuen Ressourcengruppe die folgenden Schritte aus:

1. Melden Sie sich beim Azure-Portal an.
2. Klicken Sie auf **Ressourcengruppen**.
3. Klicken Sie auf **Create** (Erstellen).
4. In der Registerkarte **Grundlagen**:
   - **4a** Wählen Sie in der Dropdown-Liste Ihr **Abonnement** aus.
   - **4b** Geben Sie einen neuen Namen für die Ressourcengruppe ein.
   - **4c** Wählen Sie in der Dropdown-Liste **Region** den Speicherort. Beispiel: `Zentralindien`
   - **4d** Klicken Sie auf **Weiter: Tags >**.
5. Klicken Sie auf der Registerkarte **Tags** auf **Weiter: Überprüfen + Erstellen >**.
6. Klicken Sie auf der Registerkarte **Überprüfen + Erstellen** auf **Erstellen**.

Erstellen eines virtuellen Netzwerks und Teilnetzes

1. Melden Sie sich beim Azure-Portal an.
2. Geben Sie **virtuelles Netzwerk** in die Suche ein.
3. Wählen Sie unter Dienste **Virtuelle Netzwerke**.
4. Klicken Sie auf **Create** (Erstellen).
5. Geben Sie auf der Registerkarte **Grundlagen** die folgenden Details an:

Feld	Beschreibung
Abonnement	Wählen Sie in der Dropdown-Liste Ihr Abonnement.
Ressourcengruppe	Wählen Sie in der Dropdown-Liste eine vorhandene Ressourcengruppe.
Name	Geben Sie den Namen für das virtuelle Netzwerk an.
Region	Wählen Sie in der Dropdown-Liste den Speicherort. Beispiel: `Zentralindien`

   - **5a** Klicken Sie auf **Weiter: IP-Adressen >**.
6. Klicken Sie auf der Registerkarte IP-Adressen auf **Teilnetz hinzufügen**.
   - **6a** Klicken Sie auf **Teilnetz hinzufügen**.
     - **6a1** Geben Sie den Namen für das Teilnetz an. Beispiel: `Standard`.
     - **6a2** Geben Sie den Teilnetz-Adressbereich an. Beispiel: `10.1.0.0/24`.
     - **6a3** Klicken Sie auf **Hinzufügen**.
   - **6b** Klicken Sie auf **Weiter: Sicherheit >**.

7 Behalten Sie auf der Registerkarte **Sicherheit** die Standardwerte für alle Felder bei und klicken Sie dann auf **Weiter: Tags >**.

8 Klicken Sie auf der Registerkarte **Tags** auf **Weiter: Überprüfen + Erstellen >**.

9 Überprüfen Sie Ihre Einstellungen auf der Registerkarte **Überprüfen + Erstellen** und klicken Sie dann auf **Erstellen**.

Erstellen eines Anwendungs-Gateways

1 Melden Sie sich beim Azure-Portal an.

2 Klicken Sie auf **Ressource erstellen**.

3 Gehen Sie zu **Kategorien** > **Networking** > **Anwendungs-Gateway**.

4 Geben Sie auf der Registerkarte **Grundlagen** die folgenden Details an:

Feld	Beschreibung
Abonnement	Wählen Sie in der Dropdown-Liste Ihr Abonnement.
Ressourcengruppe	Wählen Sie in der Dropdown-Liste eine vorhandene Ressourcengruppe.
Name des Anwendungs-Gateways	Geben Sie den Namen des Anwendungs-Gateways an.
Region	Wählen Sie in der Dropdown-Liste den Speicherort. Beispiel: `Zentralindien`
Ebene	Wählen Sie die gewünschte Ebene. Beispiel: **Standard V2**.
Min. Anzahl Instanzen	Geben Sie den Wert **0** an.
Max. Anzahl Instanzen	Geben Sie den Wert **10** an.
Virtuelles Netzwerk	Wählen Sie das virtuelle Netzwerk und das entsprechende erstellte Teilnetz. Weitere Informationen hierzu finden Sie in „Erstellen eines virtuellen Netzwerks und Teilnetzes“, auf Seite 221.

4a Behalten Sie die Standardwerte für die übrigen Felder bei und klicken Sie auf **Weiter: Frontends >**.

5 Auf der Registerkarte **Frontends**:

5a Wählen Sie **Öffentlich**.

5b Klicken Sie unter **Öffentliche IP-Adresse** auf **Neue hinzufügen**.

5b1 Geben Sie den Namen der öffentlichen IP-Adresse an. Beispiel: idmgateway.centralindia.cloudapp.azure.com.

5b2 Klicken Sie auf **OK**.

5c Klicken Sie auf **Weiter: Backends >**

6 Auf der Registerkarte **Backends**:

6a Klicken Sie auf **Backend-Pool hinzufügen**.

6a1 Geben Sie den Namen des Backend-Pools an.

6a2 Wählen Sie **Ja**, um einen Backend-Pool ohne Ziele hinzuzufügen.

6a3 Klicken Sie auf **Hinzufügen**.

6b Klicken Sie auf **Weiter: Konfiguration >**.

7 Auf der Registerkarte **Konfiguration**:

7a Klicken Sie unter **Routing-Regeln** auf **Routing-Regel hinzufügen**.

7b Geben Sie den Namen der Regel an.

7c Geben Sie auf der Registerkarte **Listener** die folgenden Details an:

Feld	Beschreibung
Listener-Name	Geben Sie den Namen des Listeners an.
Frontend-IP	Wählen Sie in der Dropdown-Liste die Option **Öffentlich**.
Protokoll	Wählen Sie **HTTP**.
Port	Geben Sie den Wert **80** an.

7d Behalten Sie die Standardwerte für die restlichen Felder bei.

7e Geben Sie auf der Registerkarte **Backend-Ziele** die folgenden Details an:

Feld	Beschreibung
Backend-Ziel	Wählen Sie in der Dropdown-Liste das Backend-Ziel.
HTTP-Einstellungen	Klicken Sie auf **Neue hinzufügen** und geben Sie den Namen der HTTP-Einstellungen an. Behalten Sie die Standardwerte für alle Felder bei und klicken Sie dann auf **Hinzufügen**.

7e1 Klicken Sie auf **Hinzufügen**.

7f Klicken Sie auf **Weiter: Tags >**.

8 Klicken Sie auf der Registerkarte **Tags** auf **Weiter: Überprüfen + Erstellen >**.

9 Überprüfen Sie Ihre Einstellungen auf der Registerkarte **Überprüfen + Erstellen** und klicken Sie dann auf **Erstellen**.

HINWEIS: Weitere Informationen über die Konfiguration des Anwendungs-Gateways finden Sie unter „Konfigurieren des Anwendungs-Gateways“, auf Seite 226.

Erstellen einer VM-Instanz

Erstellen Sie eine separate virtuelle Maschine zum Hosten der OpenText Identity Manager-Komponenten.

1. Melden Sie sich beim Azure-Portal an.
2. Geben Sie **virtuelle Maschinen** in die Suche ein.
3. Wählen Sie unter Dienste **Virtuelle Maschinen**.
4. Klicken Sie auf **Erstellen** und wählen Sie dann **Virtuelle Maschine**.
5. In der Registerkarte **Grundlagen**:
   - **5a** Wählen Sie in der Dropdown-Liste Ihr **Abonnement** aus.
   - **5b** Wählen Sie in der Dropdown-Liste eine vorhandene Ressourcengruppe (weitere Informationen finden Sie unter „Erstellen einer Ressourcengruppe“, auf Seite 221).
   - **5c** Geben Sie den **Namen der virtuellen Maschine** an.
   - **5d** Wählen Sie in der Dropdown-Liste **Region** den Speicherort. Beispiel: `Zentralindien`
   - **5e** Wählen Sie in der Dropdown-Liste **Image** den gewünschten **Windows Server**. Beispiel: `Windows Server 2019`.
   - **5f** Wählen Sie in der Dropdown-Liste **Größe** die Größe der virtuellen Maschine.
   - **5g** Geben Sie den **Benutzernamen** und das **Passwort** an und wählen Sie **Passwort bestätigen**.
   - **5h** Wählen Sie unter Lizenzierung die Option **Windows Server-Lizenz** und dann zur Bestätigung die berechtigte **Windows Server-Lizenz mit Software Assurance**.
   - **5i** Behalten Sie die Standardwerte für die restlichen Felder bei.
   - **5j** Klicken Sie auf **Weiter: Konfiguration > Datenträger**.
6. Auf der Registerkarte **Datenträger**:
   - **6a** Wählen Sie in der Dropdown-Liste **BS-Datenträgertyp** den Datenträgertyp. Beispiel: `Premium SSD`.
   - **6b** Wählen Sie in der Dropdown-Liste den erforderlichen Verschlüsselungstyp.
   - **6c** Klicken Sie auf **Weiter: Networking >**.
7. Auf der Registerkarte **Networking**:
   - **7a** Wählen Sie das virtuelle Netzwerk und das entsprechende erstellte Teilnetz. Weitere Informationen finden Sie unter „Erstellen eines virtuellen Netzwerks und Teilnetzes“, auf Seite 221.
   - **7b** Wählen Sie unter der Netzwerksicherheitsgruppe die Option **Erweitert**.
   - **7c** Wählen Sie in der Dropdown-Liste eine vorhandene Netzwerksicherheitsgruppe.
     - **7c1** (Bedingt) Wenn die Netzwerksicherheitsgruppe nicht verfügbar ist, klicken Sie auf **Neu erstellen**.
     - **7c2** Geben Sie den Namen der Netzwerksicherheitsgruppe an.
     - **7c3** Klicken Sie auf **Eingangsrolle hinzufügen** und geben Sie die erforderlichen Details an.
     - **7c4** Klicken Sie auf **Ausgangsrolle hinzufügen** und geben Sie die erforderlichen Details an.
     - **7c5** Klicken Sie auf **OK**.

7d Behalten Sie die Standardwerte für die restlichen Felder bei.

7e Klicken Sie auf **Weiter: Verwaltung >**.

8 Behalten Sie auf der Registerkarte **Verwaltung** die Standardwerte für alle Felder bei und klicken Sie dann auf **Weiter: Erweitert >**.

9 Behalten Sie auf der Registerkarte **Erweitert** die Standardwerte für alle Felder bei und klicken Sie dann auf **Weiter: Tags >**.

10 Behalten Sie auf der Registerkarte **Tags** die Standardwerte für alle Felder bei und klicken Sie dann auf **Weiter: Überprüfen + Erstellen >**.

11 Überprüfen Sie Ihre Einstellungen auf der Registerkarte **Überprüfen + Erstellen** und klicken Sie dann auf **Erstellen**.

Aktualisieren von Host-Einträgen in der VM

Auf die OpenText Identity Manager-Komponente kann mit dem öffentlichen DNS-Namen des Anwendungs-Gateways oder mit dem Alias-DNS-Datensatz zugegriffen werden. Damit die OpenText Identity Manager-Komponenten miteinander kommunizieren können, bearbeiten Sie die Host-Dateien auf jeder VM und fügen Sie einen Eintrag zur Auflösung des Hostnamens hinzu.

Tabelle 20-1 *Aktualisieren von Host-Einträgen*

Komponenten	Beschreibung

Identity-Engine	Navigieren Sie in der Identity Engine-VM zur Datei **hosts**. Beispiel:
	`C:\Windows\System32\drivers\etc\hosts`
	Bearbeiten Sie die Hostdatei mit folgendem Eintrag:
	`<IP-Adresse der Identity Engine-VM> <Privater DNS-Name der Identity Engine-VM>`
	Beispiel:
	`10.0.1.1 identityengine.example.com`
	`<IP-Adresse der Identity Applications-VM> <Öffentlicher DNS-Name des Anwendungs-Gateways>`
	Beispiel:
	`10.0.1.2 idmgateway.centralindia.cloudapp.azure.com`

Komponenten	Beschreibung

Identity Applications	Navigieren Sie in der Identity Engine-VM zur Datei **hosts**. Beispiel:
	
	C:\Windows\System32\drivers\etc\hosts
	
	Bearbeiten Sie die Hostdatei mit folgendem Eintrag:
	
	`<IP-Adresse der Identity Engine-VM> <Privater DNS-Name der Identity Engine-VM>`
	
	Beispiel:
	
	`10.0.1.1 identityengine.example.com`
	
	`<IP-Adresse der Identity Applications-VM> <Öffentlicher DNS-Name des Anwendungs-Gateways>`
	
	Beispiel:
	
	`10.0.1.2 idmgateway.centralindia.cloudapp.azure.com`

Weitere Informationen zum Aktualisieren der Host-Einträge für Identity Reporting finden Sie in **unter** Identity ApplicationsTabelle 20-1 auf Seite 225.

HINWEIS: Weitere Informationen zur Installation der OpenText Identity Manager-Komponenten finden Sie unter „Installationsverfahren“, auf Seite 46.

Einrichten von Designer

1 Starten Sie eine Instanz der virtuellen Maschine in einem öffentlichen Teilnetz. Weitere Informationen finden Sie unter „Erstellen einer VM-Instanz“, auf Seite 224.

   Verwenden Sie für die Windows-Sicherheitsgruppe nur den Port `rdesktop`. Beispiel: 3389.

2 Installieren Sie Designer. Weitere Informationen finden Sie in Teil V, „Installation von Designer“, auf Seite 135.

Konfigurieren des Anwendungs-Gateways

Konfigurieren Sie das Anwendungs-Gateway, damit externe Netzwerke die OpenText Identity Manager-Komponenten verwenden können, die auf den virtuellen Maschinen gehostet werden.

1 Konfigurieren Sie einen separaten Backend-Pool für die OpenText Identity Manager-Komponenten wie Identity Applications, Formulare und Identity Reporting.

   1a Klicken Sie in **Backend-Pools** auf **Hinzufügen**.

   1b Geben Sie die folgenden Informationen an:

Feld	Beschreibung
Name	Geben Sie den Namen eines Backend-Pools zur Kennzeichnung der OpenText Identity Manager-Komponente an.
Typ	Geben Sie den Typ auf eine der folgenden Arten an: ◆ **IP-Adresse oder FQDN:** Geben Sie die IP-Adresse oder den FQDN der erforderlichen OpenText Identity Manager-Komponente an. ◆ **Virtuelle Maschine:** Wählen Sie die virtuelle Maschine aus, auf der die erforderliche OpenText Identity Manager-Komponente gehostet wird.

1c Klicken Sie auf **OK**.

Wiederholen Sie diesen Schritt, um weitere Backend-Pools zu erstellen.

2 Konfigurieren Sie separate HTTP-Einstellungen für die OpenText Identity Manager-Komponenten wie Identity Applications, Formulare und Identity Reporting.

HINWEIS: Vergewissern Sie sich, dass Sie das öffentliche Zertifikat für die erforderlichen OpenText Identity Manager-Komponenten exportiert haben.

2a Klicken Sie unter **HTTP-Einstellungen** auf **Hinzufügen**.

2b Geben Sie die folgenden Informationen an:

Feld	Beschreibung
Name	Geben Sie den Namen einer HTTP-Einstellung zur Kennzeichnung der OpenText Identity Manager-Komponente an.
Protokoll	Wählen Sie HTTPS aus.
Port	Geben Sie den Port der OpenText Identity Manager-Komponente an. Beispiel: ◆ **Identity Applications:** 8543 ◆ **Formulare:** 8600 ◆ **Identity Reporting:** 8643
Zertifikate für die Backend-Authentifizierung	1. Wählen Sie "Neu erstellen" aus. 2. Geben Sie den Namen des Zertifikats an. 3. Navigieren Sie zum exportierten öffentlichen Zertifikat für die entsprechende OpenText Identity Manager-Komponente und laden Sie sie herauf. 4. Klicken Sie auf "Zertifikat hinzufügen".

2c Klicken Sie auf **OK**.

Wiederholen Sie diesen Schritt, um weitere HTTP-Einstellungen zu konfigurieren.

3 Konfigurieren Sie einen separaten Listener für die OpenText Identity Manager-Komponente wie Identity Applications, Formulare und Identity Reporting.

HINWEIS: Vergewissern Sie sich, dass Sie das .PFX-Zertifikat aus dem Identitätsdepot exportiert haben.

3a Klicken Sie unter **Listener** auf **Einfach**.

3b Geben Sie die folgenden Informationen an:

Feld	Beschreibung
Name	Geben Sie den Namen des Listener zur Kennzeichnung der OpenText Identity Manager-Komponente an.
Frontend-IP-Konfiguration	1. Wählen Sie das virtuelle Netzwerk und das vorher erstellte Teilnetz aus. Weitere Informationen finden Sie unter „Erstellen eines virtuellen Netzwerks und Teilnetzes“, auf Seite 221. 2. Geben Sie den Namen und die Portnummer der Anwendung an. Beispiel: **Identity Applications:** 8543 **Formulare:** 8600 **Identity Reporting:** 8643
Protokoll	Wählen Sie **HTTPS** aus.
Zertifikat	1. Navigieren Sie zum PFX-Zertifikat und laden Sie es herauf. 2. Geben Sie den Namen und das Passwort des Zertifikats an.

3c Klicken Sie auf **OK**.

Wiederholen Sie diesen Schritt, um weitere Listener zu konfigurieren.

4 Erstellen Sie eine Basisregel für die OpenText Identity Manager-Komponenten wie Identity Applications, Formulare und Identity Reporting und verknüpfen Sie diese Regel mit dem entsprechenden Backend-Pool, dem Listener und der HTTP-Einstellung.

4a Klicken Sie unter **Regel** auf **Hinzufügen**.

4b Geben Sie die folgenden Informationen an:

Feld	Beschreibung
Name	Geben Sie den Namen einer Regel an, durch die die OpenText Identity Manager-Komponente erkannt wird.
Listener	Wählen Sie den in Schritt 3 erstellten entsprechenden Listener aus.
Backend-Pool	Wählen Sie den in Schritt 1 erstellten entsprechenden Backend-Pool aus.
HTTP-Einstellung	Wählen Sie die in Schritt 2 erstellte entsprechende HTTP-Einstellung aus.

4c Klicken Sie auf OK.

Wiederholen Sie diesen Schritt, um weitere Regeln zu erstellen.

21 Beispielszenarien für Hybrid OpenText Identity Manager

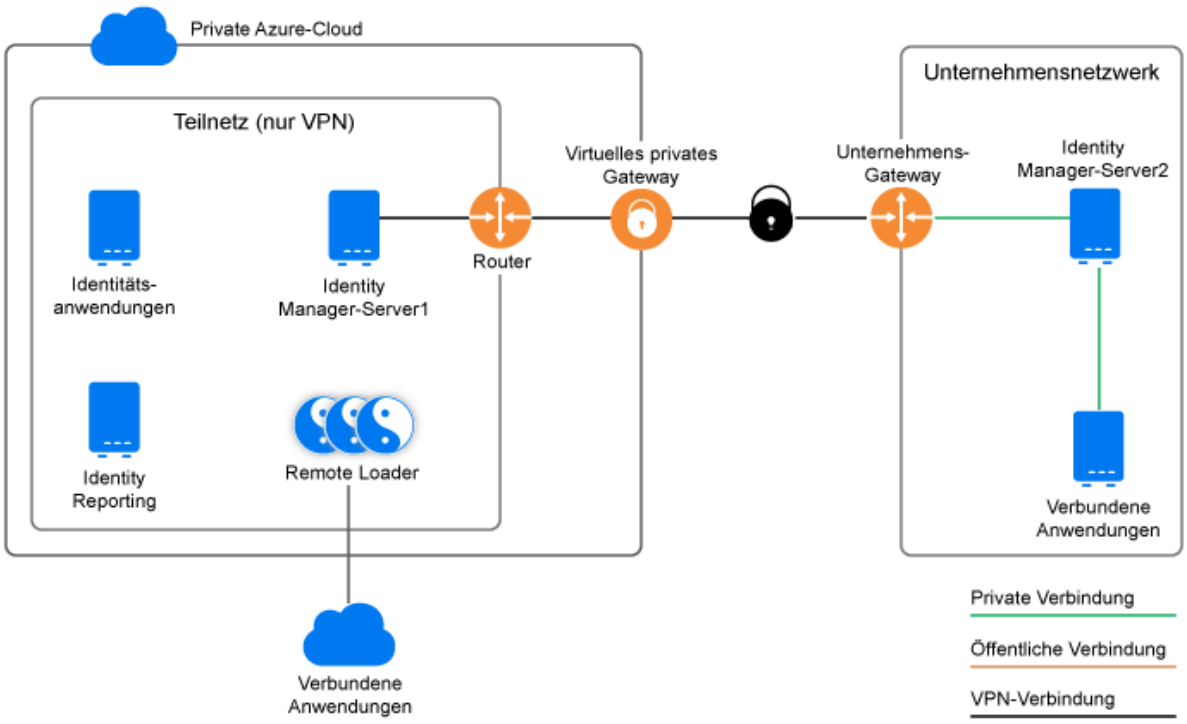
Für die OpenText Identity Manager-Komponenten kann konfiguriert werden, wo die Identitäten nahtlos zwischen dem Unternehmensstandort und MS Azure synchronisiert werden. Für die Implementierung dieser Art von Hybridszenario müssen Sie eine VPN-Verbindung zwischen dem Azure-Teilnetz und dem Unternehmensnetzwerk konfigurieren. In diesem Abschnitt werden die folgenden Hybridszenarien erläutert:

- „Verwenden der Treibersatzverbindung mehrerer Server“, auf Seite 231
- „Verwenden der OpenText eDirectory-Treiberverbindung“, auf Seite 232

Verwenden der Treibersatzverbindung mehrerer Server

In diesem Szenario verwenden mindestens zwei OpenText Identity Manager-Server denselben OpenText eDirectory-Baum und Treibersatz, wobei ein Server in der Azure-Cloud und der andere am Unternehmensstandort installiert ist. Dazu gehören vollständige Replikationsserver, die über die Replikationskanäle des Identitätsdepots die Identitäten über die VPN-Verbindung synchronisieren. Der OpenText Identity Manager-Server, der im Unternehmensnetzwerk oder in der Azure-Cloud ausgeführt wird, synchronisiert die Identitäten zwischen den entsprechenden verbundenen Anwendungen.

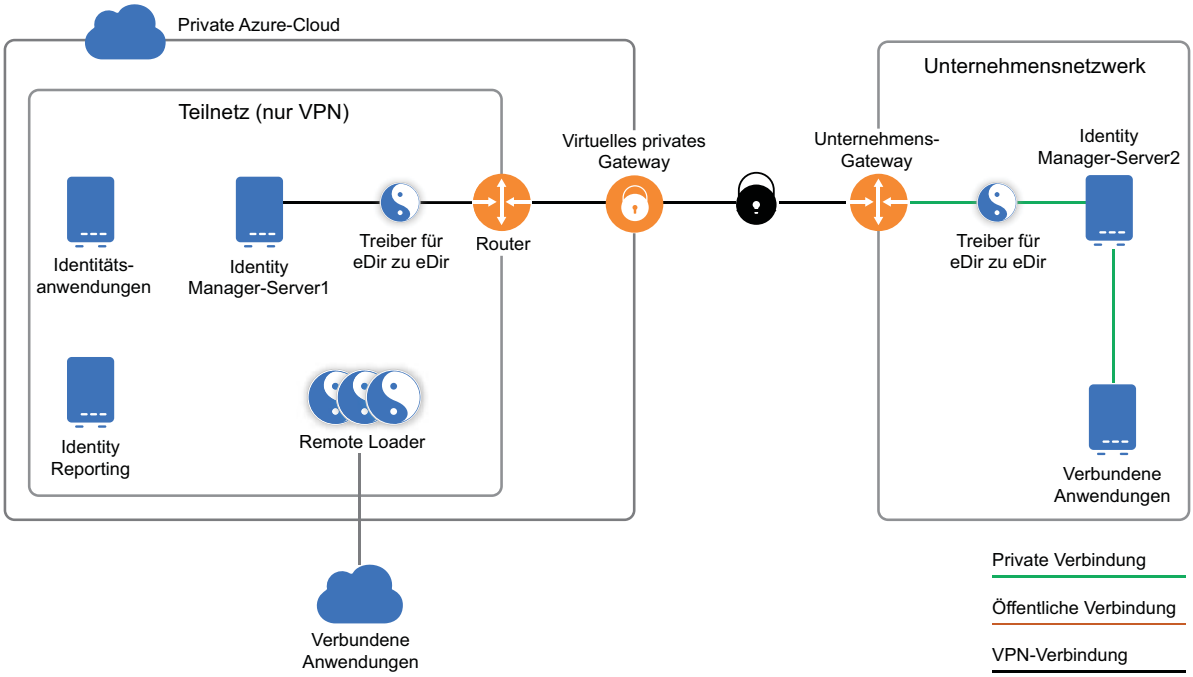
Abbildung 21-1 *Hybridszenario mit Treibersatzverbindung mehrerer Server*



Verwenden der OpenText eDirectory-Treiberverbindung

Dieses Szenario eignet sich bei Installation von OpenText Identity Manager-Servern in zwei verschiedenen OpenText eDirectory-Bäumen, wobei ein Baum zur Azure-Cloud gehört und der andere Baum zum Unternehmensnetzwerk. Bei dieser Konfiguration wird der OpenText eDirectory-Treiber zur Synchronisierung der Identitäten zwischen der Azure-Cloud und dem Unternehmensnetzwerk über eine VPN-Verbindung verwendet. Der OpenText Identity Manager-Server, der im Unternehmensnetzwerk oder in der Azure-Cloud ausgeführt wird, synchronisiert die Identitäten zwischen den entsprechenden verbundenen Anwendungen.

Abbildung 21-2 *Hybridszenario mit OpenText eDirectory-Treiberverbindung*



Die Kommunikation zwischen der Azure-Cloud und dem Unternehmensnetzwerk ist eingeschränkt. Es werden nur die Deltaänderungen synchronisiert. Sie können die Synchronisierung der Attribute durch Konfigurieren der Treiberfilter steuern. Zudem haben Sie die Möglichkeit, weitere Steuerelemente zur Synchronisierung von Attributen über die Richtlinien-Engine zu definieren. Beispielsweise kann die Synchronisierung des Passwortattributs eingeschränkt werden und Benutzer können die Erlaubnis erhalten, verschiedene Passwörter für den Zugriff auf die OpenText Identity Manager-Server von der Azure-Cloud und dem Unternehmensnetzwerk zu verwenden.

X Bereitstellen von OpenText Identity Manager für Hochverfügbarkeit

Durch die Hochverfügbarkeit lassen sich wichtige Netzwerkressourcen wie Daten, Anwendungen und Dienste effizient verwalten. Wir unterstützen durch Clustering oder Hypervisor-Clustering wie VMWare Vmotion die Hochverfügbarkeit Ihrer OpenText Identity Manager-Lösung. Bei der Planung einer Hochverfügbarkeitsumgebung gelten die folgenden Überlegungen:

- Die folgenden Komponenten stehen zur Installation in einer Hochverfügbarkeitsumgebung zur Verfügung:
  - Identitätsdepot
  - OpenText Identity Manager-Engine
  - Remote Loader
  - Identity Applications mit Ausnahme von Identity Reporting
- Wenn Sie das Identitätsdepot in einer Clusterumgebung ausführen, wird auch die Identity Manager-Engine geclustert.

HINWEIS: OpenText Identity Manager unterstützt nicht die LDAP- oder LDAPS-Kommunikation mit Lastausgleich zwischen dem Identitätsdepot und Identity Applications.

Weitere Informationen zum ...	Erklärt in ...
Festlegen der Serverkonfiguration für Identity Manager-Komponenten	Informationen hierzu finden Sie unter Hochverfügbarkeitskonfiguration im *Überblick und Planungshandbuch zu OpenText™ Identity Manager CE 24.4 (v4.10)*.
Ausführen des Identitätsdepots in einem Cluster	Beispiellösung für eine Identity Manager-Clusterbereitstellung Bereitstellen von OpenText eDirectory in Hochverfügbarkeits-Clustern (https://www.netiq.com/documentation/edirectory-93/edir_install/data/bnew1gz.html) im *OpenText eDirectory-Installationshandbuch* (https://www.netiq.com/documentation/edirectory-93/)
Ausführen der Identity Applications in einem Cluster	Beispiellösung für eine Identity Applications-Clusterbereitstellung

Wenden Sie sich an den Technischen Support von (https://www.netiq.com/support/) , um weitere Informationen zur Bereitstellung von Hochverfügbarkeitssystemen und Disaster Recovery in Ihrer OpenText Identity Manager-Umgebung zu erhalten.

Im folgenden Kapitel finden Sie die Schritte zum Installieren und Konfigurieren der OpenText Identity Manager-Komponenten in einer Hochverfügbarkeitsumgebung:

- Kapitel 22, „Vorbereiten der Installation von OpenText Identity Manager in einer Clusterumgebung“, auf Seite 235
- Kapitel 23, „Beispiellösung für eine Identity Manager-Clusterbereitstellung“, auf Seite 239
- Kapitel 24, „Beispiellösung für eine Identity Applications-Clusterbereitstellung“, auf Seite 241

22 Vorbereiten der Installation von OpenText Identity Manager in einer Clusterumgebung

- Voraussetzungen
- Vorbereiten eines Clusters für Identity Applications

Voraussetzungen

- Identitätsdepot
- Identity Applications
- Datenbank für Identity Applications

Identitätsdepot

Wir empfehlen, vor der Installation des Identitätsdepots in einer Cluster-Umgebung die folgenden Überlegungen zu lesen:

- Es müssen mindestens zwei Windows-Server mit Clustersoftware vorhanden sein.
- Die Clustersoftware muss externen gemeinsam genutzten Speicher unterstützen, wobei ausreichend Speicherplatz für alle Identitätsdepot- und NICI-Daten vorhanden sein muss:
  - Die Identitätsdepot-DIB muss sich im gemeinsam genutzten Clusterspeicher befinden. Die Zustandsdaten für das Identitätsdepot müssen sich im gemeinsam genutzten Speicher befinden, damit sie für den Clusterknoten verfügbar sind, der zurzeit die Dienste ausführt.
  - Die Root-Identitätsdepot-Instanz auf den Clusterknoten muss so konfiguriert sein, dass sie die DIB des gemeinsamen Speichers verwendet.
  - Auch die NICI-Daten (NetIQ International Cryptographic Infrastructure) müssen gemeinsam genutzt werden, damit serverspezifische Schlüssel zwischen den Clusterknoten reproduziert werden. Die von allen Clusterknoten verwendeten NICI-Daten müssen sich im gemeinsam genutzten Clusterspeicher befinden.
  - Wir empfehlen, alle weiteren OpenText eDirectory-Konfigurationsdaten und Protokolldaten im gemeinsam genutzten Speicher abzulegen.
- Sie müssen eine virtuelle IP-Adresse besitzen.
- (Bedingt) Wenn Sie OpenText eDirectory als Rahmenstruktur für das Identitätsdepot verwenden, unterstützt das Dienstprogramm `nds-cluster-config` lediglich die Root-OpenText eDirectory-Instanz. eDirectory bietet keine Unterstützung für die Konfiguration von mehreren Instanzen und die Nicht-Root-Installation von OpenText eDirectory in einer Cluster-Umgebung.

Weitere Informationen zur Installation des Identitätsdepots in einer geclusterten Umgebung finden Sie im Abschnitt Bereitstellen von eDirectory in Hochverfügbarkeits-Clustern (https://www.netiq.com/documentation/edirectory-93/edir_install/data/bnew1gz.html) im *eDirectory-Installationshandbuch (https://www.netiq.com/documentation/edirectory-93/edir_install/data/bookinfo.html)*.

Identity Applications

Wenn die Datenbank für Identity Applications in einer Umgebung installiert werden soll, in der sich Tomcat-Cluster befinden, sind die folgenden Überlegungen zu beachten:

- Der Cluster muss einen eindeutigen Clusterpartitionsnamen, eine Multicast-Adresse und einen Multicast-Port aufweisen. Mithilfe dieser eindeutigen Kennungen werden mehrere Cluster voneinander unterschieden, sodass Leistungsprobleme und ungewöhnliches Verhalten vermieden werden.
  - Für jedes Mitglied des Clusters müssen Sie dieselbe Port-Nummer als Listener-Port für die Datenbank der Identity Applications angeben.
  - Für jedes Mitglied des Clusters müssen Sie denselben Hostnamen oder dieselbe IP-Adresse für den Server angeben, auf dem die Datenbank der Identity Applications gehostet wird.
- Die Uhren der Server im Cluster müssen synchronisiert werden. Wenn die Serveruhren nicht synchronisiert sind, kann eine frühzeitige Zeitüberschreitung von Sitzungen eintreten, sodass das HTTP-Sitzungs-Failover nicht einwandfrei funktioniert.
- Wir raten davon ab, mehrere Anmeldungen auf verschiedenen Browser-Registerkarten oder in verschiedenen Browser-Sitzungen auf demselben Host zu verwenden. Bei einigen Browsern werden die Cookies übergreifend über alle Registerkarten und Prozesse verwendet, sodass mehrere Anmeldungen zu Problemen beim HTTP-Sitzungs-Failover führen können (neben dem Risiko einer unbeabsichtigten Authentifizierung, wenn mehrere Benutzer an einem einzigen Computer arbeiten).
- Die Clusterknoten befinden sich im selben Teilnetz.
- Ein Failover-Proxy oder eine Lastausgleichlösung ist auf einem separaten Computer installiert.

Datenbank für Identity Applications

Die Datenbankserver ermöglichen jeweils das Datenbank-Clustering. Wir führen keine offiziellen Tests von Cluster-Datenbankkonfigurationen durch, da das Clustering unabhängig von der Funktionsfähigkeit des Produkts erfolgt. Cluster-Datenbankserver werden daher nur mit den folgenden Warnhinweisen unterstützt:

- Standardmäßig ist die maximale Anzahl der Verbindungen auf 100 festgelegt. Dieser Wert ist möglicherweise zu niedrig, um die Workflow-Anforderungen in einem Cluster zu verarbeiten. Sie sehen möglicherweise die folgenden Ausnahmen:

  ```
  (java.sql.SQLException: Data source rejected establishment of
  connection, message from server: "Too many connections."
  ```

  Legen Sie die Variable `max_connections` in Datei `my.cnf` auf einen höheren Wert fest.

- Unter Umständen müssen einige Funktionen oder Aspekte des Cluster-Datenbankservers deaktiviert werden. Beispielsweise muss die Transaktionsreproduktion in bestimmten Tabellen deaktiviert werden, da beim Einfügen eines doppelten Schlüssels bestimmte Bedingungen verletzt würden.
- NetIQ bietet keine Hilfestellung beim Installieren, Konfigurieren oder Optimieren des Cluster-Datenbankservers. Dies gilt auch für die Installation der NetIQ-Produkte auf einem Cluster-Datenbankserver.
- NetIQ setzt alles daran, mögliche Probleme im Zusammenhang mit der Nutzung von NetIQ-Produkten in einer Cluster-Datenbankumgebung zu beheben. Die Fehlersuchmethoden in einer komplexen Umgebung erfordern häufig eine enge Zusammenarbeit, damit Probleme gelöst werden können. Wir bieten Fachkenntnisse zur Analyse, Planung und Fehlerbehebung von OpenText-Produkten. Der Kunde muss Fachkenntnisse für die Analyse, Planung und Fehlersuche von Drittanbieterprodukten erbringen. Wir bitten die Kunden, die aufgetretenen Probleme zu reproduzieren oder das Verhalten der Komponenten in einer Umgebung ohne Clustering zu reproduzieren, sodass potenzielle Probleme mit der Cluster-Einrichtung von Problemen mit den OpenText-Produkten getrennt werden können.

Vorbereiten eines Clusters für Identity Applications

Identity Applications unterstützen HTTP-Sitzungsreproduktion und Sitzungs-Failover. Wenn bei einem Knoten, auf dem eine Sitzung läuft, eine Fehlfunktion auftritt, wird die Sitzung auf einem anderen Server im Cluster fortgesetzt, ohne dass der Benutzer eingreifen müsste. Bevor Sie Identity Applications in einem Cluster installieren, bereiten Sie die Umgebung vor.

- „Erläuterungen zu Clustergruppen in Tomcat-Umgebungen“, auf Seite 237
- „Festlegen der Systemeigenschaften für Workflow-Engine-IDs“, auf Seite 237
- „Verwenden eines einzigen Master-Schlüssels für alle Benutzeranwendungen im Cluster“, auf Seite 238

Erläuterungen zu Clustergruppen in Tomcat-Umgebungen

Die Benutzeranwendungs-Clustergruppe nutzt einen UUID-Namen, sodass das Risiko von Konflikten mit anderen Cluster-Gruppen, die die Benutzer ggf. zu ihren Servern hinzufügen, minimiert wird. Sie können die Konfigurationseinstellungen für die Benutzeranwendungs-Clustergruppe mit den Benutzeranwendungsverwaltungsfunktionen bearbeiten. Änderungen der Clusterkonfiguration für einen Serverknoten werden erst nach einem Neustart dieses Knotens wirksam.

Festlegen der Systemeigenschaften für Workflow-Engine-IDs

Auf jedem Server im Cluster, auf dem Identity Applications gehostet werden, kann eine Workflow-Engine ausgeführt werden. Damit der Cluster und die Workflow-Engine die größtmögliche Leistung erbringen, sollte jeder Server im Cluster denselben Partitionsnamen und dieselbe Partitions-UDP-

Gruppe verwenden. Außerdem muss jeder Server im Cluster mit einer eindeutigen ID für die Workflow-Engine gestartet werden, da das Clustering für die Workflow-Engine unabhängig vom Cache-Rahmenwerk der Identity Applications erfolgt.

Legen Sie die Systemeigenschaften für Tomcat fest, damit die Workflow-Engines ordnungsgemäß ausgeführt werden.

1. Erstellen Sie für jeden Identity Applications-Server im Cluster jeweils eine neue JVM-Systemeigenschaft.
2. Geben Sie der Systemeigenschaft den Namen `com.novell.afw.wf.`*`Engine-ID`*; die Engine-ID muss dabei eindeutig sein.

Verwenden eines einzigen Master-Schlüssels für alle Benutzeranwendungen im Cluster

Identity Applications verschlüsseln vertrauliche Daten mit einem Master-Schlüssel. Alle Identity Applications in einem Cluster müssen denselben Master-Schlüssel verwenden. In diesem Abschnitt wird beschrieben, wie Sie sicherstellen, dass alle Identity Applications in einem Cluster denselben Master-Schlüssel verwenden.

Weitere Informationen zum Verschlüsseln vertraulicher Daten in Identity Applications finden Sie unter Verschlüsseln vertraulicher Identity Applications-Daten im *OpenText™ Identity Manager CE 24.4 (v4.10) – Administratorhandbuch zu Identity Applications*.

1. Installieren Sie die Benutzeranwendung auf dem ersten Knoten im Cluster.
2. Beachten Sie im Fenster „Sicherheit – Master-Schlüssel“ des Installationsprogramms den Speicherort der Datei `master-key.txt`, die den neuen Master-Schlüssel für Identity Applications enthält. Standardmäßig befindet sich diese Datei im Installationsverzeichnis.
3. Installieren Sie Identity Applications auf den anderen Knoten im Cluster.
4. Klicken Sie im Fenster „Sicherheit – Master-Schlüssel“ auf **Ja** und dann auf **Weiter**.
5. Kopieren Sie im Fenster „Master-Schlüssel importieren“ den Master-Schlüssel aus der Textdatei, die Sie in Schritt 2 erstellt haben.

23 Beispiellösung für eine Identity Manager-Clusterbereitstellung

In diesem Anhang finden Sie schrittweise Anleitungen zum Konfigurieren von OpenText Identity Manager in einer Cluster-Umgebung auf einer Plattform mit Windows 2016.

- „Voraussetzungen“, auf Seite 239
- „Konfigurieren von OpenText Identity Manager in einem OpenText eDirectory-Cluster“, auf Seite 239
- „Clustering für Remote Loader“, auf Seite 240

Voraussetzungen

Identity Vault 9.3 wird in einer Clusterumgebung unter Windows 2016 ausgeführt. Weitere Informationen zum Einrichten eines eDirectory-Clusters finden Sie unter Clustering von eDirectory-Diensten unter Windows (https://www.netiq.com/documentation/edirectory-93/edir_install/data/bnevye9.html) im *OpenText eDirectory-Installationshandbuch (https://www.netiq.com/documentation/edirectory-93/edir_install/data/bookinfo.html)*.

HINWEIS: Das Identitätsdepot unterstützt keinen Lastausgleich mit mehreren Clusterknoten. OpenText eDirectory-Cluster dienen einzig als Failover.

Konfigurieren von OpenText Identity Manager in einem OpenText eDirectory-Cluster

In diesem Abschnitt wird vorausgesetzt, dass Sie bereits einen OpenText eDirectory-Cluster eingerichtet haben.

Konfigurieren Sie OpenText Identity Manager mit dem nachfolgenden Verfahren in einer OpenText eDirectory-Cluster-Umgebung.

1. Stellen Sie im **Cluster Manager** die Priorität der OpenText eDirectory-Clusterrollen auf dem primären Knoten auf **Kein Autostart** ein.
2. Halten Sie den sekundären Knoten an.
3. Installieren Sie die OpenText Identity Manager-Engine auf dem primären Knoten. Aktivieren Sie hierzu im OpenText Identity Manager-Installationsassistenten die Option **Metaverzeichnis-Server**.

   WICHTIG: Die OpenText Identity Manager-Engine muss im lokalen Speicher installiert werden.

   ---

4 Der OpenText Identity Manager-Installationsassistent hält die OpenText eDirectory-Clusterrolle während der Installation an. Wenn diese Rolle angehalten ist, wird sie unter Umständen als fehlerhaft gemeldet. Starten Sie die OpenText eDirectory-Clusterrolle nach der Installation über den **Cluster Manager**.

5 Legen Sie die erforderliche Priorität für die OpenText eDirectory-Clusterrolle fest und aktivieren Sie den sekundären Knoten.

6 Installieren Sie die OpenText Identity Manager-Engine mit dem Befehl `DCLUSTER_INSTALL` auf einem sekundären Knoten.

Beispiel: `idm_install.exe -DCLUSTER_INSTALL="true"`

Clustering für Remote Loader

1 Installieren Sie den Remote Loader auf dem primären und dem sekundären Clusterknoten.

HINWEIS: Der Remote Loader muss auf dem primären und dem sekundären Clusterknoten jeweils in demselben freigegebenen Speicherpfad installiert werden.

---

2 (Bedingt) Wenn die sichere Kommunikation für den Remote Loader gilt, speichern Sie alle SSL-Zertifikate in einem freigegebenen Speicher.

3 Bevor Sie die Remote Loader-Clusterrolle erstellen, öffnen Sie die Remote Loader-Konsole und wählen Sie **Remote Loader als Windows-Dienst**.

4 Erstellen Sie unter **Cluster Manager > Rollen** eine neue Remote Loader-Clusterrolle.

Geben Sie die folgenden Informationen für die Rolle an:

Rollentyp: Generischer Dienst

Dienst auswählen: Remote Loader-Instanz (als Windows-Dienst registriert)

Name: Name der Clusterrolle

Adresse: Eindeutige IP-Adresse

Speicher auswählen: Freigegebener Clusterspeicher

Registrierungseinstellungen replizieren

1. `HKEY_LOCAL_MACHINE\SOFTWARE\Novell\RLConsole`
2. `HKEY_LOCAL_MACHINE\SOFTWARE\Novell\DirXML Remote Loader\Command port 8000`

   Geben Sie den Registrierungspfad der Remote Loader-Instanz an, die in den Cluster aufgenommen werden soll.
3. `HKEY_LOCAL_MACHINE\SOFTWARE\Novell\PassSync`

HINWEIS

- Standardmäßig nimmt jede Clusterrolle nur genau einen Windows-Dienst an. Geben Sie daher für jede Remote Loader-Instanz jeweils einen eindeutigen Befehlsport und einen zugehörigen Registrierungspfad an.
- Der Passwortfilter des Active Directory-Treibers wird in einem Windows-Cluster nicht unterstützt.

---

24 Beispiellösung für eine Identity Applications-Clusterbereitstellung

In diesem Abschnitt finden Sie Anweisungen zum Konfigurieren der Identity Applications in einer Clusterumgebung auf dem Tomcat-Anwendungsserver mit einer Beispielbereitstellung.

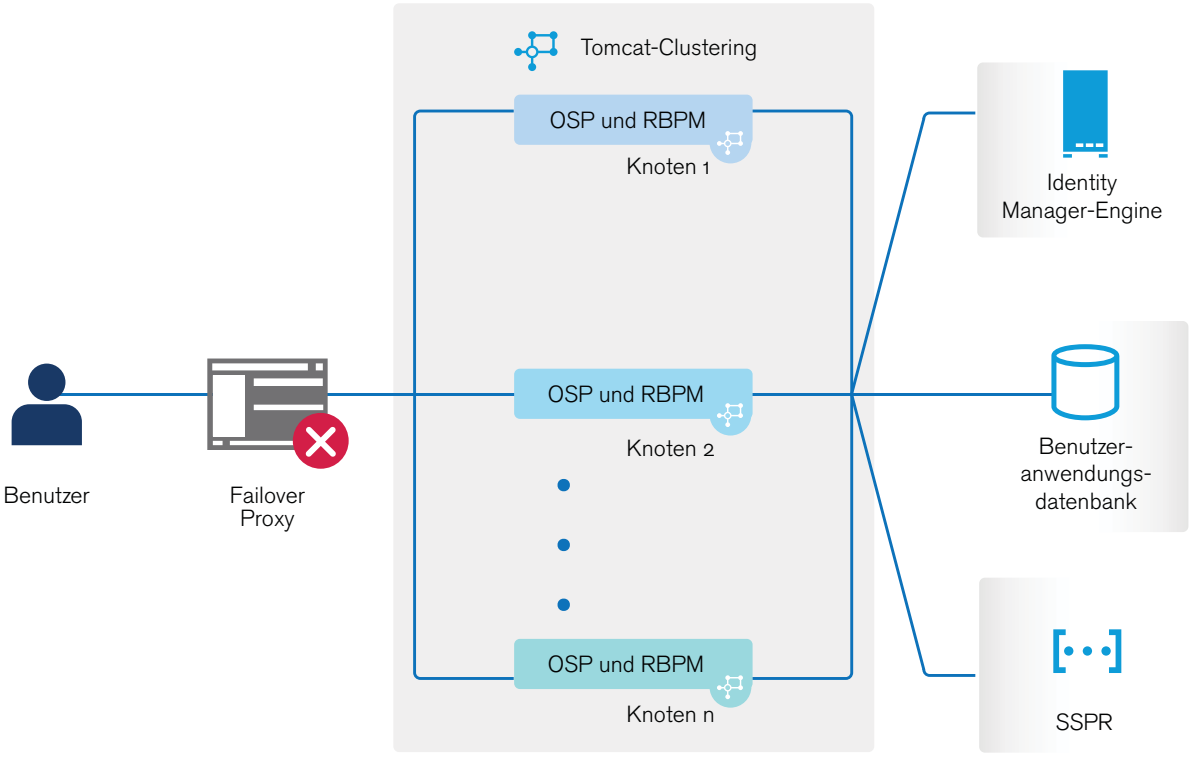
Zum Aufbau eines Clusters müssen verschiedene Tomcat-Instanzen (Knoten) gruppiert werden. Wenn ein aktiver Server ausfällt, sind Identity Applications über andere Clusterknoten zugänglich. Für ein Failover erstellen Sie einen Cluster der Identity Applications und konfigurieren diese so, dass sie als einzelner Server fungieren. Diese Konfiguration enthält jedoch nicht Identity Reporting.

Es wird empfohlen, eine Lastausgleichsoftware zu verwenden, um alle Benutzeranforderungen zu verarbeiten und diese den Serverknoten im Cluster zuzustellen. Das Lastausgleichprogramm ist normalerweise Teil des Clusters. Es versteht sowohl die Clusterkonfiguration als auch die Failover-Richtlinien. Wählen Sie eine Lösung aus, die sich am besten für Sie eignet.

Abbildung 24-1 zeigt ein Beispiel einer Bereitstellung mit einem Zwei-Knoten-Cluster mit den folgenden Annahmen:

- Die gesamte Kommunikation wird über das Lastausgleichprogramm weitergeleitet.
- Komponenten wie die Identity Manager-Engine und die Benutzeranwendung sind auf separaten Servern installiert. Dies ist der empfohlene Ansatz für eine Bereitstellung auf Produktionsebene.
- Sie sind bereits vertraut mit dem Installationsverfahren für OpenText eDirectory, die Identity Manager-Engine, Identity Applications, den Apache Tomcat-Anwendungsserver und die Datenbanken für die Benutzeranwendung.
- OSP (One Single-Sign On Provider) und die Benutzeranwendung sind auf demselben Clusterknoten installiert. OSP kann jedoch auch auf einem anderen Server in der Produktionsumgebung installiert werden. In diesem Fall müssen Sie einige Änderungen an der Konfiguration durchführen. Diese finden Sie in „Installationsvorgang“, auf Seite 243.
- SSPR (Single Sign-On Password Reset) wird auf separaten Computern installiert. Dies ist der empfohlene Ansatz für eine Bereitstellung auf Produktionsebene.
- PostgreSQL wird als Datenbank für die Benutzeranwendung verwendet. Alle anderen Datenbanken, die von Identity Manager 4.10 unterstützt werden – wie Oracle, SQL-Server oder PostgreSQL – eignen sich jedoch genauso gut dafür.
- Alle Benutzeranwendungsknoten kommunizieren mit derselben Instanz von OpenText eDirectory und der Datenbank mit der Benutzeranwendung. Die Anzahl der Benutzeranwendungsinstanzen kann je nach Bedarf erhöht werden.

Abbildung 24-1 *Beispiellösung für eine Clusterbereitstellung*



HINWEIS: Ein Cluster mit zwei Knoten bildet die Mindestkonfiguration für die Hochverfügbarkeit. Die in diesem Abschnitt beschriebenen Konzepte können jedoch leicht zu einem Cluster mit weiteren Knoten erweitert werden.

Zum besseren Verständnis der schrittweisen Konfiguration verweisen wir in den folgenden Abschnitten des Dokuments auf diese Beispielbereitstellung.

Voraussetzungen

- Zwei Server mit Windows Server 2022, Windows Server 2022 R2 oder Windows Server 2016 für die Knoten.
- Installationen von Identity Manager-Komponenten mit Version 4.10 oder höher. Informationen zum Aufrüsten auf OpenText Identity Manager 4.10 finden Sie im Kapitel 16, „Aufrüsten der OpenText Identity Manager-Komponenten“, auf Seite 167.
- Alle Knoten müssen dieselben Anwendungsserver-Zeit aufweisen. Am einfachsten stellen Sie dies sicher, indem Sie die Knoten so konfigurieren, dass sie dieselben Netzwerkzeitserver zur Zeitsynchronisierung über NTP verwenden.
- Die Clusterknoten befinden sich im selben Teilnetz.
- Ein Failover-Proxy oder eine Lastausgleichlösung ist auf einem separaten Computer installiert.
- Um ein Clustering für Formulare zu erreichen, starten Sie zwei Instanzen des Lastausgleichsprogramms auf dem Server – eine für Identity Applications und eine für den Formular-Renderer.

Installationsvorgang

In diesem Abschnitt finden Sie schrittweise Anleitungen zum Installieren einer neuen Instanz der Identity Applications auf Tomcat und der anschließenden Konfiguration für ein Clustering.

1. Installieren Sie die OpenText Identity Manager-Engine. Schrittweise Anleitungen finden Sie unter „Installationsverfahren“, auf Seite 46. Für eine Bereitstellung auf Produktionsebene empfiehlt es sich, die Identity Manager-Engine auf einem separaten Server zu installieren.
2. Erstellen Sie die folgenden Treiber und stellen Sie sie für Identity Applications bereit:
   - Benutzeranwendungstreiber
   - Rollen- und Ressourcenservice-Treiber
3. Installieren Sie die folgenden Identity Manager-Komponenten auf Knoten1:
   a. Benutzeranwendung

      Konfigurieren Sie die folgenden Einstellungen während des Installationsvorgangs:

      i. Wählen Sie **Tomcat** als Anwendungsserver aus.

      ii. Wählen Sie **PostgreSQL** als Datenbankplattform aus.

      HINWEIS: Es ist möglich, eine der von OpenText Identity Manager 4.10 unterstützten Datenbanken zu verwenden.

      ---

      iii. Geben Sie die erforderlichen Datenbankdetails auf den folgenden Seiten an.

      iv. Kopieren Sie die JAR-Datei mit dem Datenbanktreiber (`postgresql-42.6.1-.jar`) vom PostgreSQL-Server auf alle Benutzeranwendungsknoten im Cluster.

      HINWEIS: Wenn Sie andere von Identity Manager 4.10 unterstützte Datenbanken wie Oracle oder SQL Server verwenden, müssen Sie die entsprechenden JAR-Dateien mit dem Treiber vom Server, auf dem die Datenbank installiert ist, auf alle Benutzeranwendungsknoten im Cluster kopieren. Weitere Informationen finden Sie unter „Konfigurieren der Datenbank für Identity Applications“, auf Seite 71.

      ---

      v. Suchen Sie die kopierte JAR-Datei mit dem Datenbanktreiber und wählen Sie sie aus.

      vi. Wählen Sie in den Details der Seite "Neue Datenbank" oder "Vorhandene Datenbank" die Option **Neue Datenbank** aus.

      vii. Geben Sie auf der Seite "Identity Manager-Konfiguration" einen eindeutigen Namen im Feld **Workflow-Engine-ID** an. Beispiel: Der eindeutige Name kann Engine1 für Knoten1 lauten.

      viii. Wählen Sie auf der Seite "Sicherheit – Master-Schlüssel die Option **Nein** aus, um einen neuen Master-Schlüssel zu erstellen.

      Identity Applications verschlüsseln vertrauliche Daten mit einem Master-Schlüssel. Da es sich hierbei um die erste Instanz der Identity Applications in einem Cluster handelt, müssen Sie das Installationsprogramm anweisen, einen neuen Master-Schlüssel zu erstellen. Wählen Sie hierzu **Nein** aus. In einem Cluster muss für das Benutzeranwendungs-Clustering jede Instanz der Benutzeranwendung denselben Master-Schlüssel verwenden. Wählen Sie während der Konfiguration dieser Instanzen die Option **Ja** aus. Dadurch wird der vorhandene Schlüssel importiert und es wird immer derselbe Master-Schlüssel verwendet.

4. Führen Sie in Knoten2 die folgenden Schritte durch:
    a. Installieren Sie Tomcat mit einem Installationsprogramm Ihrer Wahl (wählen Sie während des Installationsvorgangs nur Tomcat aus).
    b. Installieren Sie OSP.

       Geben Sie während des Installationsvorgangs die IP-Adresse und Portnummer des Identity Manager-Engine(OpenText eDirectory)-Servers auf der Seite mit den Authentifizierungsdetails an.
    c. Installieren Sie die Benutzeranwendung.

       Konfigurieren Sie die folgenden Einstellungen während des Installationsvorgangs:
        i. Wählen Sie **Tomcat** als Anwendungsserver aus.
        ii. Wählen Sie **PostgreSQL** als Datenbankplattform aus.

        HINWEIS: Es ist möglich, eine der von OpenText Identity Manager 4.10 unterstützten Datenbanken zu verwenden.

        iii. Geben Sie auf den folgenden Seiten während des Installationsvorgangs die erforderlichen Datenbankdetails an.
        iv. Kopieren Sie die JAR-Datei mit dem Datenbanktreiber (`postgresql-42.6.1-.jar`) vom PostgreSQL-Server zu Knoten2.

        HINWEIS: Wenn Sie eine andere von Identity Manager 4.10 unterstützte Datenbank wie Oracle oder SQL Server verwenden, müssen Sie die entsprechenden JAR-Dateien mit dem Treiber vom Server, auf der die Datenbank installiert ist, auf alle Benutzeranwendungsknoten im Cluster kopieren.

        v. Suchen Sie die kopierte JAR-Datei mit dem Datenbanktreiber und wählen Sie sie aus.
        vi. Wählen Sie in den Details der Seite "Neue Datenbank" oder "Vorhandene Datenbank" die Option **Vorhandene Datenbank** aus.
        vii. Geben Sie auf der Seite "Identity Manager-Konfiguration" einen eindeutigen Namen im Feld **Workflow-Engine-ID** an. Beispiel: Der eindeutige Name kann Engine2 für Knoten2 lauten.
        viii. Wählen Sie zum Erstellen eines neuen Master-Schlüssels auf der Seite "Sicherheit – Master-Schlüssel" die Option **Ja** aus.

        Für das Benutzeranwendungs-Clustering muss jede Instanz der Benutzeranwendung denselben Master-Schlüssel verwenden. Wählen Sie die Option **Ja** aus. Dadurch wird der vorhandene Schlüssel importiert und es wird immer derselbe Master-Schlüssel verwendet. Dieser Schlüssel wird erstellt, wenn Sie die erste Instanz der Benutzeranwendung in Knoten1 installiert haben.

        Den Masterschlüssel erhalten Sie in der Datei „ism-configuration properties“, die sich unter `C:\NetIQ\IDM\apps\tomcat\conf` in Knoten1 befindet. Der Parameter mit dem Master-Schlüssel lautet `com.novell.idm.masterkey`.
        ix. Klicken Sie auf **Installieren**, um die Installation abzuschließen.

HINWEIS: Detaillierte Informationen zum Installieren von Identity Applications finden Sie unter „Installationsverfahren“, auf Seite 46.

5. Starten Sie auf dem Lastausgleichsprogramm-Server eine Instanz des Lastausgleichsprogramms mit der Portnummer für Identity Applications und eine weitere Instanz des Lastausgleichsprogramms mit der Portnummer des Formular-Renderers für alle Cluster-Knoten. Beispiel:
   - `./balance 8543 apps1-au.edu.in:8543 ! apps2-au.edu.in:8543`
   - `./balance 8600 apps1-au.edu.in:8600 ! apps2-au.edu.in:8600`
6. Installieren Sie SSPR auf einem separaten Computer.

   Notieren Sie sich vor der Installation die folgenden Einstellungen und geben Sie diese während des Installationsvorgangs an:

   a. Installieren Sie **Tomcat**. Installationsanleitungen finden Sie in Schritt 4a.

   b. Installieren Sie **SSPR**.

      Führen Sie während der SSPR-Installation die folgenden Schritte durch:

      i. Wählen Sie auf der Seite "Anwendungsserver-Verbindung" die Option **Connect to external authentication server** (Mit externem Authentifizierungsserver verbinden) und geben Sie den DNS-Namen des Servers an, auf dem das Lastausgleichprogramm installiert ist.

      ii. Geben Sie auf der Seite "Authentifizierungsdetails" die **IP-Adresse** und den **Port** des Identity Manager-Engine-Servers an. Das Passwort für die Zertifikate der Zertifizierungsstelle lautet `changeit`.

   c. Wenn die Installation abgeschlossen ist, starten Sie SSPR (`https://<IP>:<Port>/sspr/private/config/ConfigEditor`) und melden Sie sich an. Klicken Sie auf **Konfigurationseditor** > **Einstellungen** > **Sicherheit** > **Whitelist-URL für die Umleitung**.

      i. Klicken Sie auf **Wert hinzufügen** und geben Sie die folgende URL an:

      `https:<DNS_für_Failover><port>/osp`

      ii. Speichern Sie die Änderungen.

      iii. Klicken Sie auf der Seite "SSPR-Konfiguration" auf **Einstellungen** > **OAuth-SSO** und bearbeiten Sie die OSP-Links; ersetzen Sie dazu die IP-Adressen durch den DNS-Namen des Servers, auf dem die Lastausgleichsoftware installiert ist.

      iv. Klicken Sie auf **Einstellungen** > **Anwendung** und aktualisieren Sie die Weiterleitungs- und Abmeldungs-URLs; ersetzen Sie dazu die IP-Adressen durch den DNS-Namen des Servers, auf dem die Lastausgleichsoftware installiert ist.

   d. Starten Sie zur Aktualisierung der SSPR-Informationen auf Knoten1 das Konfigurationsprogramm unter `C:\NetIQ\idm\apps\UserApplication\configupdate.bat`.

      Klicken Sie im Fenster, das sich nun öffnet, auf **SSO-Clients** > **Self Service Password Reset** und geben Sie die Werte für die Parameter **Client-ID**, **Passwort** und **OSP Auth redirect URL** (URL zur Umleitung der OSP-Authentifizierung) ein.

HINWEIS: Vergewissern Sie sich, dass die Werte für diese Parameter in Knoten2 aktualisiert werden.

---

7. Führen Sie die folgenden Konfigurationsaufgaben in den Clusterknoten durch:

   a. Starten Sie Tomcat in allen Clusterknoten neu.

b. Weitere Informationen zum Link „Passwort ändern“ finden Sie in „Aktualisieren der SSPR-Links im Dashboard für eine dezentrale Umgebung oder eine Cluster-Umgebung“, auf Seite 71.

c. Überprüfen Sie, ob die Links „Passwort vergessen“ und „Passwort ändern“ mit der SSPR-IP-Adresse in Knoten2 aktualisiert sind.

HINWEIS: Wenn die Links „Passwort vergessen“ und „Passwort ändern“ bereits mit der SSPR-IP-Adresse aktualisiert sind, brauchen Sie keine Änderungen vorzunehmen.

---

8. Stoppen Sie Tomcat in Knoten1 und generieren Sie eine neue `osp.jks`-Datei. Geben Sie dazu den DNS-Namen des Lastausgleichservers an und führen Sie den folgenden Befehl aus:

   ```
   C:\NetIQ\Common\JRE\bin\keytool -genkey -keyalg RSA -keysize 2048 -keystore osp.jks -storepass <Passwort> -keypass <Passwort> -alias osp -validity 1800 -dname "cn=<IP/DNS_des_Lastausgleichprogramms>"
   ```

   Beispiel: `C:NetIQ\idm\apps\jre\bin\ -genkey -keyalg RSA -keysize 2048 -keystore osp.jks -storepass changeit -keypass changeit -alias osp -validity 1800 -dname "cn=mydnsname"`

   HINWEIS: Das Schlüsselpasswort muss dasselbe sein wie das während der OSP-Installation angegebene Passwort. Alternativ kann dies auch mit dem Konfigurationsaktualisierungsprogramm und dem Keystore-Passwort geändert werden.

   ---

9. (Bedingt) Führen Sie folgenden Befehl aus, um zu überprüfen, ob die `osp.jks`-Datei mit den Änderungen aktualisiert wurde:

   ```
   C:\NetIQ\Common\JRE\bin\keytool -list -v -keystore osp.jks -storepass changeit
   ```

10. Sichern Sie die ursprüngliche `osp.jks`-Datei, die sich unter `C:\NetIQ\idm\apps\osp` befindet, und kopieren Sie die neue `osp.jks`-Datei an diesen Speicherort. Die neue `osp.jks`-Datei wurde in Schritt 8 erstellt.

11. Kopieren Sie die neue `osp.jks`-Datei in Knoten1 in alle anderen Benutzeranwendungsknoten im Cluster.

12. Für jeden Knoten im Cluster:

    a. Navigieren Sie zum Verzeichnis `C:\netiq\idm\apps\sites` und bearbeiten Sie die Datei `ServiceRegistry.json`, um Details für das Lastausgleichsprogramm hinzuzufügen.

       ```
       {"serviceRegisteries":[{"serviceID":"IDM","restUrl":"https://<DNS of the load balancer>:8543/IDMProv"}]}
       ```

    b. Navigieren Sie zum Verzeichnis `C:\netiq\idm\apps\sites\` und bearbeiten Sie die Datei `config.ini`, um DNS und Portnummer für das Lastausgleichprogramm hinzuzufügen.

       ```
       OSPIssuerUrl=https://<DNS of the load balancer>:8543/osp/a/idm/auth/oauth2
       OSPRedirectUrl=https://<DNS of the load balancer>:8600/forms/oauth.html
       ClientID=forms
       OSPLogoutUrl=https://<DNS of the load balancer>:8543/osp/a/idm/auth/app/logout
       ```

13. Starten Sie das Konfigurationsprogramm in Knoten1 und ändern Sie alle URL-Einstellungen wie den URL-Link zur Landeseite und die OAuth-Umleitungs-URL zum DNS-Namen des Lastausgleichprogramms auf der Registerkarte „SSO-Client“.

    a. Speichern Sie die Änderungen im Konfigurationsprogramm. Überprüfen Sie die Datei `ism-configuration properties` auf Änderungen und ändern Sie sie, falls URLs immer noch auf den DNS und Port von Knoten 1 zeigen.

    b. Um diese Änderung widerzuspiegeln, kopieren Sie die Datei `ism-configuration properties` unter `C:\NetIQ\IDM\apps\tomcat\conf` von Knoten1 in alle anderen Benutzeranwendungsknoten im Cluster.

    HINWEIS: Sie haben die Datei `ism.properties` von Knoten1 in alle anderen Knoten im Cluster kopiert. Wenn Sie bei der Installation der Benutzeranwendung Pfade angegeben haben, müssen Sie dafür sorgen, dass die entsprechenden Pfade korrigiert werden; verwenden Sie dazu das Konfigurationsaktualisierungsprogramm in den Clusterknoten.

    In diesem Szenario sind OSP und die Benutzeranwendung auf demselben Server installiert; daher wird für die Umleitungs-URLs derselbe DNS-Name verwendet.

    Wenn OSP und Benutzeranwendung auf verschiedenen Servern installiert sind, müssen Sie die OSP-URLs zu einem anderen DNS-Namen ändern, der auf das Lastausgleichprogramm verweist. Wiederholen Sie dies für alle Server, auf denen OSP installiert ist. Dadurch werden alle OSP-Anforderungen über das Lastausgleichprogramm an den DNS-Namen des OSP-Clusters zugestellt. Dazu muss für OSP-Knoten ein separater Cluster vorhanden sein.

    ---

14. Führen Sie die folgenden Schritte in der Datei `setenv.sh` im Verzeichnis `/TOMCAT_INSTALLED_HOME/bin/` durch:

    a. Für ein erfolgreiches `mcast_addr`-Binding muss für JGroups die Eigenschaft `preferIPv4Stack` auf **true** festgelegt sein. Fügen Sie dazu die JVM-Eigenschaft "-Djava.net.preferIPv4Stack=true” in Datei `setenv.sh` in allen Knoten hinzu.

    b. Fügen Sie "`-Dcom.novell.afw.wf.Engine-id=Engine1`" in Knoten1 der `setenv.sh`-Datei hinzu. Fügen Sie entsprechend einen eindeutigen Engine-Namen für jeden Knoten im Cluster hinzu. Beispiel: Für Knoten2 fügen Sie den Engine-Namen als Engine2 hinzu.

15. Aktivieren Sie das Clustering in der Benutzeranwendung.

    a. Starten Sie Tomcat in Knoten1.

    Starten Sie keine anderen Server.

    b. Melden Sie sich bei der Benutzeranwendung als Administrator der Benutzeranwendung an.

    c. Klicken Sie auf **Konfiguration** > **Caching und Cluster**.

    Die Benutzeranwendung zeigt die Seite „Cache-Management“ an.

    d. Klicken Sie auf **Cluster-Cache-Konfiguration** und wählen Sie für die Eigenschaft **Clusterfähig** die Option **Wahr** aus.

    e. Klicken Sie auf **Speichern**.

    f. Starten Sie Tomcat neu.

HINWEIS: Wenn Sie "Lokale Einstellungen aktivieren" ausgewählt haben, wiederholen Sie diesen Vorgang für jeden Server im Cluster.

Der Benutzeranwendungscluster verwendet JGroups für die Cache-Synchronisierung in allen Knoten mit der Standard UDP. Falls Sie lieber TCP anstatt dieses Protokolls verwenden möchten, finden Sie die entsprechenden Anleitungen unter Konfigurieren der Benutzeranwendung zur Verwendung von TCP (https://www.netiq.com/documentation/idm45/agpro/data/b6iiw3v.html).

16. Aktivieren Sie den Berechtigungsindex für das Clustering. Weitere Informationen hierzu finden Sie im „Aktivieren des Berechtigungsindex für das Clustering“, auf Seite 249.
17. Aktivieren Sie den Tomcat-Cluster.

    Öffnen Sie die Tomcat `server.xml` -Datei unter `/TOMCAT_INSTALLED_HOME/conf/` und kommentieren Sie diese Zeile in dieser Datei in allen Clusterknoten aus:

    ```
    <Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>
    ```

    Zur erweiterten Tomcat-Clusterkonfiguration beachten Sie die Schritte auf der Dokumentationswebsite zu Apache .
18. Starten Sie Tomcat in allen Knoten neu.
19. Konfigurieren Sie den Benutzeranwendungstreiber für das Clustering.

    In einer geclusterten Umgebung wird ein einzelner Benutzeranwendungstreiber mit mehreren Instanzen der Benutzeranwendung verwendet. Der Treiber speichert verschiedene anwendungsspezifische Informationen (z. B. die Workflow-Konfiguration und Clusterinformationen). Sie müssen den Treiber so konfigurieren, dass er den Hostnamen oder die IP-Adresse des Dispatchers oder Lastausgleichprogramms für den Cluster verwendet.

    a. Melden Sie sich bei der Instanz der OpenText Identity Console an, die Ihr Identitätsdepot verwaltet.
    b. Wählen Sie unter der Kachel " Identity Manager" die Option **OpenText Identity Manager-Verwaltung**.
    c. Wählen Sie den Treibersatz, der Ihren Benutzeranwendungstreiber enthält.
    d. Klicken Sie auf das Treibersymbol.
    e. Gehen Sie zu **Konfiguration**.
    f. Klicken Sie auf die Dropdown-Liste **Treiberparameter**.
    g. Ändern Sie auf der Registerkarte **Treibereinstellungen > Host** zum Hostnamen oder der IP-Adresse des Lastausgleichsprogramms.
    h. Klicken Sie auf **Speichern**.
    i. Starten Sie den Treiber neu.
20. Wiederholen Sie zum Ändern der URL des Rollen- und Ressourcenservice-Treibers die Schritte 19a bis 19f und klicken Sie auf **Treiberkonfiguration**. Aktualisieren Sie die **Benutzeranwendungs-URL** mit dem DNS-Namen des Lastausgleichprogramms.
21. Vergewissern Sie sich, dass die Sitzungstreue für den Cluster aktiviert ist, der in der Lastausgleichsoftware für die Benutzeranwendungsknoten erstellt wurde.

Die meisten Lastausgleichprogramme bieten eine Funktion zur Zustandsprüfung, um herauszufinden, ob ein HTTP-Server aktiv ist und die Überwachung durchführt. Die Benutzeranwendung enthält eine URL, die zum Konfigurieren des HTTP-Server-Zustands auf Ihrem Lastausgleichprogramm verwendet wird. Die URL lautet:

```
http://<Knoten-IP>:port/IDMProv/jsps/healthcheck.jsp
```

Aktivieren des Berechtigungsindex für das Clustering

In diesem Abschnitt finden Sie Anweisungen zur Aktivierung des Berechtigungsindex für das Clustering.

1. Melden Sie sich bei der OpenText Identity Console auf Node1 an und gehen Sie zur **Strukturansicht**.
2. Wählen Sie im linken Bereich der Strukturansicht **System** > **Treibersatz**, der den Benutzeranwendungstreiber enthält.
3. Wählen Sie dann **AppConfig** > **AppDefs**.
4. Wählen Sie im linken Bereich **Konfiguration**.
5. Wählen Sie unter **Bewertete Attribute** das Attribut XMLData und legen Sie die Eigenschaft `com.netiq.idm.cis.clustered` auf **true** fest.

   Beispiel:

   ```
   <Eigenschaft>
   <Schlüssel>com.netiq.idm.cis.clustered</Schlüssel>
   <Wert>true</Wert>
   </Eigenschaft>
   ```
6. Klicken Sie auf **Speichern**.

25 Deinstallieren der OpenText Identity Manager-Komponenten

In diesem Abschnitt wird die Deinstallation der OpenText Identity Manager-Komponenten beschrieben. Bei einigen Komponenten sind gewisse Voraussetzungen für die Deinstallation zu beachten. Lesen Sie jeweils den gesamten Abschnitt für eine Komponente, bevor Sie die Deinstallation starten.

HINWEIS: Vor der Deinstallation der OpenText Identity Manager-Komponenten müssen Sie alle Dienste anhalten, beispielsweise Tomcat, PostgreSQL und ActiveMQ.

Deinstallieren von Identity Reporting

Vor dem Deinstallieren des Identitätsdepots müssen Sie sich über die OpenText eDirectory-Baumstruktur und die Speicherorte der Replikationen informieren. Beispielsweise müssen Sie feststellen, ob sich gleich mehrere Server im Baum befinden.

1 (Bedingt) Wenn der OpenText eDirectory-Baum mehrere Server enthält, führen Sie die folgenden Schritte aus:

   1a (Bedingt) Wenn sich Masterreproduktionen auf dem Server befinden, müssen Sie einen anderen Server in diesem Reproduktionsring zum Master bestimmen, bevor Sie OpenText eDirectory entfernen können.

   Weitere Informationen finden Sie unter „Managing Partitions and Replicas“ (https://www.netiq.com/documentation/edirectory-93/edir_admin/data/a2iiiik.html) (Verwalten von Partitionen und Reproduktionen) im *eDirectory-Administrationshandbuch* (https://www.netiq.com/documentation/edirectory-93/edir_admin/data/bookinfo.html).

   1b (Bedingt) Wenn der Baum auf dem Server, auf dem OpenText eDirectory installiert ist, die einzige Kopie einer Partition enthält, führen Sie entweder diese Partition mit der übergeordneten Partition zusammen, oder kopieren Sie eine Reproduktion dieser Partition auf einen anderen Server, und machen Sie diesen Server zum Masterreproduktionsserver.

   Weitere Informationen finden Sie unter „Managing Partitions and Replicas“ (https://www.netiq.com/documentation/edirectory-93/edir_admin/data/a2iiiik.html) (Verwalten von Partitionen und Reproduktionen) im *OpenText eDirectory-Administrationshandbuch* (https://www.netiq.com/documentation/edirectory-93/edir_admin/data/bookinfo.html).

   1c Führen Sie eine Zustandsüberprüfung der OpenText eDirectory-Datenbank aus. Beheben Sie alle eventuell auftretenden Probleme, bevor Sie den Vorgang fortsetzen.

   Weitere Informationen hierzu finden Sie unter „Keeping eDirectory Healthy“ (https://www.netiq.com/documentation/edirectory-93/edir_admin/data/a5ziqam.html) (Funktionsfähigkeit von OpenText eDirectory aufrechterhalten) im *OpenText eDirectory - Administrationshandbuch* (https://www.netiq.com/documentation/edirectory-93/edir_admin/data/bookinfo.html).

2 Deinstallieren Sie das Identitätsdepot:

Öffnen Sie die Option „Software“ in der Systemsteuerung. Unter Windows Server 2012 R2 klicken Sie beispielsweise auf **Programme und Funktionen**. Klicken Sie mit der rechten Maustaste auf **OpenText eDirectory**, und klicken Sie auf **Deinstallieren**.

3 (Bedingt) Wenn der eDirectory-Baum mehrere Server enthält, führen Sie die folgenden Schritte aus:

3a Löschen Sie alle serverspezifischen Objekte, die noch im Baum verblieben sind.

3b Führen Sie eine weitere Zustandsprüfung durch, damit gewährleistet ist, dass der Server ordnungsgemäß aus dem Baum entfernt wurde.

Weitere Informationen hierzu finden Sie unter „Keeping eDirectory Healthy“ (https://www.netiq.com/documentation/edirectory-93/edir_admin/data/a5ziqam.html) (Funktionsfähigkeit von eDirectory aufrechterhalten) im *eDirectory - Administrationshandbuch* (https://www.netiq.com/documentation/edirectory-93/edir_admin/data/bookinfo.html).

Entfernen von Objekten aus dem Identitätsdepot

Im ersten Schritt der Deinstallation von OpenText Identity Manager müssen alle OpenText Identity Manager-Objekte aus dem Identitätsdepot gelöscht werden. Wenn der Treibersatz erstellt wird, fordert Sie der Assistent dazu auf, eine eigene Partition für den Treibersatz zu erstellen. Wenn ein Treibersatzobjekt auch als Partitionsstammobjekt in eDirectory fungiert, muss die Partition zunächst mit der übergeordneten Partition zusammengeführt werden, bevor Sie das Treibersatzobjekt löschen können.

So entfernen Sie Objekte aus dem Identitätsdepot:

1 Führen Sie eine Zustandsprüfung der eDirectory-Datenbank durch, und beheben Sie alle eventuell aufgetretenen Fehler, bevor Sie den Vorgang fortsetzen.

Weitere Informationen hierzu finden Sie unter „Keeping eDirectory Healthy“ (https://www.netiq.com/documentation/edirectory-93/edir_admin/data/a5ziqam.html) (Funktionsfähigkeit von eDirectory aufrechterhalten) im *eDirectory -Administrationshandbuch* (https://www.netiq.com/documentation/edirectory-93/edir_admin/data/bookinfo.html).

2 Melden Sie sich bei der Identity Console als Administrator mit vollständigen Berechtigungen für den OpenText eDirectory-Baum an.

3 Wählen Sie **Partitionsverwaltung**.

4 Wechseln Sie zum Treibersatzobjekt, das das Root-Objekt der Partition ist, und markieren Sie es. Klicken Sie anschließend auf **OK**.

5 Warten Sie, bis der Zusammenführungsprozess abgeschlossen ist, und klicken Sie anschließend auf **OK**.

6 Löschen Sie das Treibersatzobjekt.

Wenn Sie das Treibersatzobjekt löschen, werden alle mit diesem Treibersatz verknüpften Treiberobjekte gelöscht.

7 Wiederholen Sie Schritt 3 bis Schritt 6 für alle Treibersatzobjekte in der eDirectory-Datenbank, bis alle gelöscht wurden.

8 Wiederholen Sie Schritt 1, damit gewährleistet ist, dass alle Zusammenführungen abgeschlossen sind und alle Objekte gelöscht wurden.

Deinstallieren der OpenText Identity Manager-Engine

Beim Installieren der OpenText Identity Manager-Engine wird ein Deinstallationsskript auf dem OpenText Identity Manager-Server gespeichert. Mithilfe dieses Skripts können Sie alle Dienste, Pakete und Verzeichnisse entfernen, die während der Installation erstellt wurden.

HINWEIS: Bevor Sie die OpenText Identity Manager-Engine deinstallieren können, muss zunächst das Identitätsdepot entsprechend vorbereitet werden. Weitere Informationen finden Sie unter „Entfernen von Objekten aus dem Identitätsdepot“, auf Seite 252.

Auf einem Windows-Server deinstallieren Sie die OpenText Identity Manager-Engine über die Option „Software“ in der Systemsteuerung. Unter Windows 2012 R2 klicken Sie beispielsweise auf **Programme und Funktionen**. Klicken Sie mit der rechten Maustaste auf **OpenText Identity Manager**, und klicken Sie auf **Deinstallieren**.

Deinstallieren von Remote Loader

Beim Installieren des Remote Loader wird ein Deinstallationsskript auf dem OpenText Identity Manager-Server gespeichert. Mithilfe dieses Skripts können Sie alle Dienste, Pakete und Verzeichnisse entfernen, die während der Installation erstellt wurden.

Auf einem Windows-Server deinstallieren Sie den Remote Loader über die Option „Software“ in der Systemsteuerung.

Deinstallieren der Identity Applications

Sie müssen alle Komponenten des rollenbasierten Bereitstellungsmoduls (RBPM) deinstallieren, beispielsweise die Treiber und die Datenbank.

Wenn Sie die mit dem RBPM verknüpften Laufzeitkomponenten deinstallieren müssen, startet das Deinstallationsprogramm den Server automatisch neu, sofern Sie das Deinstallationsprogramm nicht im Automatikmodus unter Windows ausführen. Der Windows-Server muss manuell neu gebootet werden.

HINWEIS: Vor der Deinstallation des RBPM deinstallieren Sie die OpenText Identity Manager-Engine. Weitere Informationen finden Sie unter „Deinstallieren der OpenText Identity Manager-Engine“, auf Seite 253.

Löschen der Treiber für das rollenbasierte Bereitstellungsmodul

Sie können den Benutzeranwendungstreiber und den Rollen- und Ressourcenservice-Treiber wahlweise in Designer oder in der OpenText Identity Console löschen.

1 Halten Sie den Benutzeranwendungstreiber, den Rollen- und den Ressourcenservice-Treiber an. Führen Sie den entsprechenden Vorgang für die verwendete Komponente aus:

- **Designer:** Klicken Sie mit der rechten Maustaste auf die Treiberzeile und klicken Sie anschließend auf **Live > Treiber anhalten**.

- **OpenText Identity Console:** Klicken Sie auf der Seite „Treibersatz-Überblick“ auf die obere rechte Ecke des Treiberabbilds und dann auf **Treiber anhalten**.

2. Löschen Sie den Benutzeranwendungstreiber und den Rollen- und Ressourcenservice-Treiber. Führen Sie den entsprechenden Vorgang für die verwendete Komponente aus:
   - **Designer:** Klicken Sie mit der rechten Maustaste auf die Treiberzeile und wählen Sie **Löschen**.
   - **OpenText Identity Console:** Klicken Sie auf der Seite „Treibersatz-Überblick“ auf **Treiber > Treiber löschen** und dann auf den zu löschenden Treiber.

Deinstallieren der Identity Applications

Sie müssen die Benutzeranwendung und die zugehörige Datenbank von Tomcat deinstallieren. In diesem Verfahren wird das Entfernen der Benutzeranwendung und der zugehörigen Datenbank aus Tomcat und PostgreSQL beschrieben. Wenn Sie einen anderen Anwendungsserver und eine andere Datenbank verwenden, beachten Sie die Dokumentation für diese Produkte.

WICHTIG: Gehen Sie beim Entfernen der Benutzeranwendung vorsichtig vor. Hierbei werden alle Ordner und Dateien aus dem Ordner gelöscht, in dem die Skripte und die unterstützenden installiert wurden. Beim Entfernen der Dateien könnten Sie gleichzeitig unbeabsichtigt Tomcat oder PostgreSQL deinstallieren. Der Name des Deinstallationsordners lautet beispielsweise in der Regel `C:\NetIQ\idm\apps\UserApplication`. Dieser Ordner enthält auch die Ordner für Tomcat und PostgreSQL.

---

1. Melden Sie sich bei dem Server an, auf dem Sie die Benutzeranwendung installiert haben.
2. Öffnen Sie die Option „Software“ in der Systemsteuerung. Unter Windows Server 2012 R2 klicken Sie beispielsweise auf **Programme und Funktionen**.
3. Klicken Sie mit der rechten Maustaste auf **OpenText Identity Manager-Benutzeranwendung**, und klicken Sie auf **Deinstallieren**.

Deinstallieren der Identity Reporting-Komponenten

Die Komponenten von Identity Reporting müssen in der nachstehenden Reihenfolge deinstalliert werden:

1. Löschen Sie die Treiber. Weitere Informationen finden Sie unter „Löschen der Berichterstellungstreiber“, auf Seite 255.
2. Löschen Sie Identity Reporting. Weitere Informationen finden Sie unter „Deinstallieren von Identity Reporting“, auf Seite 255.
3. Löschen Sie Sentinel. Weitere Informationen finden Sie unter Deinstallieren von Sentinel Log Management für IGA im Einrichtungshandbuch zu OpenText™ Identity Manager CE 24.4 (v4.10) für Linux.

HINWEIS: Um Speicherplatz einzusparen, wird mit den Installationsprogrammen für Identity Reporting keine JVM (Java Virtual Machine) installiert. Wenn Sie also eine oder mehrere Komponenten deinstallieren möchten, muss eine JVM im Pfad vorliegen, der in der Variablen PATH definiert ist. Falls ein Fehler bei der Deinstallation auftritt, fügen Sie den Speicherort einer JVM zur lokalen Umgebungsvariablen PATH hinzu, und starten Sie das Deinstallationsprogramm erneut.

Löschen der Berichterstellungstreiber

Sie können mit Designer oder der OpenText Identity Console die Treiber für Datensammlung und verwaltetes System-Gateway löschen.

1. Halten Sie die Treiber an. Führen Sie den entsprechenden Vorgang für die verwendete Komponente aus:
   - **Designer:** Klicken Sie für jeden Treiber jeweils mit der rechten Maustaste auf die Treiberzeile, und klicken Sie dann auf **Live > Treiber anhalten**.
   - **OpenText Identity Console:** Klicken Sie für jeden Treiber auf der Seite „Treibersatz-Überblick“ jeweils auf die obere rechte Ecke des Treiberabbilds und dann auf **Treiber anhalten**.
2. Löschen Sie die Treiber. Führen Sie den entsprechenden Vorgang für die verwendete Komponente aus:
   - **Designer:** Klicken Sie für jeden Treiber jeweils mit der rechten Maustaste auf die Treiberzeile, und klicken Sie dann auf **Löschen**.
   - **OpenText Identity Console:** Klicken Sie auf der Seite „Treibersatz-Überblick“ auf **Treiber > Treiber löschen** und dann auf den zu löschenden Treiber.

Deinstallieren von Identity Reporting

Vor dem Löschen von Identity Reporting müssen zunächst der DCS-Treiber und der MSGW-Treiber gelöscht werden. Weitere Informationen finden Sie unter „Löschen der Berichterstellungstreiber“, auf Seite 255.

WICHTIG: Bevor Sie das Deinstallationsprogramm für Identity Reporting starten, müssen Sie die generierten Berichte aus dem Installationsverzeichnis von Identity Reporting in einen anderen Speicherort auf dem Computer kopieren. Bei der Deinstallation werden alle Dateien und Ordner aus dem Verzeichnis entfernt, in dem die Berichterstellung installiert war. Beispiel: Berichterstellungs-Installationsordner `C:\NetIQ\idm\apps\IDMReporting`.

Öffnen Sie zum Deinstallieren von Identity Reporting die Option „Software“ in der Systemsteuerung. Unter Windows Server 2012 R2 klicken Sie beispielsweise auf **Programme und Funktionen**. Klicken Sie mit der rechten Maustaste auf **Identity Reporting**, und klicken Sie auf **Deinstallieren**.

Deinstallation von Analyzer

WICHTIG: Das Analyzer-Tool ist nicht in der ISO für OpenText Identity Manager 4.10 enthalten. Wenn Analyzer bereits installiert ist, aktualisieren Sie ihn auf Version 4.8.5 und verwenden Sie ihn mit OpenText Identity Manager 4.10.

1. Schließen Sie Analyzer.
2. So deinstallieren Sie Analyzer.

   Öffnen Sie die Option „Software“ in der Systemsteuerung. Unter Windows Server 2008 klicken Sie beispielsweise auf **Programme und Funktionen**. Klicken Sie mit der rechten Maustaste auf **Analyzer für OpenText Identity Manager**, und klicken Sie auf **Deinstallieren**.

Deinstallation von Designer

1. Schließen Sie Designer.
2. Deinstallieren Sie Designer mit dem entsprechenden Verfahren für Ihr Betriebssystem:

   Öffnen Sie die Option „Software“ in der Systemsteuerung. Unter Windows Server 2008 klicken Sie beispielsweise auf **Programme und Funktionen**. Klicken Sie mit der rechten Maustaste auf **Designer für OpenText Identity Manager**, und klicken Sie auf **Deinstallieren**.

26 Fehlerbehebung

In diesem Abschnitt finden Sie nützliche Hinweise für die Fehlersuche, wenn Probleme beim Installieren von OpenText Identity Manager auftreten. Weitere Informationen zur Fehlersuche für OpenText Identity Manager finden Sie im Handbuch der entsprechenden Komponente.

Fehlersuche bei der OpenText Identity Manager-Engine

Die nachfolgende Tabelle enthält die möglichen Probleme und Vorschläge für Gegenmaßnahmen. Falls das Problem weiterhin auftritt, wenden Sie sich an Ihren zuständigen OpenText-Ansprechpartner.

Problem	Empfohlene Vorgehensweise
Die OpenText Identity Manager-Engine kann nicht gestartet werden, wenn der OpenText eDirectory-Initialisierungsprozess im Gange ist. Dieses Problem tritt meist auf, wenn die OpenText eDirectory-DIB sehr groß ist.	Als Behelfslösung führen Sie die folgenden Schritte aus: 1. Erstellen Sie eine Systemumgebungsvariable mit dem Namen **SLEEP_BEFORE_ENGINE_STARTUP** und legen Sie den Wert der Variable von 0 bis 600 fest. Der Wert wird in Sekunden angegeben. **HINWEIS:** Wenn Sie einen ungültigen Wert oder einen Wert größer als 600 eingeben, wird der Wert standardmäßig auf 600 festgelegt. 2. Starten Sie OpenText eDirectory neu. 3. (Bedingt) Überprüfen Sie das `dhost.log`, um die Meldungen und Protokolle einzusehen.
In einer Umgebung mit mehreren Servern wird eine nicht erkannte erweiterte Ausnahme angezeigt.	Vergewissern Sie sich, dass der Primärserver über eine Lese-Schreib-Partition für den Sekundärserver verfügt: 1. Melden Sie sich bei der OpenText Identity Console an. 2. Wählen Sie **Partitionsverwaltung**. 3. Wählen Sie den Sekundärserver aus. 4. Weisen Sie dem Server in der **Reproduktionsansicht** Lese- und Schreibrechte zu. **HINWEIS:** Vergewissern Sie sich, dass Sie den Sekundärserver im Treibersatz hinzugefügt haben.

Fehlersuche bei Identity Applications und der RBPM-Installation

Die nachfolgende Tabelle enthält die möglichen Probleme und Vorschläge für Gegenmaßnahmen. Falls das Problem weiterhin auftritt, wenden Sie sich an Ihren zuständigen OpenText-Ansprechpartner.

Problem	Empfohlene Vorgehensweise
Die Widgets **Rollen** und **Eigene Aufgaben** auf der Dashboard-Seite zeigen keine Daten an. Wenn Sie in der Konsole Ihres Browsers nachsehen, wird ein 404-Fehler angezeigt. Dieses Problem tritt auf, wenn der Standardkontext für die Bereitstellung von `IDMProv` in einen benutzerdefinierten Kontext geändert wird.	Um dieses Problem zu beheben, müssen Sie die REST-API-URL in den betroffenen Widgets ändern. Führen Sie die folgenden Schritte aus: 1. Melden Sie sich im OpenText Identity Manager-Dashboard als Administrator an. 2. Navigieren Sie zur Dashboard-Seite und klicken Sie auf "Dashboard verwalten". 3. So bearbeiten Sie die Widget-Konfiguration im Widget **Rollen**: a. Klicken Sie auf ⚙. b. Ändern Sie im Feld **URL** den standardmäßigen `IDMProv`-Kontext wie folgt:`/<Benutzerdefinierter Kontext>/rest/access/assignments/advanced?nextIndex=1&sortBy=name&sortOrder=ASC&forceRefresh=true&searchScope=role&size=20` Dabei ist `<benutzerdefinierter Kontext>` der Kontext, den Sie in Ihrer OpenText Identity Manager-Bereitstellung verwenden. c. Klicken Sie auf **Anwenden**. 4. So bearbeiten Sie die Widget-Konfiguration im Widget **Eigene Aufgaben**: a. Klicken Sie auf ⚙. b. Ändern Sie im Feld **URL** den standardmäßigen Kontext `IDMProv` wie folgt in einen benutzerdefinierten Kontext:`/<Benutzerdefinierter Kontext>/rest/access/tasks/list?fromIndex=1&size=10&q=*&sortOrder=asc&sortBy=createTime&assignedTo=assignedTo&recipient=recipientAsMe&expireUnit=weeks&expireWithin=&proxyUser=&assignStatus=&delegatedTasks=false&status=` c. Klicken Sie auf **Anwenden**. 5. Klicken Sie auf **Bearbeitung fertiggestellt**.

Problem	Empfohlene Vorgehensweise
Wenn die in einem Cluster installierten Identity Applications aktualisiert werden und Tomcat neu gestartet wird, funktioniert das Clustering nicht wie erwartet.	Führen Sie in allen Knoten des Clusters folgende Vorgänge aus: 1. Navigieren Sie zur Datei `server.xml` im Ordner `C:\NetIQ\IDM\apps\tomcat\conf`. 2. Heben Sie den Kommentar für die folgende Zeile in der Datei `server.xml` auf. `<Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>` 3. Stellen Sie alle benutzerdefinierten Konfigurationen aus dem gesicherten Tomcat-Verzeichnis wieder her. 4. Starten Sie Tomcat neu.
Bei der Aufrüstung wird das Standardadministratorkonto für Identity Applications nicht als `cn=uaadmin.ou=sa.o=data` festgelegt. In der Datei `catalina.out` wird der folgende Fehler protokolliert. `AuthorizationManagerService [RBPM] Error occured calculating effective rights for attribute: nrfAccessMgrRevokeRole on object: cn=complianceAdmin,cn=System,cn=Level20,cn=RoleDefs,cn=RoleConfig,cn=AppConfig,cn=UserApplication,cn=Driver Set,o=system for trustee: cn=uaadmin,ou=sa,o=data.com.novell.srvprv.spi.security.IDMAuthorizationException: Error occured calculating effective rights for attribute: nrfAccessMgrRevokeRole on object: cn=complianceAdmin,cn=System,cn=Level20,cn=RoleDefs,cn=RoleConfig,cn=AppConfig,cn=UserApplication,cn=Driver Set,o=system for trustee: cn=uaadmin,ou=sa,o=data.at com.novell.idm.security.authorization.ldap.LdapRightsUtil.getPropertyRights(LdapRightsUtil.java:152)` `Unable to fetch roles from edirectory in the predefined time set.`	1. Navigieren Sie zur Datei `setenv.bat` und ändern Sie den Wert der Eigenschaft `-Dncpclient_req_timeout` im Eintrag `CATALINA_OPTS` in *1150*. 2. Starten Sie Tomcat neu.

Problem	Empfohlene Vorgehensweise
Sie möchten eine oder mehrere Konfigurationseinstellungen für Identity Applications ändern, die Sie während der Installation vorgenommen haben: ◆ Identitätsdepot-Verbindungen und -Zertifikate ◆ Email-Einstellungen ◆ Benutzeridentität und Benutzergruppen in der OpenText Identity Manager-Engine ◆ Access Manager- oder iChain-Einstellungen	Das Dienstprogramm für die Konfiguration kann unabhängig vom Installationsprogramm ausgeführt werden. Führen Sie im Installationsverzeichnis (standardmäßig unter `C:\NetIQ\idm\apps\UserApplication\`) den folgenden Befehl aus: `configupdate.bat`
Beim Starten von Tomcat tritt die folgende Ausnahme auf: `port 8180 already in use`	Schließen Sie alle Instanzen von Tomcat (oder anderer Server-Software), die möglicherweise bereits laufen. Wenn Sie Tomcat neu konfigurieren und einen anderen Port als Port 8180 festlegen möchten, bearbeiten Sie die `config`-Einstellungen für den Benutzeranwendungstreiber.
Beim Starten von Tomcat meldet die Anwendung, dass keine verbürgten Zertifikate gefunden werden können.	Starten Sie Tomcat in jedem Fall mit dem JDK, das bei der Installation von Identity Applications angegeben wurde.
Die Anmeldung bei der Portaladministratorseite ist nicht möglich.	Überprüfen Sie, ob ein Konto für den Identity Applications-Administrator vorhanden ist. Dieses Konto ist nicht mit dem OpenText Identity Console-Administratorkonto identisch.
Auch mit einem Administratorkonto können keine neuen Benutzer angelegt werden.	Der Administrator für Identity Applications muss ein Trustee des Containers der obersten Ebene sein und sollte über Supervisor-Rechte verfügen. Sie können versuchen, die Rechte des Identity Applications-Administrators mit denen des LDAP-Administrators gleichzusetzen (in der OpenText Identity Console).
Beim Starten des Anwendungsservers treten Keystore-Fehler auf.	Ihr Anwendungsserver verwendet nicht das bei der Installation von Identity Applications angegebene JDK. Importieren Sie die Zertifikatsdatei mithilfe des Befehls `keytool`: `keytool -import -trustcacerts -alias` *`aliasName`* `-file` *`certFile`* `-keystore ..\lib\security\cacerts -storepass changeit` ◆ Ersetzen Sie *aliasName* durch einen beliebigen eindeutigen Namen für dieses Zertifikat. ◆ Ersetzen Sie *certFile* durch den vollständigen Pfad und Namen der Zertifikatsdatei. ◆ Das Keystore-Standardpasswort lautet `changeit` (falls Sie ein anderes Passwort festgelegt haben, geben Sie es an).

Problem	Empfohlene Vorgehensweise
Es werden keine Email-Benachrichtigungen gesendet.	Überprüfen Sie mit dem `configupdate`-Dienstprogramm, ob Sie Werte für die Identity Applications-Konfigurationsparameter **Email-Von** und **Email-Host** angegeben haben. Führen Sie im Installationsverzeichnis (standardmäßig unter `C:\NetIQ\idm\apps\UserApplication\`) den folgenden Befehl aus: `configupdate.bat`

Fehlersuche bei der Installation und Deinstallation

Die nachfolgende Tabelle enthält die möglichen Probleme und Vorschläge für Gegenmaßnahmen. Falls das Problem weiterhin auftritt, wenden Sie sich an Ihren zuständigen OpenText-Ansprechpartner.

Problem	Empfohlene Vorgehensweise
OpenText Identity Manager autorisiert und kommuniziert sicher mit seinen Komponenten über digitale Zertifikate. Die Zertifikate des Identitätsdepots müssen in die Schlüsselspeicher-Dateien `idm.jks` und `tomcat.ks` importiert werden. Wenn Sie jedoch versuchen, nach dem Import der Zertifikate auf Identity Applications zuzugreifen, kann die folgende Fehlermeldung auftreten: `javax.net.ssl.SSLHandshakeException: PKIX-Pfadüberprüfung fehlgeschlagen: java.security.cert.CertPathValidatorException: Widerrufstatus konnte nicht ermittelt werden.` Beim Validieren der Zertifikate werden die Zertifikatswiderruflisten (CRLs) überprüft, die durch das Feld CRL-Verteilungspunkt (CDP) angegeben sind. Dadurch wird festgelegt, ob das Zertifikat widerrufen wurde oder nicht. Die CRLDPs sind sowohl im Stammzertifikat als auch in den Zwischenzertifikaten verfügbar, die sich in den Keystore-Dateien `tomcat.ks` und `idm.jks` befinden. Die Überprüfung von Zertifikaten auf Widerruf ist jedoch standardmäßig deaktiviert. Infolgedessen ist der PKIX Trust Manager nicht in der Lage, den Widerrufstatus der Zertifikate zu ermitteln.	Zur Behebung dieses Problems aktivieren Sie die Überprüfung der CRL-Verteilungspunkte, indem Sie die Eigenschaft `-Dcom.sun.security.enableCRLDP` auf `true` festlegen. Gehen Sie zum Festlegen der Eigenschaft folgendermaßen vor: 1. Halten Sie Tomcat an. 2. Rufen Sie die Datei `setenv.sh` auf, die sich im `bin`-Ordner von Tomcat befindet. Beispiel: `C:\NetIQ\idm\apps\tomcat\bin\setenv.bat`. 3. Fügen Sie in CATALINA_OPTS die Eigenschaft `-Dcom.sun.security.enableCRLDP=true` hinzu: `export CATALINA_OPTS="-Dcom.sun.security.enableCRLDP=true"` 4. Starten Sie Tomcat.

Problem	Empfohlene Vorgehensweise
Nach dem Aufrüsten von OpenText Identity Manager ist die Anmeldung beim OpenText Identity Manager-Dashboard für Benutzer, die keine Administratoren sind, extrem langsam. Das Laden der Anwendungen und der Dashboard-Seiten wird erheblich verzögert. Dieses Problem tritt aufgrund der verschachtelten Gruppensuche auf, die standardmäßig aktiviert ist. Die Anwendung sucht nach den Berechtigungen, die der angemeldete Benutzer über die verschachtelte Gruppenzugehörigkeit übernommen hat, unabhängig davon, ob es in der Umgebung verschachtelte Gruppen gibt.	(Bedingt) Die folgenden Schritte gelten für OpenText Identity Manager 4.8.5 und höher. 1. Melden Sie sich bei dem Server an, auf dem Identity Applications auf die Version 4.8.5 aufgerüstet wurde. 2. Navigieren Sie zum Speicherort `C:\NetIQ\IDM\apps\tomcat\conf`. 3. Öffnen Sie die Datei `ism-configuration.properties` in einem Texteditor. 4. Fügen Sie am Ende der Datei folgende Eigenschaft hinzu: `DirectoryService/realms/jndi/params/USE_NESTED_GROUPS=false` 5. Speichern Sie die Datei und starten Sie Tomcat neu.
Nachdem Sie Identity Applications auf die Version 4.8.x aufgerüstet haben, können Sie sich nicht mehr beim Identity Applications-Dashboard anmelden. Dieses Problem tritt auf, wenn der Truststore-Pfad des Identitätsdepots während des Aufrüstens von Identity Applications nicht auf den richtigen Speicherort der Keystore-Datei (`cacerts`) aktualisiert wird. In der Datei `catalina.out` wird folgende Ausnahme protokolliert: `com.netiq.idm.auth.oauth.AuthenticationCommunicationException: javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path validation failed: sun.security.validator.ValidatorException: TrustAnchor with subject "CN=***, OU=idm, O=***, L=***, ST=***, C=**" ist kein Zertifikat einer Zertifizierungsstelle"`  Identity Applications verwendet die Umgebungsvariable JAVA_HOME, die auf `<install_path>\Common\JRE` festgelegt ist. Wenn der Truststore-Pfad in JAVA_HOME nicht auf die Datei `cacerts` festgelegt ist, schlägt die SSL-Kommunikation fehl. Dies führt zu einem SSL-Fehler in Verbindung mit 'TrustAnchor' (Trust Anchor wird als erweiterte Java-Sicherheitsprüfung für SSL-Zertifikate verwendet).	Gehen Sie wie folgt vor, um dieses Problem zu beheben: 1. Halten Sie den Tomcat-Dienst an. 2. Melden Sie sich am Identity Applications-Server an und starten Sie das Dienstprogramm `configupdate`, das sich unter `<Installationspfad>\idm\apps\configupdate` befindet. 3. Gehen Sie auf der Registerkarte Benutzeranwendung zu **Identitätsdepot-Zertifikate** und vergewissern Sie sich, dass der **Truststore-Pfad** auf `<Installationspfad>\Common\JRE\lib\security\cacerts` festgelegt ist. 4. Starten Sie den Tomcat-Dienst.

Problem	Empfohlene Vorgehensweise

Nach dem Aufrüsten von OpenText Identity Manager auf Version 4.8.1 in einer verteilten Umgebung schlägt die Anmeldung bei Identity Applications fehl. Die folgende Fehlermeldung wird angezeigt:
`Ihr Anmeldevorgang wurde nicht erfolgreich abgeschlossen.`
Die Anmeldung bei Identity Applications erfordert Vertrauensanker-Zertifikat für die Herstellung einer sicheren Verbindung zwischen den Identity Applications und dem OSP. Ein Vertrauensanker-Zertifikat muss die Basiseinschränkungserweiterung enthalten, wobei als Subjekttyp „CA“ festgelegt ist. OpenText Identity Manager verwendet die Eigenschaft `jdk.security.allowNonCaAnchor`, um die Vertrauensanker im Zertifikat zu validieren. Standardmäßig ist diese Eigenschaft auf `false` festgelegt. Wenn die Vertrauensanker in den Zertifikaten nicht gefunden werden, kann daher die Verbindung zwischen Identity Applications und OSP nicht hergestellt werden, und die Anmeldung schlägt fehl. In der Datei `idm-osp.log` bemerken Sie außerdem die folgende Ausnahme:
`sun.security.validator.ValidatorException: TrustAnchor with subject "CN=***, L=***, O=***" is not a CA certificate`
	Um dieses Problem zu lösen, müssen Sie eine der folgenden Bedingungen erfüllen:
	◆ Stellen Sie sicher, dass es sich bei den Zertifikaten, die zum Aufbau einer sicheren Verbindung zwischen den Identity Applications und dem OSP verwendet werden, um verbürgte Zertifizierungsstellenzertifikate mit der entsprechenden Basiseinschränkungserweiterung handelt.
	◆ Bei selbstsignierten und benutzerdefinierten Zertifikaten, denen die Clients vertrauen, können Sie die Eigenschaft `jdk.security.allowNonCaAnchor` ändern, um nicht von einer Zertifizierungsstelle stammende Zertifikate ohne die Basiseinschränkungserweiterung zuzulassen. Führen Sie die folgenden Aktionen durch, um die Java-Sicherheitseinstellungen zu ändern:
	1. Navigieren Sie zum Verzeichnis `C:\NetIQ\idm\apps\jre\lib\security\java.security`.
	2. Legen Sie folgenden Eigenschaftswert fest: `jdk.security.allowNonCaAnchor=true`.
	3. Speichern Sie die Datei.

Nach dem Aufrüsten von Identity Applications auf Version 4.8.1 können Sie keine Formulare öffnen, während Sie im Identity Applications-Dashboard Berechtigungen anfordern.	Gehen Sie wie folgt vor, um dieses Problem zu beheben: 1. Drücken Sie Windows + R auf Ihrer Tastatur, geben Sie `services.msc` ein und wählen Sie **OK**, um die Schnittstelle für Windows-Dienste zu öffnen. 2. Suchen Sie nach den Dienstnamen, **NetIQ Nginx-Dienst** und **NetIQ IGA-Formular-Renderer-Dienst**. Klicken Sie mit der rechten Maustaste auf den Dienst und wählen Sie die Option **Neu starten** aus. In Identity Applications wird der NGNIX-Dienst zum Rendern von Formularen im Identity Applications-Dashboard verwendet.
Nach dem Aufrüsten von Identity Applications oder Identity Reporting auf die Version 4.8 werden mehrere Einträge von PostgreSQL in der Systemsteuerung angezeigt.	Deinstallieren Sie die Vorversionen von PostgreSQL über die Systemsteuerung.

Problem	Empfohlene Vorgehensweise
Die Deinstallation meldet, dass der Deinstallationsvorgang nicht abgeschlossen wurde, in der Protokolldatei sind jedoch keine Fehler vermerkt.	Der Deinstallationsvorgang hat das Verzeichnis `netiq`, in dem sich standardmäßig die Installationsdateien befindet, nicht gelöscht. Sobald Sie die gesamte NetIQ-Software vom Computer entfernt haben, können Sie das Verzeichnis löschen.
Nach dem Aufrüsten von OpenText Identity Manager wird die folgende Eigenschaft der Datei `ism-configuration.properties` hinzugefügt: `com.netiq.idm.osp.ldap.admin-dn = cn=admin,ou=sa,o=system`	Kommentieren Sie die Eigenschaft in der Datei `ism-configuration.properties` aus und starten Sie Tomcat neu. Die Funktionsfähigkeit wird nicht eingeschränkt.
Nach dem Aufrüsten von OpenText Identity Manager wird die folgende SSPR-Eigenschaft der Datei `ism-configuration.properties` hinzugefügt, auch wenn SSPR in Ihrer Bereitstellung nicht enthalten ist: `com.netiq.sspr.redirect.url = https://___SSPR_IP___:___SSPR_TOMCAT_HTTPS_PORT___/sspr/public/oauth`	Kommentieren Sie die Eigenschaft in der Datei `ism-configuration.properties` aus und starten Sie Tomcat neu. Die Funktionsfähigkeit wird nicht eingeschränkt.
Tomcat kann nach dem Aufrüsten von OpenText Identity Manager nicht gestartet werden. Sie stellen fest, dass die Tomcat-Protokolle einige Ausnahmen und einen Kommunikationsfehler zwischen der Workflow-Engine und dem Identitätsdepot enthalten.	1. Melden Sie sich bei der OpenText Identity Console an. 2. Navigieren Sie zu **Zertifikatsverwaltung** > **Server-Zertifikatsverwaltung**. 3. Aktivieren Sie das Kontrollkästchen **SSL CertificateDNS** und klicken Sie auf **Exportieren**. 4. Wählen Sie in der Dropdown-Liste **Zertifikate** die Option *SSL CertificateDNS* aus. 5. Deaktivieren Sie das Kontrollkästchen **Privaten Schlüssel exportieren**. Stellen Sie sicher, dass **Exportformat** auf *DER* festgelegt ist. 6. Klicken Sie auf **OK** > **Exportiertes Zertifikat speichern**, um das Zertifikat auf Ihr System herunterzuladen. 7. Melden Sie sich beim Identity Applications-Server an. 8. Halten Sie Tomcat an. 9. Navigieren Sie zum Verzeichnis `opt/netiq/common/jre/bin` und importieren Sie das Zertifikat mit dem folgenden Befehl in die Datei `idm.jks`: `opt/netiq/common/jre/bin/keytool -import -trustcacerts -alias <Zertifikat-Aliasname> -keystore /opt/netiq/idm/apps/tomcat/conf/idm.jks -file <heruntergeladene Zertifikatdatei>` 10. Starten Sie Tomcat neu.

Problem	Empfohlene Vorgehensweise
Nach dem Aufrüsten von OpenText Identity Manager 4.7.4 auf 4.8 wird der Tomcat-Dienst nicht gestartet und in den Protokolldateien werden keine Fehler gemeldet. Dieses Problem tritt auf, wenn der Heartbeat-Zeitgeber in der afenginestate-Tabelle der igaworkflow-Datenbank nicht richtig aktualisiert wurde.	Um dieses Problem zu lösen, melden Sie sich bei einem Datenbank-Verwaltungswerkzeug wie pgAdmin an. Führen Sie die folgende Abfrage aus, um den Heartbeat-Zeitgeber in der afenginestate-Tabelle der igaworkflow-Datenbank manuell zu aktualisieren. `update afenginestate set heartbeat=now()::timestamp;`
Nach der Installation von Identity Reporting über die Standard Edition und der Ausführung des Tomcat-Service wird möglicherweise dieser Fehler angezeigt: `"Error loading bootstrap configuration properties. Unable to obtain properties from bootstrap configuration."`	Starten Sie den Tomcat-Service neu.

Fehlersuche bei der Anmeldung

Die nachfolgende Tabelle enthält die möglichen Probleme und Vorschläge für Gegenmaßnahmen. Falls das Problem weiterhin auftritt, wenden Sie sich an Ihren zuständigen OpenText-Ansprechpartner.

Problem	Empfohlene Vorgehensweise
Wenn Identity Applications und Identity Reporting auf demselben Server installiert sind und Sie Konfigurationsänderungen mit dem Konfigurationsaktualisierungsprogramm durchführen, das sich im Verzeichnis <`Reporting-Installationsordner`>`\bin` befindet, kann das OpenText Identity Manager-Dashboard nicht gestartet werden. Der folgende Fehler wird in der Protokolldatei `catalina.out` gemeldet: `EboPortalBootServlet [RBPM] +++++ACHTUNG!: Dieser Portalanwendungskontext, IDMProv, stimmt nicht mit der portal.context-Eigenschaft überein, die in der Datei PortalService-conf/config.xml festgelegt ist. Pro Datenbank ist nur ein Portal zulässig Mithilfe des vorigen Portalkontexts wurden Daten geladen. Zur Behebung müssen Sie zum vorherigen Portalnamen, NoCacheFilter, zurückkehren. Bitte lesen Sie in der Dokumentation nach.`	Verwenden Sie für alle Konfigurationsänderungen das Konfigurationsaktualisierungsprogramm, das sich im Verzeichnis `C:\NetIQ\idm\apps\UserApplication` befindet.

Problem	Empfohlene Vorgehensweise
Der Benutzer kann sich in einer großen Umgebung (> 2 Millionen Objekte) nicht anmelden.	Ergänzen Sie sowohl den OpenText eDirectory-Master-Server als auch den Reproduktionsserver mit einem Index für das Attribut `mail(Internet-Email-Adresse)` mit der Regel `Wert`.
Beim Abmelden von der Seite der Identity Applications zeigt SSPR den Fehler `5053 ERROR_APP_UNAVALIABLE` (Fehler – Anwendung nicht verfügbar).	Ignorieren Sie diesen Fehler. Die Funktionsfähigkeit wird nicht eingeschränkt.
Bei der ersten Anmeldung bei den Identity Applications werden keine Challenge-Response-Fragen angezeigt.	1. Prüfen Sie, ob der SSPR-Server ein mit FQDN erstelltes Zertifikat enthält. 2. Melden Sie sich beim Identity Applications-Server an und starten Sie das ConfigUpdate-Dienstprogramm (`<Installationspfad>\apps\UserApplication`). 3. Navigieren Sie zu **SSO-Clients** > **Selbstständiges Zurücksetzen des Passworts** und prüfen Sie, ob die Einstellungen fehlerfrei sind. Wenn SSPR auf einem separaten Server installiert ist, muss das SSPR-Zertifikat in die Datei `idm.jks` auf dem Identity Applications-Server unter `/netiq/idm/apps/tomcat/conf` importiert werden.

Problem	Empfohlene Vorgehensweise
Browser zeigt beim Zugriff auf die SSPR-URL eine leere Seite an.	Dieser Fall tritt ein, wenn SSPR nicht ordnungsgemäß für OSP konfiguriert ist. Das SSPR-Protokoll zeigt die folgenden Informationen: `2018-01-24T22:24:02Z, ERROR, oauth.OAuthConsumerServlet, 5071 ERROR_OAUTH_ERROR (unexpected error communicating with oauth server: password.pwm.error.PwmUnrecoverableException: 5071 ERROR_OAUTH_ERROR (io error during oauth code resolver http request to oauth server: Certificate for <IP> doesn't match any of the subject alternative names: [IP]))` 1. Prüfen Sie, ob der Tomcat-Server, auf dem OSP ausgeführt wird, ein gültiges, mit FQDN erstelltes Zertifikat enthält. Melden Sie sich beim Identity Applications-Server an und starten Sie das ConfigUpdate-Dienstprogramm. Navigieren Sie zu **SSO-Clients > Selbstständiges Zurücksetzen des Passworts** und prüfen Sie, ob die Einstellungen fehlerfrei sind. 2. Melden Sie sich bei SSPR an und umgehen Sie dabei die OSP-Anmeldemethode (Beispiel: `https://<SSPR-Server-IP>:<Port>/sspr/private/Login?sso=false`). 3. Navigieren Sie zum **Konfigurationseditor** oben rechts auf der Seite. 4. Wählen Sie **Passwort konfigurieren** und klicken Sie auf **Anmelden**. 5. Navigieren Sie zu **LDAP** > **LDAP-Verzeichnisse** > **Standard** > **Verbindung**. 6. Wenn das LDAP-Zertifikat nicht korrekt ist, klicken Sie auf **Löschen**. 7. Importieren Sie das Zertifikat mit **Vom Server importieren** erneut. 8. Navigieren Sie zu **Einstellungen > Single-Sign-On(SSO)-Client > OAuth** und prüfen Sie, ob das richtige Zertifikat unter **OAUTH-Webservice-Serverzertifikat** angezeigt wird. 9. Wenn das Zertifikat nicht korrekt ist, klicken Sie auf **Löschen**. 10. Importieren Sie das Zertifikat mit **Vom Server importieren** erneut.

Problem	Empfohlene Vorgehensweise
Wenn Sie sich nach der Installation aller Komponenten nicht beim Datenerfassungsdiensttreiber (Identity Manager Driver for Data Collection Service) oder bei Identity Reporting anmelden können und die Fehlermeldung „Login failed, please try again“ (Anmeldung fehlgeschlagen, versuchen Sie es erneut) angezeigt wird	Starten Sie den Servercomputer neu und starten Sie den Tomcat-Dienst neu.

Behebung des SSPR-Seitenanforderungsfehlers

Die nachfolgende Tabelle enthält die möglichen Probleme und Vorschläge für Gegenmaßnahmen. Falls das Problem weiterhin auftritt, wenden Sie sich an Ihren zuständigen OpenText-Ansprechpartner.

Problem	Empfohlene Vorgehensweise
Fehlermeldung über nicht funktionierende Seitenanforderung in SSPR Dieses Problem tritt auf, wenn Sie auf einer SSPR-Seite auf die Schaltfläche **Zurück** klicken. SSPR gibt im SSPR-Fehlerprotokoll eine Nachricht über eine fehlerhafte Sequenz an, die ungefähr wie folgt aussieht: `ERROR, password.pwm.servlet.TopServlet, 5035 ERROR_INCORRECT_REQUEST_SEQUENCE (expectedPageID=3, submittedPageID=4, url=<some sspr url>`	Deaktivieren Sie die Erkennung der Zurück-Schaltfläche unter **SSPR Configuration Manager > Settings > Security > Web Security**. **HINWEIS:** Eine Änderung dieser Einstellung wirkt sich nicht auf Endbenutzer aus.

Weitere Informationen zu allgemeinen Problemen bei der Authentifizierung oder beim Anmelden bei Identity Applications finden Sie im *OpenText™ Identity Manager CE 24.4 (v4.10) – Administratorhandbuch zu Identity Applications*.

Fehlersuche zu dem Problem ".NET Remote Loader startet nicht" unter Windows 2016

Die nachfolgende Tabelle enthält die möglichen Probleme und Vorschläge für Gegenmaßnahmen. Falls das Problem weiterhin auftritt, wenden Sie sich an Ihren zuständigen OpenText-Ansprechpartner.

Problem	Empfohlene Vorgehensweise
Dieses Problem tritt zufällig auf. Es tritt möglicherweise auf, wenn die Schrifteinstellungen der Befehlseingabeaufforderung des .NET Remote Loader nicht mit den Standardeinstellungen des Host-Betriebssystems übereinstimmen.	Ändern Sie die Einstellungen der Befehlseingabeaufforderung, damit sie mit den Standardsystemeinstellungen übereinstimmen. Löschen Sie dazu den Registrierungsschlüssel HKEY_CURRENT_USER\Console und starten Sie den Server dann neu.

Fehlerbehebung 502 Fehlerhaftes Gateway beim Laden der Formulare in der Azure-Bereitstellung

Die nachfolgende Tabelle enthält die möglichen Probleme und Vorschläge für Gegenmaßnahmen. Falls das Problem weiterhin auftritt, wenden Sie sich an Ihren zuständigen OpenText-Ansprechpartner.

Problem	Empfohlene Vorgehensweise
Nach der Bereitstellung der IDM 4.8-Komponenten in der Azure-Umgebung. Wenn Sie im IDM-Dashboard auf ein Helpdesk-Ticket klicken oder versuchen, eine Aufgabe zu genehmigen, wird möglicherweise der folgende Fehler angezeigt. `502 - Web server received an invalid response while acting as a gateway or proxy server.`	Führen Sie die folgenden Schritte aus, um das Problem zu beheben: 1. Navigieren Sie in Ihrem System zum Speicherort von `Nginx\conf`. Beispiel: `C:\NetIQ\Common\Nginx\conf` 2. In der Datei `nginx.conf`: a. Fügen Sie unterhalb der Zeile **error_page 502 /502.html;** die Zeile `error_page 404 =200 /404.html` ein. b. Legen Sie **proxy_intercept_errors off;** auf `proxy_intercept_errors on;` fest. 3. Starten Sie unter Services.msc den NetIQ Nginx-Dienst neu.